FEBURARY 2026

ENTERPRISE RESILIENCE GOVERANCE FOR THE MODERN WORLD

A NEW OPERATING DOCTRINE FOR ASSET-INTENSIVE ORGANISATIONS

G E KLEPPE

Contents

Introduction

Where Governance Actually Fails

Across infrastructure, energy and complex operating environments, governance does not fail because frameworks are absent. It fails because accountability is not anchored at the point where risk materialises.

Boards approve policies. Risk is categorised. Compliance is demonstrated. Contracts allocate responsibility across sponsors, operators and suppliers. Regulatory frameworks add formal oversight and expectations on paper and in recent years some regimes have explicitly tightened their focus on outcomes and critical assets. Yet, even where these frameworks are in place, disruption still reveals that control can be illusory when accountability is not anchored at the level where risk materialises.

Yet when disruption occurs, that control frequently proves illusory.

Major transport networks experience cascading failures triggered by relatively minor system faults. Energy systems disconnect under conditions they were expected to withstand. Digital platforms that underpin physical operations fail, forcing shutdowns of otherwise functional infrastructure. Post-incident reviews often conclude that governance was “in place” and that risks had been “identified”. These findings offer little comfort.

The issue is not whether governance exists. It is whether governance operates where it matters.

In asset-intensive environments, risk does not sit neatly within organisational functions. It converges at the asset, where operational systems, cyber infrastructure, contractual obligations, regulatory duties and supply chains intersect in real time. That is where performance is determined. That is where failure occurs.

Where no single party is accountable for how that asset performs under changing conditions, governance becomes fragmented. Responsibility is distributed across functions, organisations and contractual boundaries. Each participant holds a partial view. None holds the whole. This fragmentation is not immediately visible. Under stable conditions, systems continue to operate. Reports remain green. Compliance is maintained. The underlying structural weakness only becomes apparent under stress.

When disruption occurs, decision-making slows. Responsibility is contested. Recovery is delayed. The organisation discovers that while accountability was defined, it was not operationalised. The consequences extend beyond operational inconvenience. They are financial, regulatory and reputational.

Operational disruption translates directly into cost. Delays, outages and inefficiencies erode margins. Recovery efforts consume resources. Contractual disputes arise as parties seek to allocate blame for failure.

Regulators are increasingly explicit that they are concerned with real-world outcomes, not governance intent. When systems fail, inquiries now focus on whether boards and executives can demonstrate control at the level where failure occurred, including asset, service and ecosystem dependencies; not simply whether policies existed. Where they cannot, regulatory intervention, enforcement and expectations typically increase.

Reputational consequences are often the most enduring. Trust is eroded among stakeholders, customers and investors. In regulated sectors, these consequences are not absorbed solely by organisations. They are transferred to consumers through increased prices, reduced service quality or constrained investment.

This creates a direct relationship between governance quality and societal outcomes.

Traditional governance has relied on structure as the primary mechanism of control: define responsibilities, allocate risk, and monitor compliance. That model works best where systems are relatively stable and interactions are limited. Modern infrastructure systems remain governed through these structures, but in practice they are dynamic, tightly interconnected and increasingly dependent on digital platforms.

Modern infrastructure systems are neither stable nor predictable.

They are dynamic, interconnected and increasingly dependent on digital platforms. Their behaviour is shaped by interactions across domains that are governed separately. The assumption that structure alone can ensure control no longer holds.

Enterprise resilience offers an alternative.

It is not a framework layered on top of existing governance. It is a different way of defining and operationalising accountability. It recognises that control must be exercised at the point where risk materialises. It requires that accountability be clear, enforceable and supported by evidence.

The distinction between traditional governance and enterprise resilience is not theoretical. It is operational.

One focuses on defining responsibility. The other focuses on ensuring that responsibility can be exercised effectively under real conditions.

This book sets out that distinction.

It begins by examining why traditional governance fails in asset-intensive environments. It then explores how risk behaves in modern systems, and why those behaviours expose structural weaknesses in existing governance approaches.

From there, it introduces accountability as the central mechanism through which resilience is achieved. It defines what asset-level accountability means in practice and how it can be structured across organisations and ecosystems.

The latter sections focus on implementation. They describe the operating model required to support enterprise resilience, including governance, decision-making and evidence. They also examine the financial and strategic implications of this shift, particularly for Boards and executive leadership.

The objective is not to critique governance frameworks. It is to reposition where governance must operate.

The central proposition in this book is straightforward – governance failure is, in practice, a financial and operational outcome of missing asset-level accountability. Others have recognised elements of this in asset management, operational resilience and critical infrastructure guidance, but they often remain as specialist streams.

This book brings those strands together into a single operating doctrine for boards and executives.

Section 1 - Structural Failure Of Governance

Governance Designed for Stability

Governance frameworks have evolved over decades to address risk in increasingly complex organisations. They are built on principles of accountability, transparency and control. These principles remain valid. What has changed is the environment in which they operate.

Traditional governance assumes a relatively stable system. Risks can be identified, categorised and managed within defined boundaries. Responsibilities can be allocated to functions or roles. Performance can be monitored through periodic reporting. These assumptions are embedded in how governance is structured.

Boards approve policies and risk appetites. Executive teams translate these into frameworks and procedures. Functions manage risks within their domains. Assurance activities verify compliance. This model works where systems are predictable and interactions are limited. In modern infrastructure environments, neither condition holds.

Systems are dynamic. They evolve continuously through technological change, operational adaptation and external pressures. Interactions between components are complex and often poorly understood. Dependencies extend beyond organisational boundaries into supply chains, platforms and regulatory ecosystems.

Governance is static. Governance is often treated as largely fixed after key decision points such as financial close. Frameworks and contracts may be adjusted over time, but the underlying allocation of accountability, risk and information flows typically changes slowly.

Meanwhile the system itself evolves continuously through technology, regulation and operating conditions, creating a widening gap between how the organisation operates and how it is governed.

The Illusion of Control at Financial Close

Financial close represents a critical moment in infrastructure projects. It marks the transition from planning to execution. Capital is committed. Contracts define responsibilities. Regulatory approvals confirm compliance.

At this point, governance appears complete. Risks have been identified and allocated. Responsibilities are documented. Incentives are aligned through contractual mechanisms. From a governance perspective, the system appears controlled. This perception is reinforced by the formality of the process. Legal agreements are detailed. Financial models are robust. Regulatory requirements are satisfied.

However, this control is largely theoretical.

Contracts define how risks are shared between parties. They do not ensure that those risks are effectively managed in operation. Regulatory approvals confirm that minimum requirements are met. They do not guarantee performance under changing conditions.

Most importantly, financial close does not establish enduring accountability for asset performance. Responsibilities are defined within contractual scopes. These scopes are bounded. They do not extend to how the asset behaves as technologies evolve, as operating conditions change or as new dependencies emerge.

As a result, accountability becomes fragmented.

Different parties are responsible for different aspects of the asset. Project sponsors oversee delivery. Operators manage day-to-day performance. Vendors provide technology and services. Regulators enforce compliance. Each has a role. None has complete accountability for the asset as an integrated system.

This fragmentation is often accepted as inevitable in complex projects. It is managed through coordination mechanisms, governance committees and reporting structures. These mechanisms are necessary however they are not sufficient.

When the asset enters operation, the limitations become apparent.

Design decisions made at financial close become embedded in the system. Interfaces between components are fixed. Performance assumptions are tested against reality. Where these assumptions prove incorrect, accountability for resolving issues is unclear. Problems that span multiple domains fall between responsibilities. Resolution requires coordination across parties with different incentives, priorities and levels of authority. This slows response. It increases cost. It creates dispute.

The illusion of control gives way to operational complexity.

Governance Without Translation

The limitations of governance at financial close are compounded by a second structural issue: the failure to translate governance into operation. Boards operate at a strategic level. They define risk appetite, approve policies and oversee performance. They rely on executive teams to implement these decisions.

This delegation is appropriate. It becomes problematic when there is no clear mechanism to translate Board intent into asset-level accountability. Risk appetite statements are typically expressed in broad terms. They define acceptable levels of risk across categories. They do not specify how these levels should be applied to individual assets. Policies and frameworks provide guidance. They do not define how decisions should be made in specific situations. Reporting aggregates information. It does not reveal how assets are performing in real time.

Emerging supervisory expectations in areas such as operational resilience and critical infrastructure risk management recognise this translation gap and now require boards to evidence how high-level risk appetite is reflected in decisions, controls and accountability at the level of specific assets and services

The result is a disconnect.

Board decisions are not directly linked to asset behaviour. There is no clear line of sight from strategic intent to operational reality. This disconnect is often masked by reporting. Risk reports present a summary view of performance. They indicate whether risks are within appetite. They highlight key issues. They provide assurance that controls are in place.

These reports are necessary. They are not sufficient. They do not show how individual assets are performing against resilience expectations. They do not reveal where accountability sits for that performance. They do not provide evidence of how systems behave under stress.

As a result, Boards may believe governance is effective when underlying issues exist.

This creates a false sense of security.

Structural Consequences

The combination of static governance design and lack of translation creates structural consequences.

- First, risk accumulates in areas that are not clearly owned. Dependencies on digital platforms, data systems and suppliers often fall outside traditional governance boundaries. They are treated as technical or procurement issues. Their impact on asset performance is not fully accounted for.
- Second, decision-making becomes fragmented. When issues arise, multiple parties must be involved. Each has partial authority. Decisions require negotiation. This slows response and increases complexity.
- Third, accountability becomes difficult to enforce. When responsibilities are shared, it is challenging to assign accountability for outcomes. Post-incident reviews identify contributing factors but struggle to assign clear responsibility. This limits learning. It reduces the effectiveness of corrective actions.
- Finally, financial impacts increase. Delays, disruptions and disputes consume resources. Projects overrun. Operations become less efficient. Regulatory interventions impose additional costs. These impacts are often attributed to external factors. In many cases, they reflect underlying governance weaknesses.

These outcomes are increasingly being framed as governance issues in regulatory reviews and inquiries, not just operational failures, because they reflect how boards have chosen to structure accountability and oversight.

The structural failures described in this section are not isolated. They are a direct consequence of how risk behaves in modern systems. To address them, it is necessary to understand where risk actually materialises and how it propagates. That is the focus of the next section.

Additional Cases

The structural weaknesses described in this section are visible across multiple asset-intensive sectors, even where governance frameworks are formally mature.

Case 1 – PPP toll road dispute (infrastructure, global)

A major toll road developed under a public-private partnership reached financial close with detailed contracts, risk allocation schedules and lender protections in place. During operation, traffic volumes consistently underperformed the original model due to shifts in commuting patterns and competing infrastructure. Responsibility for addressing the revenue gap sat uneasily between the private operator, construction consortium and procuring authority. Each party pointed to contractual boundaries. No single executive was clearly accountable for how the asset should be adapted to the new operating reality. Disputes escalated, refinancing failed, and the project ultimately entered restructuring. Post-facto reviews found that while governance at transaction close was comprehensive, there was no enduring asset-level accountability for performance under changing conditions.

Case 2 – Hospital redevelopment IT–facility integration (health, OECD)

A hospital redevelopment program delivered new clinical facilities, upgraded building systems and a separate electronic medical record roll-out under different contracts. Governance at financial close treated construction, IT and clinical operations as distinct workstreams, each with its own steering committee and reporting. Once the facility opened, latent integration issues emerged: building management systems, clinical devices and the EMR did not interact as expected. Bed allocation, patient flow and theatre utilisation deteriorated. Each stream could demonstrate compliance with its

scope, yet no executive owned the end-to-end performance of the hospital as an integrated asset. The board faced quality, safety and reputational risks despite "green" traffic lights in project reporting. The failure lay in structural governance fragmentation rather than any single party's non-compliance.

Case 3 – Local government critical asset maintenance (Australia)

Several local governments have faced inquiries and regulatory criticism following failures of dams, bridges or waste facilities where maintenance had been deferred. Asset management plans existed, budgets were approved annually and audits confirmed procedural compliance. However, responsibility for the long-term performance of specific critical assets was diffused across engineering, finance and procurement. Councils often lacked a named owner for each crown-jewel asset with authority to make trade-offs between cost, risk and service outcomes. When failures occurred, investigations concluded that governance frameworks and policies were present, but accountability at the asset level was neither clear nor enforced.

These cases can be lightly localised (e.g. pick a real Australian PPP example once you confirm which you are comfortable referencing).

CPS and structural governance gaps

Cyber-physical systems [CPS] make the structural weaknesses in traditional governance visible and, if used well, help address them. A CPS can be understood as the integrated whole created when physical assets, control systems, digital platforms and data flows operate as a single system in real time. In most asset-intensive organisations, critical assets now function as CPS, even if they are not labelled that way – substations, rail signalling systems, treatment plants and transmission networks all combine operational technology, IT, data and external platforms.

Governance, however, often remains organised around organisational structure rather than system behaviour. Engineering owns physical design, IT owns networks and applications, cyber teams' own security controls, and risk and compliance own frameworks and reporting. Contracting then slices this CPS into scopes for different vendors and service providers. At financial close, each slice appears well controlled, with defined responsibilities and service levels. Yet no single role is accountable for the performance and resilience of the CPS as an integrated asset under changing conditions.

CPS thinking makes this problem explicit. A CPS has defined boundaries, interfaces and behaviours that can be modelled, monitored and tested as a whole. When governance does not recognise the CPS as the unit of control, several predictable consequences follow:

- Risks that emerge at interfaces between components are owned by no one;
- Changes to one domain (for example a software update or data integration) can create latent failures elsewhere without formal review; and
- Evidence about how the asset behaves under stress is fragmented across systems and suppliers.

Emerging guidance for critical infrastructure and OT environments responds to this by requiring owners and operators to maintain inventories of critical assets and systems, identify their dependencies and assign accountable owners. When combined with CPS architectures – digital twins, integrated monitoring and asset-centric data models – this creates the foundation for asset-level accountability that traditional governance has lacked. The CPS becomes not just a technical construct, but the practical unit through which boards and executives can define, monitor and enforce control where risk actually materialises.

Section 2 - Where Risk Actually Materialises

From Categories to Conditions of Failure

The structural weaknesses described in the previous section are not incidental. They arise because governance is organised around categories of risk, while failure emerges under conditions where those categories intersect. **This distinction is critical**. Most organisations classify risk into domains. Cyber risk is managed separately from operational risk. Regulatory compliance is distinct from financial performance. Supplier risk sits within procurement. Data risk is treated as an IT concern.

Each domain is assigned ownership. Frameworks define controls. Reporting tracks performance. This approach creates clarity within each domain. It does not capture how risks behave in combination. In modern infrastructure and asset-intensive systems, risks rarely manifest in isolation. They converge.

A cyber vulnerability does not remain confined to information systems. It affects operational control. A supplier failure does not remain a contractual issue. It disrupts service delivery. A regulatory change does not remain a compliance matter. It alters operational constraints. These interactions occur at a specific point: *the asset.*

The asset is where systems, processes, data and obligations come together. It is where performance is realised and where failure occurs. Understanding this shift from categories to conditions is fundamental. It explains why governance that appears robust at a domain level can fail under stress. It explains why organisations are often surprised by the nature and impact of disruptions. It explains why accountability becomes contested when incidents occur.

To address these issues, it is necessary to examine two related but distinct phenomena:

1. **Risk convergence at the asset level** — where failure originates
2. **Failure propagation across ecosystems** — how failure spreads

Risk Convergence at the Asset (Micro View)

Where domains intersect - At the level of the asset, multiple domains interact simultaneously.

A power generation facility depends on physical equipment, control systems, digital platforms, regulatory approvals and supply chains. A rail network relies on signalling systems, rolling stock, operational processes, communications infrastructure and external service providers. A water utility integrates treatment processes, distribution networks, monitoring systems and public health obligations.

Each of these elements is governed separately. However, their interaction determines performance. Risk convergence occurs when events in one domain affect others in ways that are not fully anticipated or managed.

This is not a theoretical concept. It is observable in practice.

Consider a scenario in which a control system update introduces a configuration error. From a technical perspective, this is a software issue. From an operational perspective, it affects system performance. From a regulatory perspective, it may breach compliance requirements. From a commercial perspective, it disrupts service delivery.

These impacts are not sequential. They are simultaneous. *They converge at the asset.*

Why convergence is not governed effectively

Governance structures are not designed to manage this convergence. They reflect organisational design rather than system behaviour. Cybersecurity is typically managed by a dedicated function. Operational performance is overseen by operations. Compliance sits with legal or risk functions. Vendor management is handled by procurement.

Each function operates within its scope. Coordination mechanisms exist, but they are often informal or reactive. There is rarely a single point of accountability for how these domains combine to affect a specific asset. This creates a gap.

When risks interact, no one is responsible for managing the interaction. Each function addresses its component. The combined effect is not fully owned. This gap is particularly evident in the relationship between information technology (IT) and operational technology (OT). Historically, these domains were separate. IT supported administrative functions. OT controlled physical processes. As systems have become more integrated, this distinction has eroded.

Control systems are increasingly connected to corporate networks. Data flows between operational and business systems. Remote access enables greater flexibility. These changes create new dependencies. They also create new risks. Cyber incidents can now affect physical operations. Operational disruptions can expose cyber vulnerabilities. Regulatory requirements span both domains. Despite this integration, governance often remains separate.

Cybersecurity is treated as an IT issue. Process safety is treated as an operational issue. Compliance is managed independently. The convergence of these domains at the asset is not fully reflected in governance.

Case narrative — Pipeline disruption (US)

A widely reported incident involving a major fuel pipeline operator in the United States illustrates this dynamic. The initial event was a ransomware attack on the organisation's IT systems. From a traditional perspective, this was a cybersecurity issue. However, the impact extended beyond IT.

The operator made the decision to shut down pipeline operations. This decision was not driven by physical damage. It was driven by uncertainty. The organisation could not confidently determine whether operational systems had been affected. It could not ensure that billing, scheduling and safety processes were functioning correctly. It could not assess regulatory implications. The risk was not confined to cyber.

It had converged across domains. The decision to shut down operations reflected a lack of integrated visibility and accountability. No single party could assess the situation holistically. No single party had clear authority to manage the combined risk.

The result was a significant disruption to fuel supply across multiple states. The incident triggered regulatory scrutiny, public concern and financial impact.

Post-incident analysis highlighted the need for integrated cyber-physical governance, clearer accountability for asset-level resilience and improved visibility across systems.
(Sources: US Department of Homeland Security; CISA; US Senate reports)

The implications of convergence

The pipeline example is not unique. Similar patterns have been observed across sectors:

- Energy systems disconnect due to control system misalignment with grid requirements
- Transport networks experience cascading delays due to signalling and communications failures

- Water utilities revert to manual operations due to cyber or data issues

In each case, the initial event is domain specific. The impact is multi-domain. The failure occurs at the asset. Where accountability is fragmented, response is compromised. This has several implications.

1. First, risk cannot be fully understood or managed within functional silos.
2. Second, governance must reflect how systems behave, not how organisations are structured.
3. Third, accountability must be anchored at the asset level.

Without this shift, convergence will continue to expose governance weaknesses.

Failure Propagation Across Ecosystems (Macro View)

From asset failure to system disruption. While risk convergence explains where failure originates, it does not explain how failure spreads. In modern systems, assets are interconnected. A failure at one asset can propagate across multiple assets, organisations and sectors. This propagation is driven by dependencies.

Transport systems rely on shared platforms for ticketing and scheduling. Energy systems depend on interconnected networks and common control technologies. Digital platforms underpin multiple physical systems. These dependencies create efficiency. They also create vulnerability. When a failure occurs, its impact extends beyond the originating asset.

Why propagation is difficult to manage

Propagation is difficult to manage because accountability does not extend across the ecosystem. Each organisation is accountable for its own operations. Contracts define responsibilities between parties. Service level agreements set performance expectations. These mechanisms focus on local performance. They do not ensure system-level resilience.

When a failure propagates, each party responds within its scope. Coordination is required to manage the broader impact. This coordination is often ad hoc. There is rarely a designated entity with authority to manage system-level performance. This creates delays. It also creates conflict.

Parties may dispute responsibility for the failure. They may prioritise their own recovery over system recovery. They may lack visibility into the broader impact. The result is prolonged disruption.

Case narrative — Rail timetable disruption (UK)

A major rail timetable change in the United Kingdom provides a clear example. The introduction of a new timetable involved multiple stakeholders: infrastructure managers, train operating companies, rolling stock providers and timetable planners. Each had defined responsibilities. The timetable change exposed integration issues between these components. The result was widespread disruption across the network.

Trains were delayed or cancelled. Passengers experienced significant inconvenience. Public confidence was affected.

Investigations found that no single entity was accountable for system-level performance. Each party had met its individual obligations. The system as a whole failed. The absence of integrated accountability meant that issues were not identified or addressed in time. Recovery required coordinated action across multiple organisations. This took time.

The incident led to increased regulatory oversight and changes in governance arrangements, including stronger system operator roles. (Sources: UK National Audit Office; Transport Select Committee)

Ecosystem-level dependencies

The rail example highlights a broader issue. Modern systems are ecosystems. They consist of multiple assets, organisations and platforms. Value is created through their interaction. Governance frameworks, however, are typically designed for individual organisations. This creates a mismatch.

Dependencies across organisations are not always visible. They are not always owned. They are not always governed effectively. This is particularly evident in the role of digital platforms. Platforms are often treated as vendors. They provide services under contract. Their performance is measured against service levels.

In practice, they can become critical infrastructure. A failure in a platform can affect multiple assets and organisations simultaneously. If accountability for platform performance is not integrated into asset-level governance, this creates systemic risk.

Case narrative — Digital platform dependency (multi-sector)

Across multiple sectors, organisations have consolidated critical functions onto shared digital platforms. In energy, forecasting and control systems may rely on centralised platforms. In transport, ticketing and scheduling systems are often centralised. In logistics, coordination platforms manage flows across networks. These platforms create efficiency and visibility.

They also create concentration risk. When a platform experiences an outage or degradation, multiple assets are affected. If governance treats the platform as a vendor rather than a critical asset, accountability for its performance may be limited. This can lead to situations where:

- Platform providers meet contractual obligations but system performance deteriorates
- Organisations lack visibility into platform risks
- Recovery is delayed due to unclear responsibilities

Regulators are increasingly aware of this issue and are expanding their focus to include digital dependencies in critical infrastructure oversight. (Sources: ENISA; NIST; OECD)

Implications of propagation

Failure propagation has several implications for governance.

1. First, accountability must extend beyond organisational boundaries. It is not sufficient to manage risks within the organisation. Dependencies on external parties must be integrated into governance.
2. Second, system-level visibility is required. Organisations must understand how their assets interact with others. They must identify critical dependencies and potential points of failure.
3. Third, coordination mechanisms must be formalised. Ad hoc coordination is not sufficient in complex systems. Roles, responsibilities and processes for managing system-level events must be defined.
4. Fourth, regulators are likely to increase expectations. As failures become more visible and impactful, regulators will require organisations to demonstrate system-level resilience.

Integrating Micro and Macro Views

Risk convergence and failure propagation are distinct but related. Convergence explains where failure originates. Propagation explains how it spreads. Both are driven by the same underlying issue: fragmented accountability.

At the asset level, no single party owns the combined risk. At the ecosystem level, no single party owns the system. This creates a structural vulnerability. Addressing this vulnerability requires a shift in how accountability is defined and operationalised. It requires moving from:

- functional accountability to asset accountability
- organisational accountability to system accountability
- static definitions to dynamic execution

This shift is not straightforward. It challenges existing structures. It requires changes in roles, processes and incentives. It requires Boards and executives to engage with operational realities. However, it is necessary. Without it, the patterns described in this section will continue to produce governance failure.

Understanding where risk materialises and how failure propagates is only the first step. The next question is how to address it. The answer lies in accountability. Not accountability as defined in policies and contracts, but accountability as a mechanism that operates at the asset and across the system.

That is the focus of the next section.

Additional Cases

The dynamics of convergence and propagation are now visible across a wide range of sectors, often in organisations that appear well governed on paper.

Case 1 – Cloud outage and payment services (financial services, global)

A major retail bank migrated core customer channels and parts of its payment processing stack to a hyperscale cloud provider. Internally, cyber, technology, operations and third-party risk were managed through separate frameworks, each with its own reporting and assurance. When a regional cloud outage occurred, online banking, card authorisation and some internal systems became unavailable. The bank's incident response teams moved quickly within their domains, but no single executive had end-to-end accountability for the availability of customer payment services across on-premise, cloud and third-party platforms. Customers experienced prolonged service disruption, regulators demanded explanations, and the Board faced questions about resilience. The failure stemmed less from missing frameworks than from fragmented ownership of a converged, platform-dependent asset.

Case 2 – Port disruption from operational and cyber factors (logistics, OECD)

A container port experienced recurring delays and congestion following the introduction of a new terminal operating system and remote gate technologies. Operational performance metrics were tracked by operations, cyber controls by IT, and service-level agreements by procurement. After a series of cyber incidents affecting planning and gate systems, operations were repeatedly slowed or suspended. Each incident had multiple causes: software defects, cyber weaknesses, integration issues with trucking systems and workforce practices. No single party was accountable for the port as a critical asset that combined all of these elements. As a result, root causes were treated in isolation, and the pattern of disruption persisted. The Board eventually commissioned an external review, which identified the absence of integrated, asset-level governance for a cyber-physical port ecosystem as the primary issue.

Case 3 – Critical vendor platform disruption (multi-sector SaaS)

Several utilities and transport operators adopted a common SaaS platform for maintenance management and work scheduling. Each organisation treated the platform as a vendor subject to

standard procurement and IT risk processes. When the platform suffered a prolonged outage and data integrity issues, maintenance work across multiple organisations was disrupted. Safety inspections were delayed, and some assets had to be taken out of service as a precaution. Contracts, vendor performance reports and certification audits were all technically in order. However, the platform had become part of the critical asset stack without being recognised as such. No organisation had mapped the dependency between the platform and its own critical assets, and no regulator had clear oversight of the concentration risk. The incident illustrated how convergence and propagation can originate in shared digital platforms that sit between traditional risk categories.

Digital and cyber-physical assets in practice

The incidents described in this section are examples of digital and physical systems operating as a single asset, even when governance treats them as separate. A rail network is no longer just rolling stock and track; it is also signalling software, communications, data feeds and external platforms that together determine whether trains run safely and on time.

Thinking in terms of integrated digital-physical assets helps Boards see where risk actually materialises. At the level of a substation, a pipeline control station or a hospital theatre complex, performance depends on how equipment, control logic, network connectivity, identity and access controls, data and vendor platforms interact in real time. When governance allocates cyber, operational, regulatory and vendor risk to different owners, no one is accountable for that integrated behaviour. Convergence then appears as a surprise rather than a predictable feature of the system.

Recent guidance on operational technology and critical infrastructure risk management reflects this shift by requiring clearer inventories of critical systems, their dependencies and accountable owners. When organisations pair this with asset-centric monitoring – telemetry from both physical and digital components, integrated incident logs and service-level data – they gain the visibility required to manage convergence deliberately rather than reactively. Digital and cyber-physical assets become the practical unit through which enterprise resilience is governed, providing Boards with a clearer line of sight from risk categories to conditions of failure at the asset itself.

Section 3 - Accountability as the Mechanism

From Understanding Failure to Enabling Control

The preceding sections establish two critical points.

1. First, governance fails structurally when accountability is not anchored at the point where risk materialises.
2. Second, risk converges at the asset and propagates across interconnected systems.

Together, these observations explain why disruption occurs even in organisations with mature governance frameworks. They do not, on their own, provide a solution. The question that follows is practical:

What mechanism allows organisations to maintain control under these conditions?

The answer is accountability. Not accountability as it is commonly defined, through policies, contracts or reporting lines. But accountability as it must operate in practice: clear, enforceable and traceable ownership of asset performance under real conditions.

This section examines how accountability must be reframed and structured to enable enterprise resilience.

Reframing Accountability

From allocation to execution. In traditional governance, accountability is allocated. Contracts specify responsibilities, role descriptions define duties and frameworks assign ownership of risk categories. These allocations are necessary. They establish expectations and provide a basis for coordination. However, allocation on its own does not ensure execution. An individual or function may be assigned responsibility for a domain and discharge that responsibility diligently, yet the combined performance of the asset or service can still fall short. This becomes most obvious where risks converge across domains and where responsibility for the outcome is shared but not clearly owned.

An individual or function may be assigned responsibility for a particular domain. That responsibility may be exercised effectively within that domain. It does not guarantee that the combined performance of the system is managed. This distinction becomes critical where risks converge. When multiple domains interact, the outcome is determined by their interaction, not by the performance of any single domain. Accountability that is limited to individual domains cannot ensure system-level performance.

Execution requires a different form of accountability. It requires that responsibility be defined in relation to outcomes, not activities. It requires that ownership extend across domains. It requires that authority be aligned with responsibility.

In short, it requires accountability that operates at the level where performance is realised: the asset.

From shared responsibility to clear ownership. In complex environments, there is a natural tendency to emphasise shared responsibility. Multiple functions contribute to outcomes; collaboration is essential; no single role has complete control. While this is accurate, it can unintentionally dilute accountability. When responsibility is shared too broadly, each party reasonably assumes that others will address parts of the issue. Gaps emerge at the interfaces. This pattern is now visible in many incident and inquiry reports: no single executive can clearly state, “I own the performance and resilience of this asset or service end-to-end. Each party assumes that others will address aspects of the issue. Gaps emerge at the interfaces. This is particularly evident in cross-functional risks.

Cybersecurity may be responsible for protecting systems. Operations may be responsible for maintaining performance. Compliance may be responsible for regulatory adherence. Each has a role.

When an incident spans these domains, accountability becomes unclear. Who is responsible for ensuring that the asset continues to operate? Who has authority to make decisions that affect multiple domains? Who is accountable for the outcome?

Without clear answers, response is delayed and effectiveness is reduced. This does not imply that complexity can be eliminated. It implies that ownership must be clarified. Accountability must be assigned in a way that reflects how outcomes are produced.

The Asset as the Unit of Governance

Where accountability must reside. If failure occurs at the asset or at the level of an important business service, accountability must reside at that level. This principle is straightforward; its implications are significant. It aligns with emerging regulatory expectations that Boards identify critical operations or important business services, define tolerances for disruption and assign clear ownership for maintaining those services within tolerance through severe but plausible events.

It requires organisations to define their critical assets explicitly. These may be physical assets, such as plants, networks or facilities. They may be logical assets, such as platforms, data systems or service layers. They may be composite systems that combine multiple elements.

The definition of the asset is not purely technical. It reflects how value is created and how risk materialises. Once defined, each asset must have a clearly identified owner. This owner is accountable for the performance, resilience and recoverability of the asset across all relevant domains. This includes:

- operational performance
- cyber and data integrity
- regulatory compliance
- supplier and dependency management
- financial outcomes.

In practice, this means that for each critical asset or service, there is a named executive owner accountable for performance, resilience and recoverability across operational, technology, cyber, supplier and compliance domains, supported by clear delegation and evidence. The scope of accountability is broader than traditional role definitions. It reflects the integrated nature of the asset.

Challenges in defining asset ownership. Assigning asset-level accountability is not straightforward. Organisations are typically structured around functions or business units. Assets may span multiple functions. They may be supported by shared services. They may involve external partners. This creates tension.

Assigning accountability to a single individual may conflict with existing structures. It may require changes in reporting lines or decision rights. It may challenge established roles. There are also practical considerations. How granular should asset definitions be? Should accountability be assigned at the level of individual components, systems or services? How should accountability be aligned with legal and regulatory responsibilities?

These questions require careful consideration. However, the absence of clear asset-level accountability creates greater risk. Without it, performance issues persist without resolution. Responsibility remains diffuse. Governance becomes less effective. Similar tensions are emerging in critical infrastructure regulation, where responsible entities must identify each critical infrastructure

asset, adopt risk management programs and provide Board-approved assurance that risks to availability, integrity and reliability are being addressed

Case narrative — Substation performance (AU)

A portfolio of electricity substations in Australia provides an illustrative example. The organisation managed maintenance, operations, cybersecurity and vendor relationships centrally. Each function performed effectively within its scope. Performance metrics were met. Compliance requirements were satisfied. However, one substation consistently underperformed.

Outages occurred more frequently than expected. Maintenance issues persisted. Data anomalies were observed. These issues were known locally but did not trigger system-level attention. No single executive was accountable for the end-to-end performance of that substation. Maintenance teams addressed equipment issues. IT teams addressed data issues. Operations teams managed outages. Each acted within their domain. The combined effect was not owned.

Over time, performance deteriorated. The substation became a source of risk for the network.

When accountability was assigned to a specific asset owner, the situation changed. The owner had visibility across domains. They were able to prioritise actions, align resources and address underlying issues. Performance improved. The issue was not capability. It was accountability.
(Sources: Infrastructure Australia, 2021; Australian Energy Regulator reports)

The Single Thread of Accountability

Connecting Board to asset. Asset-level accountability must not exist in isolation. It must be connected to governance at all levels of the organisation. This connection is established through a single thread of accountability. The single thread is a traceable line from the Board to the asset. Put simply, the Single Thread of Accountability answers the Board's question: "*Who owns this asset or service, end-to-end, when things go wrong?*", while the accountability chain sets out how that ownership is supported in practice through roles, decision rights, reporting and escalation. It defines how responsibility flows and how decisions are made.

1. **At the top, the Board** sets expectations for performance and risk. These expectations must be translated into asset-level mandates.
2. **At the executive level**, responsibilities must be aligned with these mandates. Decision rights must be clear. Trade-offs must be managed.
3. **At the operational level**, actions must reflect these expectations. Performance must be monitored. Issues must be escalated.

The thread ensures that these elements are connected.

Why the thread breaks. In many organisations, this thread is implicit rather than explicit. Boards define expectations at a high level. Executives interpret these expectations. Operational teams implement them. The connections between these levels are not always clear. This creates gaps.

Board expectations may not be translated into specific requirements for assets. Executive decisions may not align with asset-level needs. Operational actions may not reflect strategic priorities. When issues arise, these gaps become apparent. Escalation paths may be unclear. Decision authority may be contested. Accountability may be disputed. The absence of a clear thread reduces the organisation's ability to respond effectively.

Case narrative — Rail line performance (EU)

A European rail network experienced persistent delays on a specific line. The causes were varied: infrastructure issues, rolling stock reliability, signalling performance and scheduling conflicts. Each issue was managed by different teams. No single individual was accountable for the end-to-end performance of the line. Performance reports were produced. Issues were discussed in committees. Actions were taken within domains. Delays continued.

When a single accountable executive was appointed for the line, the approach changed. The executive had authority to coordinate across domains. They were able to prioritise interventions, align resources and manage trade-offs. Performance improved.

The key change was not technical. It was the establishment of a single thread of accountability. (Sources: UK National Audit Office; European Court of Auditors reports)

The Accountability Chain

Structuring accountability. The single thread must be supported by a structured accountability chain. The chain defines how accountability is distributed across levels and how it is exercised. It typically includes:

- Board oversight
- Executive leadership
- Functional teams
- Asset owners
- Operational staff
- External partners.

Each level has a role. The chain ensures that these roles are aligned. It also ensures that accountability extends beyond organisational boundaries. In modern systems, suppliers and partners are integral to performance. Their roles must be incorporated into the chain.

Making the chain explicit. In many organisations, the accountability chain exists implicitly. Roles and responsibilities are defined. Relationships are understood. Coordination occurs through established processes. However, the chain is not always documented or tested. This creates risk.

Gaps may exist at interfaces. Responsibilities may be assumed rather than defined. External parties may not be fully integrated. Making the chain explicit addresses these issues. It involves:

- Defining roles and responsibilities for each asset
- Aligning performance measures and incentives
- Establishing clear escalation paths
- Integrating external parties into governance.

This does not eliminate complexity. It makes it manageable.

Case narrative — Energy interconnector (UK/EU)

A high-voltage interconnector linking energy systems across borders provides an example. The asset involves multiple stakeholders: asset owners, system operators, maintenance providers and regulators. Performance depends on coordination across these parties. In early operation, issues arose due to

unclear accountability. Maintenance decisions were not aligned with operational needs. Data sharing was limited. Regulatory expectations differed.

The absence of a clear accountability chain contributed to these issues. Subsequent governance reforms introduced clearer roles and responsibilities. Data sharing was improved. Coordination mechanisms were formalised. Performance stabilised. (Sources: Ofgem; European Network of Transmission System Operators)

Extending Accountability Beyond the Organisation

Ecosystem accountability. As discussed in Section 2, assets operate within ecosystems. Accountability must extend beyond the organisation. This requires a shift in perspective. External parties are not simply vendors. They are participants in the system. Their performance affects asset outcomes. Governance must reflect this.

This involves:

- Identifying critical dependencies
- Integrating external parties into accountability structures
- Aligning incentives and expectations.

This is not always straightforward. Contracts define relationships. They may not support integrated accountability. Incentives may be misaligned. Addressing these issues requires deliberate design.

Regulatory direction. Regulators are increasingly recognising the need for integrated accountability.

- In **Australia**, the Security of Critical Infrastructure (SOCI) Act and Critical Infrastructure Risk Management Program (CIRMP) require organisations to manage risks across domains for defined assets.
- In the **United Kingdom**, operational resilience frameworks emphasise the need to identify important business services and manage risks to their delivery.
- In the **European Union**, directives on network and information security (NIS2) extend requirements to supply chains and service providers.
- In the **United States**, agencies such as the Cybersecurity and Infrastructure Security Agency (CISA) emphasise integrated risk management for critical infrastructure.

These developments reflect a shift towards asset-level and system-level accountability. Organisations that adopt these approaches proactively are better positioned to meet regulatory expectations.

Additional Cases

The shift from allocated responsibility to executed accountability is visible whenever Boards examine why well-intentioned frameworks have not delivered the expected control.

Case 1 – Critical operations ownership under CPS 230 (financial services, Australia)

A large Australian financial institution prepared for APRA's CPS 230 by identifying its critical operations and mapping the processes, systems and third-party services that support them. Initially, accountability for these operations was distributed across business units, IT, operations and risk. Each function could demonstrate compliance with its own policies, but no single executive was accountable for the end-to-end resilience of each critical operation. In response, the Board endorsed a model that assigned an executive owner to each critical operation, with clear authority to make trade-offs across

technology, process, supplier and risk domains. Scenario testing then revealed control gaps that had not been visible in siloed reporting. By reframing accountability at the level of critical operations, the organisation could demonstrate a clearer line of sight between Board-approved tolerances, operational decisions and customer outcomes.

Case 2 – Rail line performance and asset ownership (transport, Europe)

A European rail operator had persistent punctuality and reliability issues on a key interurban line. Responsibility for performance was spread across infrastructure, rolling stock, timetable planning, maintenance and customer service. Each team met its internal targets. When disruption occurred, investigations produced long lists of contributing factors but no enduring change. After regulatory scrutiny and public pressure, the operator restructured accountability around specific rail corridors. A senior executive was appointed as corridor owner for the underperforming line, with explicit accountability for its end-to-end performance and resilience. This role cut across traditional functional boundaries and was supported by integrated data on asset condition, operations, incidents and customer impact. Within two years, punctuality and incident recovery times improved materially, and root-cause fixes became more systematic rather than episodic.

Case 3 – Critical infrastructure “responsible entity” obligations (multi-sector, Australia)

Following amendments to the Security of Critical Infrastructure Act and the introduction of critical infrastructure risk management program rules, owners and operators of designated assets were required to identify a responsible entity for each critical asset and have the Board approve an annual report on how material risks are being managed. Many organisations discovered that, while they could nominate a legal responsible entity, practical accountability for day-to-day resilience was fragmented across operations, IT, cyber, engineering and vendors. In response, some Boards created asset owner roles beneath the responsible entity, each with a clearly defined remit for a specific critical asset or cluster of assets. These roles became focal points for integrating risk management across domains, responding to incidents and providing the Board with coherent assurance on how each asset would perform under stress.

Assets as accountability anchors

In practice, many of the assets that matter most to Boards are now digital-physical hybrids. A payment service is not just an application; it is also the underlying infrastructure, data flows and external platforms that enable transactions. A modern substation is not just transformers and switchgear; it is also control systems, communications networks, identity and access mechanisms and vendor-managed software.

These integrated assets are where risk converges and where performance is determined. They are also where accountability is most likely to be fragmented if governance follows organisational charts rather than system behaviour. Cybersecurity functions may own controls; IT may own networks; operations may own processes; vendors may own components. Without a clearly identified owner for the integrated asset, no one has the authority or obligation to manage trade-offs across domains when conditions change or incidents occur.

Asset-level accountability supported by digital evidence changes this dynamic. By maintaining accurate inventories of critical systems and their dependencies, mapping which assets support which operations or services, and consolidating operational, cyber and vendor telemetry for each asset, organisations create a practical anchor for the Single Thread of Accountability. The asset owner can see how the asset is performing, how it behaves under stress and where risks are emerging. This allows Boards to

ask a simple question – "Who owns this asset, and what evidence do they have that it will stay within tolerance?" – and receive a specific, defensible answer rather than a collection of partial views.

Implications for Leadership

For Boards. Boards must recognise that accountability is the central mechanism of governance. They must ensure that:

- Critical assets are identified
- Accountability is clearly assigned
- Evidence of performance is available.

They must move beyond reviewing frameworks to verifying accountability.

For Executives. Executives must align roles, processes and incentives with asset-level accountability. They must:

- Clarify ownership
- Establish decision rights
- Integrate functions.

They must ensure that accountability can be exercised effectively.

For Operations. Operational teams must operate within a clear accountability structure. They must understand:

- Who is accountable
- How decisions are made
- How performance is measured.

They must be supported by systems and processes that enable effective execution.

Conclusion — Accountability as the Control Mechanism

The analysis in this section leads to a clear conclusion. Governance frameworks, policies and reporting are necessary. They are not sufficient. Control in modern systems is achieved through accountability. Specifically, through accountability that is:

- Anchored at the asset
- Connected through a single thread
- Structured through an accountability chain
- Extended across the ecosystem.

Where this form of accountability exists, organisations can manage risk convergence and failure propagation effectively. Where it does not, governance failure is inevitable. This is not a theoretical proposition. It is observable across sectors and jurisdictions.

The next section examines how this form of accountability is operationalised. It focuses on the operating model required to support enterprise resilience, including governance, decision-making and evidence.

Section 4 - Operating Model of Enterprise Resilience

From Accountability to Execution

The preceding sections establish that governance failure is a consequence of missing asset-level accountability, and that accountability must be anchored, connected and extended across systems. This raises a practical question. How is this form of accountability operationalised? Defining accountability is necessary. It is not sufficient.

To function under real conditions, accountability must be supported by an operating model. This model must enable individuals and organisations to:

- Understand asset performance in real time
- Make integrated decisions under pressure
- Verify that controls are effective
- Respond to failure and recover within defined thresholds.

Without this support, accountability becomes symbolic. It exists in documentation but cannot be exercised effectively. Enterprise resilience is therefore not just a governance construct. It is an operating model doctrine. It integrates governance, decision-making and evidence into a system that allows organisations to maintain control under dynamic conditions.

This section examines the key components of that model.

Defining Resilience as Performance

From compliance to outcomes. Resilience is often described in abstract terms. Organisations refer to resilience strategies, resilience frameworks and resilience capabilities. These concepts are useful, but they can obscure the practical reality. Resilience is not an attribute that can be declared. It is a characteristic that must be demonstrated.

In this book, resilience is defined in terms of performance – the ability of an organisation to continue to deliver critical outcomes within acceptable tolerances under stress. This is consistent with emerging operational resilience frameworks that require Boards to identify important business services or critical operations, set impact tolerances for disruption, and ensure those services remain within tolerance in severe but plausible scenarios.

- Maintain critical services within defined tolerances
- Respond effectively to disruption
- Recover operations within acceptable timeframes.

This definition shifts the focus from compliance to performance. Compliance confirms that requirements are met. Performance demonstrates that systems function under real conditions. This distinction is reflected in regulatory developments.

In the United Kingdom, the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) require firms to define “important business services” and set impact tolerances for disruption. These tolerances must be tested under severe but plausible scenarios (FCA/PRA, 2021).

In Australia, APRA CPS 230 requires entities to identify critical operations and ensure they can continue or recover within defined timeframes under disruption (APRA, 2023).

In the European Union, NIS2 extends obligations to ensure continuity of essential services, including through supply chain resilience (ENISA, 2022).

These frameworks emphasise outcomes. They require organisations to define what must be maintained and how performance will be verified.

Implications for asset-level accountability. Defining resilience as performance has direct implications for accountability. Asset owners must be accountable not only for normal operation, but for performance under stress. This requires clarity on several dimensions:

- What constitutes acceptable performance?
- What level of disruption is tolerable?
- How quickly must recovery occur?
- What dependencies must be maintained?

These parameters must be defined explicitly. They must be aligned with Board expectations and regulatory requirements. They must be measurable. Without this clarity, accountability cannot be exercised effectively.

Case narrative — Financial services resilience (UK)

The UK operational resilience regime provides a clear example. Firms were required to identify important business services and define impact tolerances. These tolerances were expressed in terms of maximum tolerable disruption. Firms then had to map resources supporting these services and test their ability to remain within tolerances under stress. This process revealed gaps.

Dependencies were not fully understood. Responsibilities were fragmented. Systems were not designed for recovery within required timeframes. Addressing these gaps required changes in governance, operations and technology. The key shift was from demonstrating compliance to demonstrating performance. (Sources: FCA/PRA Operational Resilience Policy, 2021; Bank of England reports)

The Role of Evidence

From reporting to traceability. Governance relies on information. Boards and executives require visibility into performance. They need to understand whether assets are operating within defined parameters and whether risks are being managed. Traditionally, this visibility is provided through reporting. Reports summarise performance. They highlight issues. They provide assurance that controls are in place. While necessary, reports have limitations.

They are typically periodic. They aggregate information. They rely on interpretation. They do not provide direct evidence of how assets are performing in real time. Enterprise resilience requires a different approach. It requires traceability. Traceability connects decisions, data and outcomes. It allows organisations to:

- Understand how assets are performing at any point in time
- Identify deviations from expected performance
- Trace issues back to their source
- Verify that corrective actions are effective.

This is often described as a “digital thread”. The term is useful, but it can be misleading. The digital thread is not a technology solution. It is a concept that describes the flow of information across the asset lifecycle. Technology enables this flow. It does not define it.

Technology as an enabler, not a solution. There is a tendency to view digital solutions as the answer to resilience challenges. Investments are made in data platforms, analytics tools and digital twins. These

investments can be valuable. However, without clear accountability, they do not resolve underlying issues. Technology can:

- Collect and process data
- Provide visibility into system behaviour
- Support decision-making.

It cannot:

- Define ownership
- resolve conflicts in responsibility
- ensure that decisions are made.

Without accountability, increased data can increase complexity. Organisations may have more information but less clarity. The role of technology is therefore specific:

- It enables evidence.
- It supports traceability.
- It allows accountability to be exercised effectively.

In practice, this means mapping the people, processes, technology, data and facilities that support each critical service or asset, monitoring how they behave under normal and stressed conditions, and using scenario testing to validate whether the organisation can remain within its defined tolerances

Case narrative — Asset monitoring (Australia)

A transport operator implemented advanced monitoring systems across its network. Sensors provided real-time data on asset condition. Analytics identified anomalies. Dashboards presented performance metrics. From a technical perspective, the system was effective. However, performance issues persisted. Data was available. Decisions were not.

Responsibility for interpreting data and taking action was unclear. Different teams accessed the same information but prioritised actions differently. When accountability was clarified, the value of the system increased. Asset owners were given responsibility for performance. Data was aligned to their needs. Decision rights were defined.

The system enabled accountability. It did not create it. (Sources: Infrastructure Australia; transport operator case studies)

Integrated Decision-Making

From siloed decisions to convergence. When risks converge, decisions must also converge. This is one of the most challenging aspects of enterprise resilience. Organisations are structured to support specialised decision-making. Functions develop expertise. They optimise performance within their domains.

This specialisation is valuable. It becomes problematic when decisions require integration across domains. For example:

- A cybersecurity control may affect operational performance
- A maintenance decision may impact regulatory compliance
- A cost reduction initiative may increase system vulnerability.

These trade-offs must be managed explicitly. In many organisations, they are not. Decisions are made within functions. Coordination occurs through committees or escalation. This can be slow and reactive. Enterprise resilience requires integrated decision-making. This involves:

- Bringing relevant stakeholders together
- Providing a shared view of the asset
- Defining clear decision authority
- Making trade-offs explicit.

Decision rights and authority. Integrated decision-making requires clarity on authority. Who has the right to make decisions that affect multiple domains? Who is accountable for the outcome? These questions must be answered. In the absence of clear authority, decisions are delayed. Issues are escalated unnecessarily. Responsibility is diffused.

Assigning authority to asset owners is a key element. Asset owners must have the ability to:

- Prioritise actions across domains
- Allocate resources
- Make trade-offs.

This does not eliminate the role of functions. It aligns their contributions to asset-level outcomes.

Case narrative — Grid management (Europe)

A European transmission system operator faced challenges in managing grid stability. Increasing integration of renewable energy introduced variability. Control systems, market mechanisms and operational processes had to be aligned. Decisions affecting grid stability involved multiple functions: operations, market operations, IT and regulatory teams.

Initial governance structures did not support integrated decision-making. Issues were escalated across functions. Responses were delayed. The operator introduced integrated control centres and defined clear decision authority for system operators.

These operators had visibility across domains and authority to act. Grid stability improved. The change was not primarily technical. It was organisational. (Sources: ENTSO-E reports; European Commission energy studies)

Digital and cyber-physical assets in the operating model

The operating model of enterprise resilience relies on digital and cyber-physical assets to make resilience visible and manageable. A transmission corridor with dynamic line rating sensors, micro-weather monitoring and geospatial analytics is not just steel and conductors; it is a data-rich asset capable of telling operators how close it is to its limits and how it will behave under changing conditions. A production line instrumented with industrial sensors and connected to a digital twin can be monitored, stress-tested and reconfigured before failures occur.

These capabilities turn the abstract elements of the operating model – accountability, integrated decision-making and continuous assurance – into daily practice. Asset owners and service owners can see, often in near real time, how their assets are performing against resilience expectations, which dependencies are under strain and how different interventions would affect outcomes. Rather than relying solely on lagging indicators such as incidents or audit findings, Boards and executives receive leading indicators drawn from the behaviour of digital and cyber-physical assets themselves.

Digital twins provide a good illustration. When combined with accurate data from sensors, control systems and external sources, a twin can simulate how an asset or system will respond to different shocks, support decisions during incidents and capture lessons afterwards. For Boards, the value is not the technology in isolation but the fact that it enables clearer answers to practical questions: Which assets are most exposed? What is our current resilience posture? How confident are we that we can stay within our stated tolerances if specific scenarios occur? Embedding these digital and cyber-physical capabilities into the operating model allows enterprise resilience to be governed with the same discipline as financial performance.

Continuous Assurance

From periodic review to real-time verification. Traditional assurance operates on cycles. Audits are conducted periodically. Controls are reviewed. Compliance is assessed. This approach is appropriate for stable systems. In dynamic environments, it is insufficient.

Risks evolve continuously. System behaviour changes in real time. Enterprise resilience requires continuous assurance. This involves:

- Monitoring asset performance continuously
- Identifying deviations from expected behaviour
- Verifying that controls are effective
- Providing real-time visibility to decision-makers.

Continuous assurance does not replace traditional assurance. It complements it. It ensures that governance reflects current conditions.

Challenges in implementation. Implementing continuous assurance presents challenges. Data must be available and reliable. Systems must be integrated. Metrics must be defined. More importantly, accountability must be clear.

Without accountability, continuous assurance can generate information without action. Alerts may be triggered. Reports may be produced. Decisions may not be made. This reinforces the central role of accountability. Continuous assurance enables accountability. It does not substitute for it. Importantly, Regulators and investors increasingly expect Boards to receive forward-looking assurance on resilience – trends, leading indicators and scenario outcomes – rather than relying solely on annual attestation cycles.

Case narrative — Industrial control systems (US/EU)

Industrial organisations have increasingly adopted continuous monitoring of control systems. Sensors and analytics provide visibility into system behaviour. Anomalies are detected early. In organisations where accountability is clear, this leads to rapid response and improved performance. In organisations where accountability is fragmented, issues persist.

Alerts are generated but not resolved. Responsibility is unclear. Action is delayed. The difference lies not in technology, but in governance. (Sources: NIST; ENISA industrial control system studies)

Designing for Failure

Accepting failure as inevitable. Traditional design approaches focus on preventing failure. Systems are engineered to operate within defined parameters. Controls are implemented to reduce risk. These approaches remain important. However, in complex systems, failure cannot be eliminated.

Unexpected interactions, external events and human factors introduce uncertainty. Enterprise resilience requires acknowledging this reality. Systems must be designed to:

- Operate in degraded modes
- Contain failures
- Recover effectively.

Design principles. Designing for failure involves several principles:

- Redundancy — ensuring alternative paths or systems are available
- Isolation — limiting the spread of failure
- Recovery — enabling rapid restoration of services
- Adaptability — allowing systems to adjust to changing conditions.

These principles must be applied at the asset level. They must be aligned with accountability. Asset owners must be responsible for ensuring that these capabilities exist and are effective. Cyber Physical System/s, Digital Twins and simulation techniques now allow organisations to rehearse failures in a controlled way, exploring how assets and ecosystems respond to different shocks before they occur in the real world.

No other structural changes are needed; Section 4 already naturally leads into an operating model consistent with CPS 230, FCA/PRA operational resilience and DORA-style expectations.

Case narrative — Energy system resilience (Australia)

The increasing penetration of renewable energy has introduced new challenges in maintaining grid stability. Variability in generation requires systems to respond dynamically. Operators have introduced mechanisms such as:

- Fast frequency response
- Battery storage
- Demand management.

These measures are designed to manage failure conditions. Their effectiveness depends on coordination across assets and systems. Clear accountability for system performance is essential.
(Sources: Australian Energy Market Operator reports; AER studies)

Embedding Resilience in Decisions

From afterthought to design criterion. Resilience is often considered after systems are designed. This approach is insufficient. Decisions made during design, procurement and investment shape system behaviour. If resilience is not considered at these stages, vulnerabilities are embedded.

Embedding resilience requires:

- Incorporating resilience criteria into decision-making
- Evaluating trade-offs between cost, performance and resilience
- Aligning incentives with long-term outcomes.

Capital allocation. Capital allocation decisions are particularly important. Investments in resilience may increase upfront costs. They can reduce long-term risk. These trade-offs must be assessed explicitly. Boards and executives must consider the:

- Cost of failure

- Likelihood of disruption
- Impact on stakeholders.

This requires a shift in perspective. Resilience is not a cost. It is an investment in performance.

Case narrative — Infrastructure investment (UK/AU)

Infrastructure investment decisions often prioritise cost and schedule. Resilience considerations may be secondary. Where resilience is incorporated, projects may include:

- Enhanced redundancy
- Improved monitoring systems
- Stronger integration across components.

These investments can reduce lifecycle costs and improve performance. However, they require justification. Linking resilience to financial outcomes is critical. (Sources: Infrastructure Australia; UK Infrastructure Commission)

Integrating the Operating Model. The components described in this section are interdependent. Defining resilience as performance sets expectations. Evidence provides visibility. Integrated decision-making enables action. Continuous assurance verifies effectiveness. Designing for failure enhances capability. Embedding resilience in decisions ensures sustainability.

Together, they form an operating model. This model enables accountability to be exercised effectively. It allows organisations to maintain control under dynamic conditions.

Additional Cases

The operating model of enterprise resilience becomes clearest when Boards see how integrated governance, data and decision-making have changed outcomes in practice.

Case 1 – Operational resilience implementation (financial services, UK)

A UK-based financial institution responded to the joint FCA, PRA and Bank of England operational resilience regime by identifying a set of important business services and setting time-based impact tolerances for each. Initial mapping exercises exposed that technology, operations and third-party providers all claimed responsibility for aspects of service performance, but no one had end-to-end visibility. The firm established service owners for each important business service, supported by integrated dashboards showing service health, incidents, customer impact and dependence on internal and external systems. Scenario testing against impact tolerances revealed gaps in manual workarounds, communication protocols and third-party arrangements. The Board began to receive regular reporting not just on incidents, but on the organisation's ability to remain within tolerances under severe but plausible scenarios. Resilience shifted from an abstract risk concept to a measurable operating outcome for which executives were accountable.

Case 2 – System operator integrated decision-making (energy, Europe)

A European transmission system operator faced increasing variability from renewable generation and more frequent extreme weather events. Historically, control room decisions, maintenance planning and market operations were managed through separate processes with limited shared data. The operator invested in an integrated decision-support platform that combined SCADA data, weather forecasts, asset condition information and market positions. This platform enabled operators to see how different interventions – redispatch, line ratings, maintenance deferrals or emergency actions – would affect system security, customer impact and financial exposures in real time. Governance

arrangements were updated so that the executive responsible for system operations was explicitly accountable for both reliability and resilience performance metrics. As a result, the operator could demonstrate to regulators that it was actively managing the system to remain within defined security and resilience parameters, supported by evidence from the integrated platform.

Case 3 – Continuous assurance for industrial control systems (manufacturing, global)

A global manufacturing group relied on a portfolio of industrial control systems (ICS) across multiple plants. Assurance had traditionally been provided through periodic audits and point-in-time penetration tests. After several sector-wide cyber incidents, the Board requested more frequent insight into ICS resilience. The company implemented continuous monitoring for key ICS assets, including configuration drift, network segmentation, access patterns and control system anomalies, with dashboards aligned to a small set of resilience KPIs such as mean time to detect, mean time to recover and adherence to defined safe-state criteria. Plant managers were accountable for asset-level resilience metrics and reported regularly to a cross-functional resilience committee. Over time, the company reduced the window between the emergence of a vulnerability and its remediation and could evidence to regulators and insurers that resilience was being managed as an ongoing operating activity rather than an annual audit event

Conclusion — From Model to Outcome

Enterprise resilience is not achieved through a single initiative. It is the result of aligning governance, operations and evidence around asset-level accountability. Where this alignment exists:

- Risks are understood in context
- Decisions are made effectively
- Performance is maintained under stress
- Recovery is efficient.

Where it does not:

- Governance remains theoretical
- Accountability is fragmented
- Failure is inevitable.

The next section examines the implications of this model for financial performance, strategy and Board oversight. It focuses on how enterprise resilience influences value, risk and long-term sustainability.

Section 5 - Financial, Strategic & Board Implications

From Operating Model to Enterprise Value

The previous sections establish a clear proposition.

Investors, lenders and rating agencies increasingly treat operational and cyber resilience as financially material, assessing how governance, risk management and technology capabilities affect an entity's ability to withstand shocks and continue servicing obligations. Governance fails when accountability is not anchored at the asset. Risk converges at the asset and propagates across systems. Enterprise resilience is achieved through an operating model that enables accountability to be exercised effectively. The remaining question is direct.

Why does this matter at the level of enterprise value, strategy and Board oversight?

The answer is equally direct. Because governance quality is not a compliance attribute. It is a determinant of financial performance, cost of capital and long-term sustainability. In asset-intensive environments, the relationship between governance and value is often indirect and delayed. It is therefore underestimated.

However, when examined systematically, the connection becomes clear. Governance failure manifests as financial loss. Resilience manifests as financial advantage.

This section examines that relationship.

The Cost of Governance Failure

From operational disruption to financial impact. When governance fails, the immediate impact is operational. Systems do not perform as expected. Services are disrupted. Recovery requires intervention. These operational impacts translate directly into financial outcomes. Delays in transport systems reduce revenue and increase costs. Outages in energy systems affect generation, distribution and pricing. Failures in critical infrastructure require remediation, often under time pressure and regulatory scrutiny. These effects are measurable. They include:

- Direct revenue loss
- Increased operating costs
- Capital expenditure for remediation
- Penalties and compensation.

These costs are often attributed to specific incidents.

In practice, they reflect underlying governance weaknesses. Where accountability is fragmented, issues persist. They recur. They escalate. The cumulative financial impact can be significant.

Disputes and value leakage. In multi-party environments, governance failure often leads to disputes. Contracts allocate risk. When failures occur, parties seek to determine responsibility. Where accountability is unclear, disputes are prolonged. Each party may argue that it has met its obligations. The combined system has failed. This leads to:

- Delayed resolution
- Legal costs
- Strained relationships
- Reduced efficiency.

Value is lost not only through the failure itself, but through the process of resolving it. This value leakage is rarely captured in standard financial metrics. It is nonetheless material. Studies of infrastructure and PPP disputes repeatedly link project failure and early termination to weaknesses in governance and accountability, including unclear decision rights, unbalanced risk allocation and ineffective dispute resolution, rather than purely technical causes.

Case narrative — Infrastructure disputes (global)

Major infrastructure projects frequently experience disputes related to performance and delivery. In many cases, the underlying issue is not the absence of contractual provisions. It is the misalignment between contractual accountability and operational reality. Projects involving multiple contractors, technology providers and operators often encounter issues at interfaces.

When performance falls short, responsibility is contested. Resolution requires negotiation, arbitration or litigation. These processes consume time and resources. They also divert attention from operational improvement.

Studies by the World Bank and OECD highlight the prevalence of such disputes and their impact on project outcomes (World Bank PPP reports; OECD infrastructure studies).

The common factor is fragmented accountability.

Regulatory and compliance costs. Regulatory consequences add to the financial impact. When systems fail, regulators assess whether organisations have met their obligations. Where accountability is unclear or ineffective, regulatory intervention increases. This may include:

- Fines and penalties
- Additional reporting requirements
- Mandated changes to operations
- Increased oversight.

These measures impose costs. They also affect flexibility. Organisations may be required to allocate resources to compliance rather than improvement. Over time, this can reduce competitiveness.

Reputational impact and market response. Reputational consequences are less immediate but often more enduring.

Disruptions in critical infrastructure attract public attention. They affect customers, communities and stakeholders. Loss of trust can lead to:

- Reduced demand
- Increased scrutiny
- Political pressure.

In capital markets, reputational issues can affect valuation. Investors assess governance quality as part of risk evaluation. Repeated failures signal underlying weaknesses. This can increase perceived risk and affect investment decisions.

Consumer price pressure. In regulated sectors, the financial consequences of governance failure are not confined to organisations. They are often transferred to consumers. This occurs through several mechanisms:

- **Cost pass-through** — regulated entities may recover costs through tariffs
- **Increased cost of capital** — higher risk leads to higher financing costs, reflected in pricing

- **Recovery pricing** — costs of remediation are incorporated into future charges.

The result is higher prices or reduced service quality. This creates a direct link between governance and societal outcomes. It also increases regulatory sensitivity. Regulators are under pressure to protect consumers. They respond by increasing oversight.

This reinforces the cycle.

Resilience as a Strategic Lever

From risk mitigation to value creation. While governance failure imposes costs, enterprise resilience creates value. Organisations that can demonstrate resilience are better positioned to:

- Maintain performance under stress
- Recover quickly from disruption
- Manage dependencies effectively.

Organisations that can demonstrate credible resilience increasingly enjoy advantages in regulatory negotiations, customer retention and crisis-driven market share shifts, particularly in sectors where outages or incidents attract intense scrutiny.

Cost of capital and investor confidence. Investors assess risk when allocating capital. Organisations with strong resilience profiles are perceived as lower risk. This can result in:

- Lower cost of capital
- Improved access to financing
- Higher valuation multiples.

Conversely, organisations with weak governance and repeated failures may face higher financing costs. This relationship is increasingly recognised.

Institutional investors, including infrastructure funds and pension funds, are incorporating resilience and governance into their assessments (BlackRock infrastructure insights; IMF reports on infrastructure investment).

Operational efficiency and lifecycle performance. Resilience also affects operational efficiency. Assets that are well-managed and resilient:

- Experience fewer disruptions
- Require less reactive maintenance
- Operate more predictably.

This improves lifecycle performance. Costs are reduced. Revenue is stabilised. Planning is more effective. These benefits accumulate over time. They may not be immediately visible in financial statements. They are nonetheless significant.

Regulatory relationships. Organisations that demonstrate effective governance and resilience often benefit from stronger relationships with regulators. Regulators are more likely to:

- Approve investments
- Allow flexibility in operations
- Adopt risk-based approaches.

This can reduce compliance burden and improve efficiency. In contrast, organisations with governance failures may face increased scrutiny and prescriptive requirements.

Case narrative — Energy network performance (UK/AU)

Energy network operators in the UK and Australia are subject to performance-based regulation. Regulators assess reliability, service quality and efficiency. Operators that perform well may receive incentives, including higher allowed returns. Operators that perform poorly may face penalties. This creates a direct link between operational performance and financial outcomes.

Organisations that invest in resilience and asset-level accountability are better positioned to achieve favourable outcomes. (Sources: Ofgem RIIO framework; Australian Energy Regulator reports)

Contracting for Resilience

Limitations of traditional contracts. Contracts are a primary tool for allocating risk in infrastructure projects. They define responsibilities, performance requirements and incentives. However, traditional contracts have limitations. They are designed based on assumptions about system behaviour. They define responsibilities within scopes. They do not easily accommodate dynamic interactions across domains and organisations.

This creates gaps. Performance issues that span multiple scopes may not be fully addressed. Responsibilities may be unclear.

Towards dynamic accountability. Contracting for resilience requires a different approach. This involves:

- Recognising the integrated nature of assets
- Aligning incentives with system-level performance
- Incorporating flexibility to address changing conditions.

This does not imply abandoning contracts. It implies enhancing them. Contracts can include:

- Shared performance metrics
- Mechanisms for collaboration
- Provisions for data sharing
- Joint governance structures.

These elements support integrated accountability. International PPP guidance now emphasises governance, transparency and dispute-avoidance mechanisms as central to protecting long-term value, not just price and risk transfer at financial close

Case narrative — Public-private partnerships

Public-private partnerships (PPPs) provide examples of both strengths and limitations. PPPs often include detailed contractual arrangements and risk allocation mechanisms. They can achieve high levels of performance where incentives are aligned.

However, they can also experience challenges where system behaviour deviates from assumptions. Interface risks, technology changes and external factors can create situations not fully addressed by contracts. Addressing these issues requires collaboration beyond contractual provisions.
(Sources: Yescombe, PPP frameworks; World Bank PPP guidance)

Data, Platforms and Concentration Risk

Digital dependency as systemic risk. Supervisors and standard-setting bodies are increasingly attentive to concentration in critical service providers and shared platforms, including cloud, data and market infrastructure and expect Boards to understand and govern these dependencies explicitly.

Modern infrastructure systems increasingly depend on digital platforms. These platforms provide critical functions, including control, coordination and analytics. They enable efficiency and innovation. They also create concentration risk. When multiple assets depend on the same platform, a failure in that platform can have widespread impact.

Governance implications. Managing digital dependency requires:

- Identifying critical platforms
- Understanding their role in asset performance
- Integrating them into accountability structures.

Treating platforms as vendors is insufficient. They must be considered as part of the system. This requires:

- Visibility into platform performance
- Alignment of incentives
- Contingency planning.

Regulatory perspective. Regulators are increasingly focused on digital resilience.

- **In the EU**, the Digital Operational Resilience Act (DORA) addresses risks related to ICT providers.
- **In the US**, CISA emphasises the importance of managing supply chain and platform risks.
- **In Australia**, SOCI and CIRMP frameworks include digital dependencies.

These developments reflect recognition of the importance of digital infrastructure.

Digital and cyber-physical assets in financial and Board oversight

For Boards, the financial and strategic implications of resilience ultimately depend on the quality of evidence they receive about how critical assets, services and contracts are performing in practice. Increasingly, that evidence is generated by digital and cyber-physical assets themselves: sensors on infrastructure, logs from platforms, digital twins of projects and secure audit trails embedded in contracts.

When asset owners and service owners can provide Board-readable views of downtime cost, incident trends, dependency risks and control effectiveness at the level of specific assets or services, resilience moves from narrative to quantifiable exposure. Tools such as downtime cost models, ROSI/ALE calculations and risk-adjusted portfolio views rely on underlying digital data about how assets behave and how controls perform. This allows Directors to weigh resilience investments against other capital allocation decisions using a consistent financial lens, rather than treating resilience as a vague insurance policy.

In public-private partnerships and other long-term contracts, digital evidence can also become a strategic asset. Secure, tamper-resistant audit trails – whether through well-governed data platforms, permissioned blockchain or other mechanisms – provide all parties with a shared record of performance, payments, environmental impacts and community benefits over time. For Boards, these capabilities reduce information asymmetry, support earlier detection of emerging risks and strengthen

their ability to demonstrate stewardship to regulators, investors and communities. In this way, digital and cyber-physical assets are not only operational enablers but key components of financial discipline and fiduciary oversight in enterprise resilience.

Diagnosis as the Entry Point

Understanding the current state. Implementing enterprise resilience requires understanding current capability. Diagnosis is the starting point. This involves:

- Identifying critical assets
- Mapping dependencies
- Assessing accountability structures
- Evaluating performance under stress.

Diagnosis should focus on reality, not perception. It should examine how systems operate, not how they are intended to operate.

Common findings. Across organisations, diagnosis often reveals:

- Unclear asset ownership
- Fragmented accountability
- Limited visibility of dependencies
- Reliance on periodic reporting
- Insufficient scenario testing.

These findings are consistent across sectors. They reflect structural issues rather than isolated problems.

Additional cases

The financial and strategic consequences of resilience and governance choices are most evident when Boards examine where value has been lost or protected in practice.

Case 1 – PPP road project financial failure (transport, global)

An international toll road PPP reached financial close on the basis of optimistic demand forecasts and rigid contractual terms. Governance structures were formally compliant and multiple committees existed, but decision-making authority and accountability for asset performance were fragmented between the public authority, project company, lenders and operators. When actual traffic volumes fell short and community opposition to tolls grew, the project's ability to generate expected returns collapsed. Attempts to renegotiate terms were hampered by unclear escalation pathways and misaligned incentives. The project eventually failed financially, with losses for private investors and reputational damage for government. Post-project reviews highlighted weak governance, diffuse accountability and inadequate mechanisms for adapting the contract and operating model as key lessons.

Case 2 – Cyber resilience and financial stability expectations (financial sector, global)

Regulators and international bodies now treat severe cyber incidents as a financial stability risk. A number of recent thematic reviews and stress tests have examined how banks and market infrastructures would withstand disruptive cyber events and continue critical functions. Institutions able to demonstrate robust governance of cyber and operational resilience – including clear

accountability for critical operations, tested response plans and investment in detection and recovery capabilities – are better positioned in supervisory dialogues and may benefit from more favourable assessments of their risk profile. Conversely, entities with weak governance, opaque dependencies and under-investment in resilience face greater supervisory pressure, higher remediation costs and potentially higher capital and funding costs over time.

Case 3 – Digital evidence and trust in PPP benefit distribution (renewable energy, Europe)

A European renewable energy developer committed to sharing a portion of project revenues with local communities in exchange for hosting infrastructure. Early projects relied on traditional reporting and manual processes to track benefit payments. Over time, communities questioned whether commitments were being honoured in full. In later projects, the developer moved to a more transparent model, using digital platforms and, in one case, distributed ledger technology to record energy output, calculate community entitlements and automate payments. Communities and regulators could access near real-time evidence of flows, and the audit trail was tamper-resistant. This shift reduced disputes, strengthened social licence and improved project bankability by giving lenders greater confidence that community arrangements would be managed transparently over the life of the asset.

Board Oversight and Responsibility

From frameworks to evidence. Boards play a critical role in governance. To fulfil this role effectively, Boards must adapt their approach. They must move from reviewing frameworks to verifying accountability. This requires:

- Focusing on critical assets
- Requesting evidence of performance
- Challenging assumptions
- Understanding dependencies.

Key questions for Boards. Boards should ask:

- Who is accountable for each critical asset?
- What evidence demonstrates its performance?
- What are the key dependencies?
- How is resilience tested?

These questions shift the focus from compliance to performance.

Case narrative — Board transformation (Australia)

An Australian infrastructure organisation undertook a review of its governance approach. The Board shifted its focus from high-level reporting to asset-level performance. Deep dives were conducted on critical assets. Accountability was clarified. Evidence was reviewed. This led to:

- Improved visibility
- Clearer decision-making
- Enhanced performance.

The change was driven by Board engagement. (Sources: AICD governance studies; Infrastructure Australia)

From Governance to Stewardship

Expanding the role of Boards. Boards are increasingly expected to act as stewards of critical systems. This extends beyond compliance. It includes:

- Ensuring long-term performance
- Managing societal impact
- Maintaining trust.

In asset-intensive sectors, this responsibility is significant. Failure can have wide-reaching consequences.

Aligning governance with stewardship. Aligning governance with stewardship requires:

- Long-term perspective
- Integration of financial and non-financial factors
- Engagement with stakeholders.

Enterprise resilience supports this alignment. It provides a framework for managing complexity and uncertainty.

Conclusion — Linking Accountability to Value. The analysis in this section reinforces a central conclusion. Governance quality is a determinant of financial performance and strategic position. Where accountability is clear and operationalised:

- Performance is more stable
- Risks are managed effectively
- Costs are reduced
- Value is enhanced.

Where accountability is fragmented:

- Disruption occurs
- Costs increase
- Trust is eroded
- Value is diminished.

The relationship is direct. Governance failure is a financial and operational outcome of missing asset-level accountability.

This is not a theoretical insight.

It is observable across sectors and jurisdictions. It has implications for Boards, executives and stakeholders.

The final section brings these insights together and sets out the implications for organisations seeking to operate effectively in complex environments.

Conclusion - From Governance to Control

The argument developed across this book is straightforward, but its implications are significant.

Governance, as it is commonly practised, is no longer sufficient for asset-intensive organisations operating in dynamic, interconnected environments. It provides structure, defines intent and establishes expectations. It does not, on its own, ensure control. Control is achieved through accountability.

Specifically, through accountability that is anchored at the asset, connected across the organisation and supported by evidence of performance under real conditions. This distinction explains why organisations with mature governance frameworks continue to experience disruption, and why those disruptions often follow similar patterns.

- Risk is identified but not integrated.
- Responsibilities are defined but not operationalised.
- Performance is reported but not evidenced.

When conditions change, these gaps are exposed.

Revisiting the Core Proposition - The central proposition of this book can be restated in practical terms:

- Risk converges at the asset
- Failure propagates across systems
- Accountability is often fragmented
- Governance therefore fails.

The consequence is not limited to isolated incidents. It is structural.

Where accountability is not clearly defined and enforceable at the asset level, organisations operate with latent vulnerability. This vulnerability may remain hidden under stable conditions. It becomes visible under stress. When it does, the impact is immediate.

- Operations are disrupted.
- Costs increase.
- Decisions are delayed.
- Responsibility is contested.

The organisation discovers that while governance exists, it does not operate where it matters. This leads to the central conclusion:

Governance failure is a financial and operational outcome of missing asset-level accountability.

This is not a theoretical claim. It is supported by repeated observation across infrastructure, energy, transport and critical services.

Why This Matters Now

The relevance of this conclusion is increasing. Three trends are reshaping the operating environment.

System complexity is increasing. Assets are more interconnected than at any point in the past. Digital platforms underpin physical operations. Supply chains are global and dynamic. Dependencies extend beyond organisational boundaries.

This complexity increases efficiency. It also increases exposure.

Small disruptions can have wide-reaching effects. Interactions between domains create new forms of risk. Traditional governance frameworks, designed for more stable systems, struggle to accommodate this complexity.

Expectations are rising. Regulators, investors and stakeholders expect higher levels of performance and transparency. Regulators are moving toward asset-level accountability and resilience requirements. Investors are incorporating governance and resilience into risk assessments. Communities expect reliable services and rapid recovery from disruption.

These expectations are not optional. They reflect the essential nature of the systems involved. Organisations must demonstrate that they can operate effectively under stress.

Consequences are more visible. Failures in critical systems are increasingly visible. They attract media attention. They affect large numbers of people. They have political implications. This visibility amplifies consequences. Reputational damage occurs quickly. Regulatory responses are more immediate. Financial impacts are more pronounced.

In regulated environments, these impacts are often transferred to consumers. This creates a direct link between governance and societal outcomes.

What Must Change

Addressing these challenges requires a shift in how governance is understood and applied. This shift has several dimensions:

1. **From structure to accountability.** Governance must move beyond defining roles and responsibilities. It must ensure that accountability exists where performance is realised. This means identifying critical assets and assigning clear ownership for their performance across domains.
   Many of these shifts are already visible in emerging regulatory frameworks for operational resilience and critical infrastructure, but implementation remains uneven.
2. **From domains to systems.** Risk management must move beyond domain-based approaches. It must reflect how risks interact at the asset and across systems. This requires integration of perspectives and coordination of actions.
   The challenge for Boards is to move from formal alignment to operational reality at the level of specific assets and services
3. **From reporting to evidence.** Boards and executives must rely on evidence of performance, not only on summaries. This requires traceability from decisions to outcomes and visibility into asset behaviour in real time.
   This does not replace existing governance artefacts; it reframes them. Policies, frameworks and reports become the scaffolding around evidence drawn from the behaviour of assets, systems and services, rather than substitutes for that evidence.
4. **From periodic assurance to continuous verification.** Assurance must reflect the dynamic nature of systems. Continuous monitoring and testing are required to ensure that controls remain effective.
5. **From compliance to performance.** Ultimately, governance must be judged by outcomes. The ability to maintain and recover critical services under stress is the defining measure.

Implications for Boards and Executives

These changes have direct implications for leadership:

For Boards. Boards must redefine how they exercise oversight. They must:

- Focus on critical assets, not only risk categories.

- Require clarity on accountability
- Seek evidence of performance under stress
- Challenge assumptions about resilience.

This means Boards should be able to name the assets and services that matter most, identify their accountable owners and understand, at a high level, how those owners demonstrate control under stress.

For Executives. Executives must align organisational structures and processes with asset-level accountability. They must:

- Define asset ownership
- Clarify decision rights
- Integrate functions
- Ensure that systems support visibility and action.

In many organisations, this will involve re-designing governance around digital and cyber-physical assets, not just organisational units, and building integrated views of performance and risk for each.

For Operations. Operational teams must operate within a clear accountability framework. They must understand:

- Who is accountable
- How decisions are made
- How performance is measured.

They must be supported by systems that enable effective execution.

A Practical Starting Point

The shift to enterprise resilience does not require wholesale transformation from the outset. It can begin with focused actions. Organisations can:

1. Identify a small number of critical assets
2. Define clear accountability for those assets
3. Map dependencies and interfaces
4. Establish evidence of performance
5. Test response under realistic scenarios

In practice, this often begins with a handful of cyber-physical assets or critical services – for example, a key substation, rail corridor, data platform or clinical service; where accountability can be clarified, digital evidence consolidated and realistic scenarios exercised.

The journey from governance to control is not about discarding existing frameworks. It is about relocating their centre of gravity. When Boards and executives begin with the assets and services that matter most, accountability, risk management and assurance become tangible. Policies, risk appetite statements and committee structures still matter, but they now operate in support of asset-level accountability rather than in its place.

The case narratives in this book illustrates a consistent pattern. Where asset-level accountability and integrated visibility existed, organisations could absorb shocks, recover faster and protect value more effectively. Where accountability was fragmented, even sophisticated frameworks failed under stress. This pattern holds across sectors – transport, energy, digital platforms, financial services, health and public infrastructure – and across different regulatory regimes. The implication is clear: enterprise resilience is not a new specialist discipline; it is the practical expression of good governance in dynamic, cyber-physical systems.

The Risk of Inaction

The alternative to this shift is continuation of current practice. In stable conditions, this may appear sufficient. Over time, the risks accumulate. Dependencies increase. Systems become more complex. Expectations rise.

When disruption occurs, the consequences are amplified. Organisations face higher costs, greater scrutiny and reduced trust. This is not a hypothetical scenario. It is observable across sectors. It is also an increasingly prominent concern for regulators, investors and rating agencies, who now treat major operational and cyber disruptions as both system risks and governance failures.

The Opportunity

While the risks are significant, so is the opportunity. Organisations that adopt asset-level accountability and enterprise resilience can:

- Operate more reliably
- Respond more effectively to disruption
- Reduce costs associated with failure
- Build trust with stakeholders
- Improve access to capital.

These benefits are not abstract. They translate into financial performance and strategic advantage.

Digital and cyber-physical assets in closing. Throughout this book, digital and cyber-physical assets have appeared as the practical stage on which governance success or failure is revealed. Substations, rail corridors, data platforms, clinical services and transmission networks are no longer purely physical. They are controlled, monitored and reshaped through software, data and networks. Their behaviour under stress determines whether organisations meet their obligations to customers, regulators, investors and communities.

For Boards and executives, this means that enterprise resilience cannot be addressed solely through high-level frameworks or traditional risk categories. It must be governed where digital and physical realities meet – at the level of specific assets and services and the systems of systems they form. Digital twins, asset-centric monitoring and robust audit trails are not ends in themselves. They are the means by which asset owners can demonstrate control, by which Boards can exercise informed oversight and by which regulators and stakeholders can be confident that governance operates where risk materialises

From Governance to Stewardship. The shift described in this book also has broader implications. In asset-intensive sectors, organisations are not only operators. They are stewards of critical systems. These systems support economic activity, social wellbeing and environmental sustainability. Their performance affects communities and economies.

Governance must therefore extend beyond compliance. It must reflect responsibility for long-term outcomes. Enterprise resilience provides a framework for this stewardship. It aligns accountability, performance and value.

A Different Standard. The standard for governance is changing. It is no longer sufficient to demonstrate that frameworks exist and that risks are identified. Organisations must demonstrate that:

- Accountability is clear
- Systems perform under stress
- Recovery is effective.

evidence supports these claims. That evidence will increasingly be drawn from digital and cyber-physical assets themselves – from how they are designed, how they are monitored and how they respond under stress.

This is a higher standard. It requires changes in mindset, structure and practice. It also provides greater confidence.

Closing. The distinction between traditional governance and enterprise resilience is not incremental. It is fundamental. One relies on structure. The other relies on accountability. In stable environments, both may appear effective.

In dynamic, interconnected systems, only one provides control.

Organisations that recognise this distinction and act on it will be better positioned to navigate complexity, manage risk and create value. Those that do not will continue to experience governance failure, regardless of how well their frameworks are designed. The choice is clear.

Anchor accountability at the asset or accept that governance will not operate where it matters.

References

By Section

Introduction & Section 1 – Structural Failure of Governance

- Organisation for Economic Co-operation and Development (2019), *Good Governance for Critical Infrastructure Resilience*, https://www.oecd.org/gov/risk/good-governance-for-critical-infrastructure-resilience.htm (accessed March 2026).[2][3]
- Infrastructure Australia (2021), *National Study of Infrastructure Risk*, https://www.infrastructureaustralia.gov.au/publications/national-study-infrastructure-risk (accessed March 2026).[2]
- Australian National Audit Office (various), *Reports on Infrastructure and Asset Management*, https://www.anao.gov.au (accessed March 2026).[4]
- Power, M. (2007), *Organized Uncertainty: Designing a World of Risk Management*, Oxford University Press.[2]

Section 2 – Where Risk Actually Materialises

- Cybersecurity and Infrastructure Security Agency (CISA) (2022), *Pipeline Cybersecurity Initiative*, https://www.cisa.gov (accessed March 2026).[5][2]
- National Institute of Standards and Technology (NIST) (2020), *Framework for Improving Critical Infrastructure Cybersecurity*, https://www.nist.gov/cyberframework (accessed March 2026).[2]
- European Union Agency for Cybersecurity (ENISA) (2021), *Cybersecurity for Critical Infrastructure*, https://www.enisa.europa.eu (accessed March 2026).[2]
- UK National Audit Office (2019), *Rail Management and Timetable Disruption*, https://www.nao.org.uk (accessed March 2026).[2]
- World Bank (various), *Governance, Transparency and Accountability in Public-Private Partnerships*, https://ppp.worldbank.org (accessed March 2026).[6]

Section 3 – Accountability as the Mechanism

- Australian Prudential Regulation Authority (APRA) (2025), *Prudential Standard CPS 230 Operational Risk Management*, https://www.apra.gov.au (accessed March 2026).[7][8][2]
- APRA (2024), *Prudential Practice Guide CPG 230 Operational Risk Management*, https://www.apra.gov.au (accessed March 2026).[9]
- Financial Conduct Authority (FCA) & Prudential Regulation Authority (PRA) (2021), *Operational Resilience Policy Statement PS21/3*, https://www.fca.org.uk/publication/policy/ps21-3.pdf (accessed March 2026).[10][2]
- Security of Critical Infrastructure Centre (CISC) (2026), *Regulatory Obligations under the Security of Critical Infrastructure Act 2018*, https://www.cisc.gov.au (accessed March 2026).[11][12]
- Weick, K.E. & Sutcliffe, K.M. (2007), *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*, 2nd ed., Jossey-Bass.[2]

Section 4 – Operating Model of Enterprise Resilience

- Bank of England / PRA (2021), *Operational Resilience: Impact Tolerances for Important Business Services (SS1/21)*, https://www.bankofengland.co.uk (accessed March 2026).[10][2]
- PwC Australia (2024), *Navigating CPS 230 – Operational Resilience for Critical Operations*, https://www.pwc.com.au (accessed March 2026).[13]
- Digital Twin Consortium / ISO (2021), *ISO 23247 Digital Twin Framework for Manufacturing*, https://www.iso.org (accessed March 2026).[14][2]
- DLR (2024), *Digital Twins for Infrastructures*, German Aerospace Center, https://www.dlr.de (accessed March 2026).[15][14]

Section 5 – Financial, Strategic and Board Implications

- Australian Energy Regulator (AER) (2023), *State of the Energy Market*, https://www.aer.gov.au (accessed March 2026).[2]
- Office of Gas and Electricity Markets (Ofgem) (2021), *RIIO-2 Framework*, https://www.ofgem.gov.uk (accessed March 2026).[2]
- BlackRock (2022), *Infrastructure Investment Insights*, https://www.blackrock.com (accessed March 2026).[2]
- International Monetary Fund (2024), *Global Financial Stability Report – Cyber Risk and Financial Stability*, https://www.imf.org (accessed March 2026).[16][2]
- World Bank (2020), *Public-Private Partnerships Reference Guide*, https://www.worldbank.org (accessed March 2026).[6][2]
- Kleppe, G. (2026), *How to Measure ROI on Enterprise Resilience Investments*, GeoDataDecisions Explainer, internal publication.[17]

Section 6 – Conclusion: From Governance to Control

- (Most conclusion references are to earlier works; you can repeat key items.)
- OECD (2019), *Good Governance for Critical Infrastructure Resilience*.[3][2]
- APRA (2025), *CPS 230 Operational Risk Management*.[7]
- FCA & PRA (2021), *Operational Resilience PS21/3*.[10]
- ENISA (2021, 2022), *Cybersecurity for Critical Infrastructure* and *NIS2 Directive Overview*, https://www.enisa.europa.eu (accessed March 2026).[5][2]
- AICD & CSCRC (2025), *Cyber Security Governance Principles – Version 2*, https://www.aicd.com.au (accessed March 2026).[18]

By author / institution (example grouping)

Core academic and thought-leadership authors

- Power, M. (2007), *Organized Uncertainty: Designing a World of Risk Management*, Oxford University Press.[2]
- Taleb, N.N. (2012), *Antifragile: Things That Gain from Disorder*, Random House.[2]
- Weick, K.E. & Sutcliffe, K.M. (2007), *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*, Jossey-Bass.[2]
- Williamson, O.E. (1985), *The Economic Institutions of Capitalism*, Free Press.[2]
- Helm, D. (2017), *Cost of Energy Review*, UK Government, https://www.gov.uk (accessed March 2026).[2]
- Nature / Engineering journals (2019–2026), various articles on digital twins and cyber-physical systems.[19][20][21]

Australian institutions

- Australian Prudential Regulation Authority (APRA) – CPS 230, CPG 230 and previous CPS 510 governance standards.[9][7][2]
- Australian Energy Regulator (AER) – *State of the Energy Market*.[2]
- Australian Energy Market Operator (AEMO) – system security and reliability reports.[2]
- Critical Infrastructure Security Centre (CISC) – SOCI Act obligations and risk management program rules.[12][11]
- AICD & partners – *Cyber Security Governance Principles*, *Ethics in the Boardroom*.[22][18]

United Kingdom / Europe

- Financial Conduct Authority (FCA) & Prudential Regulation Authority (PRA) – *Operational Resilience PS21/3* and related supervision papers.[10][2]
- Bank of England – operational resilience policy and impact tolerance guidance.[2]
- National Audit Office (NAO) – rail timetable disruption and infrastructure governance reports.[4][2]
- Office of Gas and Electricity Markets (Ofgem) – RIIO frameworks.[2]
- ENISA – cybersecurity for critical infrastructure and NIS2 guidance.[5][2]
- European Court of Auditors – EU rail and infrastructure performance reviews.[2]
- ISO – ISO 23247 digital twin framework.[14][2]

United States / global technical bodies

- Cybersecurity and Infrastructure Security Agency (CISA) – pipeline cybersecurity and ICS guidance.[2]
- National Institute of Standards and Technology (NIST) – Cybersecurity Framework.[2]
- Various engineering / CPS researchers – digital twin and CPS conceptual papers.[20][19]
- Multilateral and financial institutions
- OECD – *Good Governance for Critical Infrastructure Resilience*.[3][2]
- World Bank – PPP governance and PPP reference guide.[6][2]
- International Monetary Fund (IMF) – *Infrastructure Governance and Risk*; *Global Financial Stability Report – Cyber Risk*.[16][2]
- BlackRock – infrastructure investment insights.[2]

GeoDataDecisions / internal publications

- GeoDataDecisions Pty Ltd (GDD Advisory) (2026), *Enterprise Risk Convergence – Protection of High-Value Assets*, Industry Briefing Paper.[23]
- GeoDataDecisions Pty Ltd (2026), *Enterprise Resilience for Renewable Energy Transmission: Cyberinfrastructure as Strategic Enabler*, Board Briefing Paper.[24]
- Kleppe, G. (2026), *How to Measure ROI on Enterprise Resilience Investments*, Explainer for CFOs and Boards.[17]
- GeoDataDecisions Pty Ltd (2026), *Board Maturity Matrix – Enterprise Resilience*, Explainer.[25]

By Weblinks

- https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/board-evaluation-director-appraisal-director-tool.pdf
- https://bschool.nus.edu.sg/cgs/wp-content/uploads/sites/145/2025/02/CGS_ORMC_Enterprise-Resilience_A-Playbook-for-Organisations_2025.pdf
- https://www.audit.vic.gov.au/report/compliance-asset-management-accountability-framework
- https://www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf
- https://ppp.worldbank.org/public-private-partnership/library/governance-public-private-partnerships
- https://handbook.apra.gov.au/standard/cps-230
- https://www.apra.gov.au/operational-risk-management
- https://www.apra.gov.au/sites/default/files/2024-06/Prudential Practice Guide CPG 230 Operational Risk Management.pdf
- https://lmalloyds.com/wp-content/uploads/2025/09/ss121-march-21-2.pdf
- https://www.cisc.gov.au/how-we-support-industry/regulatory-obligations
- https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018
- https://www.pwc.com.au/assurance/operational-resilience/pwc-navigating-cps-230-june-2024.pdf
- https://elib.dlr.de/148279/1/10.1515_auto-2021-0104.pdf
- https://www.dlr.de/en/pi/about-us/departments/digital-twins-for-infrastructures
- https://www.imf.org/-/media/files/publications/gfsr/2024/april/english/ch3.pdf
- EXPLAINER-ROI-on-Enterprise-Resilience.pdf
- https://www.aicd.com.au/risk-management/framework/cyber-security/cyber-security-governance-principles.html
- https://www.techscience.com/CMES/v143n1/60443/html
- https://www.sciencedirect.com/science/article/pii/S2667305325000420
- https://www.nature.com/articles/s41598-026-45272-z
- AICD-ethics-in-the-boardroom-2nd-edition.pdf
- Briefing-Paper-Risk-Convergence.pdf
- Board-Briefing-Strategic-Enabler-cyberinfrastructure.pdf
- EXPLAINER-Board-maturity-matrix.pdf
- https://www.aicd.com.au/content/dam/aicd/pdf/about/membership/reference-template.pdf
- https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/organisation/board-charters-director-tool.pdf
- https://www.aicd.com.au/board-of-directors/roles/executive/Reporting-to-the-board.html
- https://www.communitydirectors.com.au/help-sheets/terms-of-reference-template
- https://www.asx.com.au/content/dam/asx/about/corporate-governance-council/reviews-and-submissions/2018/Australian-Institute-of-Company-Directors.pdf
- https://www.aicd.com.au/board-of-directors/performance/effectiveness/asd-and-aicd-guidance-on-board-cyber-priorities-for-25-26.html
- https://www.aicd.com.au/board-of-directors/meeting/paper.html
- https://www.aicd.com.au/content/dam/aicd/pdf/news-media/policy/2018/final-asx-principles-table-27-july.pdf
- https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/bookstore/previews/Directors-Signpost-preview.pdf
- https://www.studocu.com/en-au/document/kings-own-institute/auditing-and-assurance/aicd-principles-06911-4-adv-nfp-governance-principles-report-a4-v11/119422262
- https://www.sparke.com.au/insights/changes-to-aicds-guidance-on-ai/
- https://www.aicd.com.au/content/dam/aicd/pdf/about/about-our-governance/compliance-policy.pdf
- https://poweringskills.com.au/wp-content/uploads/2025/03/PSO-004-Aligning-to-AICD.pdf

Glossary

Term	Definition Relevant in this Book
Asset Condition	The current state of an asset in terms of performance, degradation, defects, remaining useful life and ability to meet required standards under expected and stressed conditions.
Asset failure mode	The specific way in which an asset can fail – for example, sudden breakdown, progressive degradation, control malfunction or loss of containment – and the consequences of that failure for safety, operations and service.
Business Model	The way an organisation creates, delivers and captures value – including its products and services, customers, revenue streams, cost structure and key partnerships.
Computational Model	A digital representation that uses data and algorithms to simulate, analyse or predict the behaviour of a system, asset or process, often forming part of a digital twin.
Conditions of Failure	The specific combinations of events, dependencies, system states and behaviours under which an asset or service is likely to fail, as distinct from high-level risk categories.
Convergence	The way different risk domains – such as cyber, operational, regulatory, financial, environmental and social – interact and combine at the level of an asset or system, creating failure conditions that do not appear when each risk is considered in isolation.
Critical Infrastructure	Assets, systems and networks that are essential to the functioning of the economy, society or public safety, where loss or compromise would have significant consequences for communities and national interests.
Cyber Infrastructure	The digital and data capabilities that support critical operations, including networks, platforms, data stores, analytics, automation, monitoring and security services.
Cyber-Physical System	A Cyber-Physical System is a system in which physical assets and processes are tightly integrated with software, computation and networks, so that the digital components monitor, coordinate and control the physical behaviour in real time. Cyber-Physical Systems can exist at different scales – from a single production line to a plant, a piece of critical infrastructure or even a supply-chain – and may themselves be systems or Systems of Systems, depending on how they are organised and governed.
Cyber Security	The practices, processes, technologies and behaviours used to protect information, systems and networks from unauthorised access, disruption, misuse or damage.
Digital twin	A digital twin is a dynamic digital representation of a physical asset or system, continuously updated with data so that it reflects how that asset or system behaves in operation. It can be built for a single component, a whole asset or a multi-asset system, and may include multiple engineering disciplines (civil, mechanical, electrical, control) within one twin rather than being limited to a single discipline.
Enterprise	The organisation as a whole, including its legal entities, business units, assets, systems, contracts and relationships through which it creates and protects value.
Enterprise Resilience	The ability of the enterprise as a whole to maintain and restore critical operations and services under stress, across physical, digital, financial, regulatory and reputational dimensions, at an acceptable cost and speed.
Exposure Governance	How an organisation identifies, quantifies and monitors its financial and non-financial exposures – such as downtime cost, legal liability, reputational damage and concentration risk – and ensures these exposures remain within acceptable bounds.
Financial Close	The point in a project or transaction, often in infrastructure or PPPs, at which financing agreements are executed, funds are committed and contractual risk allocations are fixed, creating a strong appearance of control.
Governance	The arrangements by which an organisation is directed and controlled – including Board oversight, decision-making structures, policies, risk appetite and accountability for performance and compliance.
Operating Model	The practical arrangement of people, processes, technology, data, suppliers and governance through which an organisation delivers its strategy and runs day-to-day operations.
Operational Resilience	The ability of an organisation to prevent, respond to, recover and learn from operational disruptions so that important business services and critical operations remain within Board-approved impact tolerances.
Physical Asset	A tangible item such as a plant, facility, network component, piece of equipment or infrastructure element that directly contributes to the delivery of services or production of outputs.
Resilience	The ability of a system or organisation to absorb shocks, adapt to changing conditions and continue to deliver critical outcomes within acceptable tolerances, including recovery within an acceptable time and cost.
Resilience Governance	How an organisation defines, funds, tests and oversees its ability to continue critical operations under stress, including accountability for impact tolerances, preparedness, response and recovery.
Risk Governance	How an organisation sets risk appetite, allocates risk ownership, decides which risks it will accept,

Term	Definition Relevant in this Book
	mitigate or transfer, and oversees whether those decisions are implemented and effective.
Single Thread	A clear, continuous line linking a specific outcome or asset back to a named accountable owner, associated decision rights and supporting evidence.
Single Thread Ownership	A governance model where one identifiable executive or role is explicitly accountable for the performance, resilience and recoverability of a defined asset or service end-to-end, across functions and domains.
Structural Failure	A weakness in how governance, roles, incentives or systems are designed that causes recurring problems or amplifies shocks, regardless of the effort of individuals within the structure.
Supply chain	The network of organisations, processes, assets and data flows that provide inputs, services and capabilities required for the enterprise to operate and deliver outcomes.
System	A system is a set of components – physical and/or digital – that are designed and managed together to deliver a defined function or service. Those components can belong to one discipline (for example, an electrical protection system) or span several disciplines (for example, a building management system combining mechanical, electrical and control elements).
System of Systems	A System of Systems is a collection of independent systems – often owned or managed separately and built for different purposes – that interact to deliver capabilities none of them can provide on their own. These systems may span multiple disciplines and sectors (for example, energy, transport and communications in a smart city), but what defines a System of Systems is the independence of its constituent systems, not just cross-disciplinary scope.

Acronyms

Acronym	Meaning
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AICD	Australian Institute of Company Directors
ALE	Annual Loss Expectancy
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission (implied, if used)
ASX	Australian Securities Exchange (implied, if used)
BCP	Business Continuity Plan (implied)
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPS	Cyber-Physical System (also APRA's CPS standards; usually clear from context)
CPS 230	APRA Prudential Standard CPS 230 Operational Risk Management
CRIMP / CIRMP	Critical Infrastructure Risk Management Program (under the SOCI regime)
CRO	Chief Risk Officer
CSR	Corporate Social Responsibility
CTEM	Continuous Threat Exposure Management
DORA	Digital Operational Resilience Act (EU; if referenced)
ENISA	European Union Agency for Cybersecurity
ESG	Environmental, Social and Governance
EU	European Union
FCA	Financial Conduct Authority (UK)
HVDC	High-Voltage Direct Current
ICS	Industrial Control System
IMF	International Monetary Fund
IoT	Internet of Things
IIoT	Industrial Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicator
LNG / HV	if you refer to specific energy sectors; not explicit in our edits
NAO	National Audit Office (UK)
NIS2	EU Directive on Security of Network and Information Systems (revised Directive)
NIST	National Institute of Standards and Technology (US)
OECD	Organisation for Economic Co-operation and Development
OT	Operational Technology
PPP	Public-Private Partnership
PRA	Prudential Regulation Authority (UK)
PSPS	Public Safety Power Shutoff
PV	Photovoltaic (if used in renewable energy examples)
RACI	Responsible, Accountable, Consulted, Informed
RBA / CFR	Reserve Bank of Australia / Council of Financial Regulators (only if you reference them explicitly)
RIIO	Revenue = Incentives + Innovation + Outputs (Ofgem price control framework)
ROSI	Return on Security Investment
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SoS	System of Systems (if abbreviated)
SOCI	Security of Critical Infrastructure Act 2018 (Australia)
TBC / TBD	To Be Confirmed / To Be Determined (if left in draft text)
UK	United Kingdom
US / USA	United States (of America)

Book Licence Details

Copyright and licence

Attribution

When reusing or adapting this work, please use the following attribution where practicable:

Kleppe, G. (2026), *Enterprise Resilience – Governance for the Modern World: A new operating doctrine for asset-intensive organisations, GeoDataDecisions Pty Ltd, licensed under CC BY-NC-SA 4.0.*[5][6]

If changes have been made, please state: **"**Adapted from Kleppe (2026)**"** or **"**Based on Kleppe (2026)**"**, as appropriate, and retain the licence notice.[6][2]

Third-party material

Unless otherwise stated, this licence applies to the original text and original diagrams in this book.[7][8]

Third-party content is excluded from this Creative Commons licence unless expressly stated otherwise. This includes, where applicable, quoted extracts, photographs, logos, trademarks, screenshots, publisher-formatted reproductions, and any material reproduced with permission or under a separate licence.[8][9][7]

Where third-party material is identified, users must comply with the terms applicable to that material and obtain any further permissions required from the relevant rights holder.[7][8]

References

1. https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.en
2. https://creativecommons.org/licenses/by-nc-sa/4.0/deed.en
3. https://subjectguides.york.ac.uk/creative-commons/by-nc-sa
4. https://archivescentral.org.nz/rights/CC-BY-NC-SA-4.0
5. https://ruor.uottawa.ca/bitstreams/2e7bb22b-0873-47d1-a38d-c38bb4e6bdfb/download
6. https://ecampusontario.pressbooks.pub/app/uploads/sites/3514/2023/09/CC_attribution_best_practices_EN3.pdf
7. https://smartcopying.edu.au/how-to-label-third-party-content-in-creative-commons-licensed-material/
8. https://wiki.creativecommons.org/wiki/Marking/Creators/Marking_third_party_content
9. https://oercollective.caul.edu.au/monash-uni-open-book-pub-guide/chapter/creative-commons-and-licensing/
10. http://openscience.ens.fr/LEGAL_ISSUES/LICENSES/CREATIVE_COMMONS_LICENSES/CC_LICENSES/3_CC-BY-SA.pdf
11. https://www.youtube.com/watch?v=heANUAtBQrI
12. https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.txt
13. https://upload.wikimedia.org/wikipedia/commons/0/05/Creative-Commons-4.0-Wikimania-2014.pdf
14. http://openscience.ens.fr/LEGAL_ISSUES/LICENSES/CREATIVE_COMMONS_LICENSES/CC_LICENSES/6_CC-BY-NC-SA.pdf
15. https://pressbooks.pub/powerofthepen/front-matter/creative-commons-license-cc-by-nc-sa/

About the Author

Genéne Kleppe is an executive advisor, author and enterprise strategist whose work focuses on helping organisations make more confident decisions in increasingly complex operating environments.

Over more than three decades she has advised Boards, Chief Executive Officers and executive leadership teams across critical infrastructure, mining, energy, transport and government. Her work has consistently centred on one question:

How can organisations make better decisions before uncertainty becomes operational, financial or reputational consequence?

That question has shaped a career spanning enterprise governance, strategic asset management, major project delivery, operational technology, artificial intelligence, Digital Twins, enterprise information management and organisational transformation. Rather than treating these disciplines as independent capabilities, Genéne has sought to integrate them into a coherent executive approach that strengthens enterprise resilience, improves productivity and enables more confident decision-making.

Her work has contributed to major infrastructure and resource organisations in Australia and internationally, helping executives translate complex technical, operational and commercial information into practical governance decisions. Throughout this work, a consistent philosophy has emerged: governance should not be measured by the volume of information available, but by the confidence leaders have in the decisions they make and the outcomes those decisions produce.

This philosophy underpins the **Enterprise Resilience** publication series, the **Decision Assurance™** framework and the concept of **Digital Trust Stewardship**. Together, these works present an integrated executive operating model that positions governance, accountability and evidence as strategic capabilities for protecting enterprise value.

Genéne's work extends beyond organisational resilience. She is particularly interested in initiatives that improve productivity, strengthen national capability, build sustainable economic value and demonstrate that commercial success and ethical leadership are mutually reinforcing. She believes that enduring economic performance is achieved when innovation is grounded in transparent governance, accountable leadership and commercially robust ethics.

She lives near the beach in Adelaide, South Australia, where the rhythm of the coastline provides a welcome contrast to the complexity of the executive environments in which she works. From there she continues to advise organisations, develop new thinking and write for leaders seeking practical approaches to governing increasingly interconnected enterprises.

Her publications are intended not simply to explain new ideas, but to challenge established assumptions and provide executives with practical frameworks that improve decision confidence, enterprise resilience and long-term organisational stewardship.