MARENTIS Labs

STRATEGIC GOVERNANCE AS A SERVICE · PRINCIPAL-LED · ADVERSARIAL BY DESIGN

Strategic Governance as a Service:

More Governance Has Not Produced Better Governance

This Paper Explains Why And Proposes A Solution

A Marentis Labs Research White Paper · May 2026

OWEN VALLIS

Managing Director

marentislabs.com

Disclaimers

1. No Legal, Financial, or Regulatory Advice

The information, frameworks, and analyses contained in this white paper are provided for general informational, educational, and strategic purposes only. Marentis Labs Ltd is a strategic governance advisory firm, not a law firm, accountancy firm, or a firm authorised by the Financial Conduct Authority (FCA) or Prudential Regulation Authority (PRA). The contents of this document do not constitute, and should not be construed as, legal, financial, investment, accounting, tax, or regulatory compliance advice.

References in this document to regulatory frameworks, including the Senior Managers and Certification Regime (SM&CR), the UK Corporate Governance Code, the EU Digital Operational Resilience Act (DORA), US Caremark doctrine, and related statutory or regulatory instruments, are provided for contextual and illustrative purposes only. Nothing in this document constitutes advice on any individual's or organisation's obligations, liabilities, or defences under any such regime, including the adequacy of any specific individual's compliance position under SM&CR or any equivalent personal accountability regime. Readers must not rely on this document as a substitute for seeking independent advice from qualified legal, compliance, or regulatory practitioners regarding their specific statutory duties, fiduciary obligations, or applicable regulatory requirements in any jurisdiction.

2. Forward-Looking Statements

This document contains forward-looking statements, projections, and illustrative scenarios, including statements about governance outcomes, potential value creation, loss avoidance probabilities, and regulatory trajectories. These statements are based on assumptions and information available at the time of publication. They are subject to known and unknown risks, uncertainties, and other factors that may cause actual results to differ materially from those expressed or implied. Marentis Labs Ltd makes no commitment to update forward-looking statements following publication. Readers should not place undue reliance on them.

3. Limitation of Liability and No Guarantee of Outcomes

Corporate governance and risk management involve inherent uncertainties and dynamic variables. While the methodologies and frameworks outlined in this document are designed to mitigate risk and improve governance maturity, Marentis Labs Ltd makes no representations, warranties, or guarantees, express or implied, regarding specific financial outcomes, the prevention of corporate financial losses, or the absolute prevention of governance failures.

To the fullest extent permitted by applicable law, Marentis Labs Ltd, alongside its directors, officers, employees, and agents, accepts no liability whatsoever for any direct, indirect, special, or consequential loss or damage, or any legal liabilities arising out of or related to any organisation's or individual's reliance on the strategies, frameworks, or information presented herein. Nothing in this notice shall limit or exclude liability for fraud, fraudulent misrepresentation, or any other liability which cannot lawfully be limited or excluded under English law.

4. Intellectual Property and Trade Mark Reservation

This white paper and the concepts detailed within contain proprietary intellectual property belonging exclusively to Marentis Labs Ltd. "Strategic Governance as a Service (SGaaS)", "Marentis Risk Maturity Model", "Red Team Protocol", "Risk Simulation Lab", "Pre-Mortem Diagnostic", and "Governance Pulse" are proprietary assets of Marentis Labs Ltd. The architectural models, diagnostic frameworks, and methodologies described herein are strictly confidential and may not be reproduced, distributed, transmitted, adapted, or utilised for commercial purposes by any third party without the express prior written consent of Marentis Labs Ltd. All rights reserved. Nothing in this paragraph derogates from any rights of fair dealing or other statutory exceptions under applicable copyright law.

5. Accuracy of Historical and Regulatory Information

This document references historical corporate events, public inquiries, third-party statistics, and specific regulatory frameworks (including, but not limited to, the UK Corporate Governance Code, SM&CR, EU DORA, and US Caremark case law). While Marentis Labs Ltd has sourced this information from publicly available records, academic research, and industry reports believed to be reliable at the time of publication, no representation or warranty, express or implied, is made as to the accuracy, completeness, or current validity of these references. Regulatory environments and case law are subject to continuous change. All historical case studies are provided solely for illustrative and educational purposes.

6. No Endorsement or Affiliation Implied by Citation

Citation of any third party in this document, including authors, regulators, supervisory authorities, public inquiries, professional bodies, academic institutions, and commercial organisations, is for analytical, illustrative, and educational purposes only. Such citation does not constitute or imply endorsement of Marentis Labs Ltd, the Strategic Governance as a Service framework, the Marentis Risk Maturity Model, or any conclusion presented in this document. Readers must not infer co-authorship, partnership, sponsorship, affiliation, or any commercial relationship between Marentis Labs Ltd and any cited author, organisation, or regulatory body. The views, analyses, and recommendations expressed herein are those of Marentis Labs Ltd alone.

7. Data Protection and Privacy

Marentis Labs Ltd processes personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Where this document is accessed via a gated channel or lead capture mechanism, any personal data collected in connection with that process is handled in accordance with the Marentis Labs Ltd Privacy Notice, available at 'www.marentislabs.com. This document does not itself constitute a mechanism for the collection or processing of personal data.

8. Governing Law and Jurisdiction

This document, and any non-contractual obligations arising from or in connection with it, are governed by the laws of England and Wales. Any dispute arising out of or in connection with this document shall be subject to the exclusive jurisdiction of the courts of England and Wales.

9. Copyright Notice

Company Number: 16600357

Registered Address: 167-169 Great Portland Street, 5th Floor, London, W1W 5PF, UK

Table of Contents

1 Executive Summary

Spending on governance, risk management, and compliance has never been higher. The global GRC market is estimated at approximately USD 72 billion in 2025[25] and is growing at over 13% annually.[25] Regulatory requirements have proliferated across every major jurisdiction and organisations across all sectors of the global economy have invested in risk committees, internal audit functions, compliance teams, and external advisory. Yet the frequency and severity of governance failures has not decreased.

Boeing's 737 MAX programme killed 346 people[69] and cost the company an estimated USD 20 billion, including the largest Caremark derivative settlement in Delaware history. This despite the presence of a full complement of governance structures commensurate with its status as an S&P 100 company, with a board, an audit committee, an internal audit function, external auditors, and regulatory oversight from the FAA. The Post Office prosecuted more than 900 sub-postmasters over two decades while every layer of its governance architecture, from branch-level management to the board to external legal advisers, failed to adequately challenge a system that was known to be flawed.[74] Wirecard's EUR 1.9 billion fraud[39] survived scrutiny from a supervisory board, internal audit, a "Big Four" external auditor, and BaFin as regulator. All five governance layers were present and all five failed. Silicon Valley Bank collapsed in 48 hours despite having risk committees, an internal audit function, and regulatory oversight.[3]

These are simply some of the high profile and well documented consequences of a structural problem. More governance infrastructure has not produced better governance outcomes. This paper calls this the *Governance Paradox*, and argues that the paradox has an identifiable cause and a structural solution.

The catastrophic cases that make global headlines are the extreme anchor points. The more common consequence of the same structural defects by far, is quieter, insidious value destruction, manifesting as failed M&A integrations, missed technological pivots, and the slow erosion of competitive position that no governance function is mandated to challenge. Empirical evidence from 669 listed companies across Germany, Austria, and Switzerland[30] shows that 32% suffered at least one severe corporate crisis between 2018 and 2024, and that over 80% of those events were driven by strategy and external risks, not by compliance failures. The structural defects that produce billion-pound corporate implosions also produce routine, chronic value destruction. The economic case for addressing these defects depends on preventing the strategic drift that compounds, unchallenged, for years.

1.1. The Diagnosis

Governance failures occur despite the application of a range of frameworks because of three systemic defects in how oversight is delivered:

Episodic engagement. Boards engage with risk on periodic cycles, through quarterly risk reports, annual strategy reviews, and scheduled committee meetings. But risks do not evolve on quarterly cycles. The result is governance by snapshot rather than by signal, i.e. boards see the risk environment as it was at the last reporting date, not as it is when decisions are made.

Consensus dependency. Board decision-making is structurally biased toward satisficing; accepting the first option that achieves group agreement rather than stress-testing for the most resilient path. This is a predictable consequence of bounded rationality operating in a group setting, compounded by what Kahneman, Sibony, and Sunstein identify as "noise",[35] i.e. the variability in professional judgement that even qualified decision-makers produce under identical conditions.

Absence of institutionalised challenge. No permanent function exists within most governance architectures whose explicit purpose is to challenge assumptions, stress-test decisions, and surface failure modes before they materialise. Internal audit, the function nominally positioned for this role, spends 75% of its capacity on routine assurance and compliance.[31] Risk management functions face ever increasing funding constraints for emerging-risk identification, consuming their bandwidth on business-as-usual monitoring and regulatory reporting. Neither has the mandate, the capacity, or the methodology to act as a continuous, adversarial challenge function at board level.

1.2. The Evidence

This paper examines these three defects through multiple lenses. It traces their theoretical foundations in bounded rationality, decision noise, and the structural limitations of the Three Lines model. It documents their consequences through five extended case studies, namely Boeing, Wirecard, Silicon Valley Bank, Credit Suisse*, and The Post Office. Each shows how the same structural defects produced catastrophic outcomes across different sectors, jurisdictions, and regulatory regimes. It maps the regulatory direction across the United Kingdom, European Union, and United States, demonstrating a convergence toward the very capabilities the current model cannot deliver, namely continuous oversight, effective challenge, and personal accountability.

It then examines the value gap in the Three Lines model, the measurable space between what the model is supposed to deliver and what it actually delivers in practice. It shows why traditional advisory models cannot fill that gap.

1.3. The Response

Strategic Governance as a Service (SGaaS) is the structural response to these three defects. Developed and originated by Marentis Labs, SGaaS replaces episodic oversight with continuous engagement, consensus dependency with adversarial challenge, and the absence of institutionalised challenge with a permanent, principal-led governance function that operates at board level.

SGaaS is not a replacement for internal functions, it is the resilient challenge layer that fills the structural gap the Three Lines model leaves open, through which so many corporate failures have burst.

This paper presents the evidence, the theory, and the architecture for that response. It does so with the intellectual discipline the subject demands, remaining conservative in its claims, honest about limitations, and rigorous in its sourcing. The structural defects those failures reveal are identifiable, addressable, and, for organisations willing to commission genuine challenge, solvable. This paper makes no claim that SGaaS would have prevented every failure documented in these pages; it claims that the architecture described here

*The author was previously employed at Credit Suisse. Views expressed are based on public-record analysis only.

would have changed the information available to decision-makers, and the timing at which it arrived.

1.4. Paper Structure

Phase	Purpose	Sections
I. The Problem	Establish the governance paradox through evidence and theory	Executive Summary; The Governance Paradox; The Theory of Governance Failure; The Evidence of Failure
II. The Context	Regulatory convergence, the Three Lines value gap, and the limits of existing models	The Regulatory Direction; The Value Gap in the Three Lines; Why Traditional Models Under-Deliver
III. The Response	Define SGaaS, its methodology, architecture, and economic case	Defining SGaaS; The Adversarial Methodology; The Four-Tier Architecture; The Economic Case
IV. The Test	Stress-test the proposition through objections, implementation, and conclusion	Objections and Responses; Implementation Blueprint; Conclusion

Table 1. Paper structure: phases, purpose, and sections

2 The Governance Paradox

Organisations have never spent more on governance. The global governance, risk, and compliance industry alone is now worth approximately USD 72 billion[25] and is growing at more than 13% annually. Financial crime compliance consumes over USD 206 billion[42] each year. The four largest professional services firms collectively generated more than USD 95 billion in advisory revenue in 2023,[†] a significant and growing proportion of which is directed toward risk management, regulatory compliance, and governance advisory.

Regulators, meanwhile, have responded to each successive crisis by adding new requirements. In their Cost of Compliance Report 2023, LSEG[67] tracked 61,228 regulatory events in 2022, the third-highest annual total since monitoring began in 2008, reported to regulators across 190 countries and producing the equivalent of 234 regulatory alerts every working day. The Dodd-Frank Act[71] alone runs to 2,300 pages and mandated the creation of more than 400 new rules. In Europe and the United Kingdom, the post-2008 period has produced MiFID II,[16] GDPR,[17] the Senior Managers and Certification Regime,[22] the updated UK Corporate Governance Code, DORA (EU), and dozens of sector-specific conduct and resilience requirements.

By any measure, organisations in developed markets have never spent more on governance, never employed more compliance professionals, never operated under more regulatory oversight, and never had access to more sophisticated risk management tools. The reasonable expectation would be that governance outcomes have improved commensurately.

They have not.

2.1. The Failure Record

The period since the 2008 financial crisis, the very period in which governance spending and regulatory intensity have been at their highest, has produced a continuous sequence of governance failures at extraordinary scale. These are headline cases, the visible tip of the iceberg, each investigated by regulators, litigated in courts, or examined by public inquiries, and each attributable in significant part to failures of board-level oversight, management practice, or regulatory engagement.

The Libor manipulation case, the Tesco accounting scandal, the collapse of FTX, and the Theranos deception share the same structural signature and are excluded only for space. The nine cases in Table 2 were chosen because each has been the subject of regulatory enforcement, judicial scrutiny, or public inquiry, and because the governance failure in each case is documented rather than inferred.

The cumulative financial cost is staggering. The nine cases in Table 2 alone represent, conservatively, more than USD 150 billion in direct losses, fines, settlements, and compensation, before accounting for indirect costs such as market contagion, reputational destruction, and systemic economic damage. And these are only the failures that became public.

[†]Aggregate based on individual firm annual reports: Deloitte, PwC, EY, and KPMG global revenues.
[‡]Subsequently relegated to third place following the failure of First Republic in May 2023

Year	Organisation	Governance Failure	Consequence
2001	**Enron**	Board failed to oversee off-balance-sheet SPVs; auditor conflicts unaddressed; risk committee did not challenge management's financial structures	USD 74 billion in shareholder losses; criminal convictions; Sarbanes-Oxley Act enacted
2008	**Lehman Brothers**	Board did not effectively challenge leverage and concentration risk; risk management subordinated to revenue generation	Largest bankruptcy in US history; major inflection point of the global financial crisis
2015	**Volkswagen**	Governance architecture permitted deliberate regulatory deception through emissions software; supervisory board failed to detect or challenge	EUR 32+ billion in fines, retrofits, and legal costs
2016	**Wells Fargo**	Sales practice failures creating approximately 3.5 million unauthorised accounts;[46] risk management and internal controls failed to escalate systemic misconduct[61]	USD 3+ billion in fines and settlements; CEO resignation
2018	**Carillion**	Board approved aggressive accounting; missed repeated red flags on contracts; pension obligations unaddressed	GBP 6.9 billion in liabilities; GBP 2.6 billion pension deficit; 43,000 jobs at risk[29]
2018–19	**Boeing 737 MAX**	Board committees had no explicit responsibility for aircraft safety; no structured challenge of MCAS software assumptions	346 deaths; USD 20+ billion in direct costs; USD 237.5M derivative settlement
2020	**Wirecard**	Supervisory board accepted growth narrative without adversarial examination; EUR 1.9 billion in fabricated cash balances	EUR 24 billion in market cap destruction; CEO arrested; auditor EY under investigation
2023	**Silicon Valley Bank**	CRO vacancy for nine months during critical growth; interest-rate and concentration risk ungoverned	USD 175.5 billion in deposits; second-largest US bank failure‡; USD 16.1 billion FDIC cost
2000–24	**Post Office**	20-year failure of board oversight; management narrative prioritised over statistical evidence; no challenge of Fujitsu system reliability	900+ wrongful prosecutions; over £1.44 billion in compensation paid by March 2026; statutory public inquiry

Table 2. Selected governance failures, 2001–2024: causes and consequences

2.2. The Pattern Beyond the Headlines

The case record understates the problem. Headline failures are investigated, litigated, and remembered while the broader population of governance failures are much more opaque. Recent empirical work brings that population into view. A study of 669 listed companies across Germany, Austria, and Switzerland between 2018 and 2024, found that 32% suffered at least one severe corporate crisis,[30] defined as a monthly share-price decline of 25% or more. Almost one in three listed firms in one of the most heavily regulated developed-market regions experienced a documented value-destroying event in a seven-year window. One third of those firms suffered three or more such events over the same period. The authors read the repetition as evidence of "structural weaknesses rather than random shocks", a diagnosis that aligns directly with the argument this paper develops from the case record. The cases in Table 2 are not statistical anomalies. They are the visible surface of a population-level pattern.

The structural diagnosis is not new. In a 2010 McKinsey working paper written for a board audience, Brodeur et al.[6] observed that "at nonfinancial companies there is a growing sense that their oversight of risks is superficial and their risk management activities are not well integrated in the company's management system. They suspect that their business activities may hide continued vulnerabilities that will manifest themselves in the next risk storm." This was written by four McKinsey partners in the immediate aftermath of the 2008 financial crisis. In the sixteen years since that paper was published, global governance spending has roughly tripled, the regulatory stack has expanded materially, and the crises the authors anticipated have arrived on schedule, with Wirecard in 2020, Silicon Valley Bank in 2023, the Post Office Inquiry in 2024, and the Boeing Caremark settlement in 2022. The advisory industry diagnosed the problem accurately in 2010 and has not closed the gap in the nearly two decades since.

2.3. Value Erosion: The Quiet Majority

The headline failures command attention because they are the most catastrophic examples, but they are not the most common outcome of governance failure. For every Wirecard or SVB, dozens of organisations suffer a slower, less visible form of governance failure, value erosion. Failed M&A integrations that destroy the value they were designed to capture. Missed technological pivots, most pressingly in AI adoption, where two-thirds of boards lack the knowledge to evaluate what management tells them (Section 3). Slow-burn market share loss as competitors move while the board reviews quarterly reports that confirm last quarter's strategy was adequate. These are not compliance failures. They are failures of challenge, continuity, and independence, the same three structural defects, producing damage that is chronic rather than acute.

The Hunziker et al.[30] data makes the point quantitatively. Of the 395 classified crisis events in their DACH sample, 40.8% were driven by strategy risks and a further 40.0% by external risks (395 of the 471 identified events, classified by primary risk driver). Only 19.2% fell into the preventable-risk category that compliance-oriented governance targets. Eight in ten value-destroying events originated in categories where the required response is not better controls but better challenge, namely adversarial scrutiny of strategic assumptions, continuous monitoring of competitive position, and structured dissent before consensus hardens around a course of action. The McKinsey finding that approximately 70% of mergers fail to achieve their stated value targets[47] sits in the same territory i.e., governance architectures that cannot challenge the acquisition thesis at the point of decision cannot prevent value destruction during integration.

The economic cost of strategic drift does not often appear in a single quarterly write-down. It lurks under the surface, hiding from easy detection in the twelve-percentage-point recovery gap that Hunziker et al. document (Section 11), the permanent loss of relative market position that follows a severe governance event and never closes. For mid-market firms, where a twelve-point gap against sector peers compounds over years, the cumulative cost of quiet value erosion may exceed the headline cost of a single catastrophic failure.

The case studies that follow (Section 4) are the extreme anchor points. They demonstrate, with documentary precision, what happens when the structural defects operate unchecked to their terminal conclusion. But the more common manifestation of those same defects is not an explosion. It is a slow leak, made up of strategic decisions that were never stress-tested, competitive threats that were acknowledged in board papers but never acted upon, and transformation programmes that stalled because no function was mandated to ask whether the assumptions still held.

The 2026 geopolitical and global economic environment has only compounded the pressure on boards. The World Economic Forum, in its 2026 Global Risk Report,[75] drawing on the Global Risks Perception Survey 2025–2026 and the views of over 1,300 senior risk experts surveyed in August and September 2025, reports that 50% of respondents anticipate a turbulent or stormy global outlook over the next two years, rising to 57% over ten. Only 1% anticipate a calm outlook in either horizon. The two-year figure represents a fourteen-percentage-point deterioration against the 2025 survey. The Forum frames the moment as "an age of competition" defined by "the accelerating scale, interconnectedness and speed of global risks". The governance architectures diagnosed above were designed for an environment that the practitioner consensus no longer recognises. The case for architectural change is not receding.

2.4. The Paradox Defined

The governance industry has grown and regulatory requirements have proliferated. Compliance spending has reached levels that would have been unimaginable twenty years ago, and yet the frequency and severity of governance failures has not decreased. If anything, the scale of individual failures has increased, with post-2008 incidents routinely destroying tens of billions in value.

This is the Governance Paradox: **more governance has not produced better governance.**

The Governance Paradox

The volume of governance activity (regulation, compliance, audit, risk management, board oversight) has never been greater. Yet the outcomes that governance exists to prevent continue to occur, including catastrophic failures at the extreme, and chronic strategic drift, missed pivots, and quiet value erosion across the broader population. More governance has not produced better governance outcomes.

The instinctive response to each failure has been to add more governance, with more regulation, more reporting, more oversight mechanisms, and more compliance staff. Each of the organisations that failed catastrophically already had governance frameworks, risk committees, compliance functions, internal audit departments, and external auditors. Boeing had a governance structure; Wirecard had a supervisory board; SVB had a risk committee; The Post Office had layers of management oversight. Volume was never the

problem.

The problem is not the absence of governance. It is the nature of governance as it is currently delivered.

2.5. The Question This Paper Answers

Something more fundamental is wrong with how governance is structured and delivered in medium-to-large organisations. Frameworks exist. Regulation has proliferated. Spending has reached historic levels. But regular failures have continued regardless.

This paper argues that governance fails because of three structural defects embedded in the dominant governance model, namely episodic engagement with risk, consensus-dependent decision-making, and the absence of an institutionalised challenge function. They are defects of architecture, present in organisations with well-resourced governance functions and highly competent boards, because they are products of how governance is designed rather than how it is performed.

The following sections examine each defect in turn, ground them in academic theory and empirical evidence, and present a structural response, a governance architecture specifically designed to counteract these defects through continuous, adversarial, principal-led oversight at board level.

That architecture is **Strategic Governance as a Service.**

3 The Theory of Governance Failure

Governance failure is not random. So why do organisations with governance frameworks, risk committees, internal audit functions, and external auditors still regularly experience catastrophic oversight failures?

This section proposes that governance failure is a predictable outcome of three structural defects that are embedded in how governance is designed and delivered in most medium-to-large organisations.

These defects are:

- Episodic engagement with risk
- Consensus dependent decision-making
- Absence of an institutionalised challenge function

Each defect has independent theoretical support. Taken together, they explain why governance fails despite increasing investment and point toward the architectural changes required to produce different outcomes.

The intellectual frame for this diagnosis is older than any of the defects it identifies. Karl Popper, in *The Open Society and Its Enemies*, argued that institutional theory had been pursuing the wrong question. The governance question is not *who should rule*, which presumes decision-makers who will reliably get the answer right, but *how can institutions be arranged so that bad or incompetent decisions can be detected and corrected before they do too much damage?*[55] The distinction is subtle but significant. It shifts the object of governance design away from the selection of good decisions and toward the construction of systems that surface their own errors. The three structural defects that follow are each a specific way in which conventional governance architecture disables that second discipline. Episodic engagement prevents errors from being detected in time. Consensus dependency prevents them from being named once detected. The absence of institutionalised challenge ensures that no function is adequately mandated to look for them at all.

3.1. Bounded Rationality and the Satisficing Board

In 1947, Herbert Simon published *Administrative Behavior*,[62] a study of decision-making processes in organisations that would fundamentally reshape economic and management theory. Simon's central insight was that human decision-makers do not behave as classical economics assumes. They do not survey all available options, calculate the consequences of each, and select the optimal choice. They cannot, because they are constrained by limited information, limited cognitive processing capacity, and limited time.

Simon called this condition *bounded rationality*: rationality that is bounded by the cognitive limitations of the decision-maker and the complexity of the environment in which decisions are made. Under conditions of bounded rationality, decision-makers do not optimise. They *satisfice*, a term Simon coined as a portmanteau of "satisfy" and "suffice" to describe the practice of searching for alternatives only until finding one that meets a minimum threshold of acceptability.

"Whereas economic man maximizes-selects the best alternative from among all those available to him-his cousin, the administrator, satisfices-looks for a course of action that is satisfactory or 'good enough.'" - Herbert Simon, Administrative Behavior[§].[62]

Simon's work earned him the Nobel Prize in Economics in 1978 and has been extensively validated across organisational, economic, and psychological research over the subsequent seven decades. Daniel Kahneman's *Thinking, Fast and Slow*[34] extended Simon's framework by demonstrating the specific cognitive mechanisms (anchoring, availability bias, overconfidence, and the substitution of System 1 intuition for System 2 deliberation) through which bounded rationality manifests in professional judgement. In *The Psychology of Risk*,[5] Breakwell provides complementary evidence from risk psychology, documenting how optimism bias compounds these effects. Decision-makers systematically overestimate favourable outcomes through both motivated reasoning (defensive denial of threats to self-image) and cognitive egocentrism (weighting personal experience above base-rate evidence). In a governance context, optimism bias means that boards not only process incomplete information but do so through a cognitive lens biased toward favourable interpretation of the information they receive.

3.1.1. Application to board-level governance

Boardrooms are environments in which bounded rationality operates with particular force. Directors are typically part-time, serving on multiple boards, with limited time to process the volume of material presented to them. They are dependent on management for the information they receive, creating the information asymmetry that principal-agent[¶] theory[38] predicts: an asymmetry that the executive management controls and has an inherent interest in protecting. They operate under social pressure to maintain collegial relationships and to reach consensus within the limited time available at board meetings.

Under these conditions, satisficing is a predictable cognitive outcome, not a mark of individual failure. Boards accept management's preferred narrative because challenging it requires time, information, and expertise they may not have. They approve strategies that have achieved internal consensus because the cognitive cost of reopening the analysis exceeds their available processing capacity. They focus on the agenda items management has prioritised rather than asking what has been omitted.

The consequence is a systematic bias toward acceptance and consensus. Boards that satisfice are not incompetent. They are operating exactly as bounded rationality predicts they will operate in the absence of structural mechanisms designed to counteract it.

3.1.2. The empirical signature

The cognitive argument is reinforced by a market pattern. Hunziker et al[30] analysed 471 severe share-price declines of 25% or more across Germany, Austria, and Switzerland between 2018 and 2024 (of which 395 were classified by underlying risk driver; see Section 2) and found that they cluster on the reporting calendar. The heaviest months were September (70 events), June (57), and October (56). The authors' interpretation is that "event risk clusters around reporting cycles and is often triggered by corporate announcements". The implication for governance is sharper than the statistic. Material risk does not crystallise on the reporting rhythm; its public recognition does. Boards whose engagement with risk is indexed to the same rhythm learn of material exposures at

[§] quote from the 1997 fourth edition

[¶] Principal agent theory was originally developed by Michael Jensen and William Meckling in their 1976 paper in the Journal of Financial Economics called "Theory of the firm: Managerial behavior, agency costs and ownership structure" (https://doi.org/10.1016/0304-405X(76)90026-X)

roughly the moment the market does, with no advantage of foreknowledge and no window in which to act. Episodic engagement is a documented empirical pattern in the timing of value destruction, confirmed by market data. And the pattern will not dissipate in a calmer environment: The WEF[75] reports that only 1% of over 1,300 surveyed risk experts anticipate a calm global outlook in either the two- or ten-year horizon. The cognitive defect identified here operates inside an environment that the practitioner consensus considers anything but benign.

The AI amplifier. Artificial intelligence provides a current, concrete test of bounded rationality under pressure. Deloitte,[44] in a survey of 695 board members and C-suite executives across 56 countries in January and February 2025, found that 66% of respondents report their boards have "limited to no knowledge or experience" with AI. Nearly one-third (31%) say AI is not on the board agenda at all. Only 17% address it at every meeting. The bounded-rationality prediction is precise. Boards that lack the cognitive resources to evaluate a risk domain will engage with it episodically rather than continuously, and will default to accepting management's framing rather than challenging it. The Deloitte findings confirm the prediction in the domain where governance stakes are rising fastest. Two-thirds of boards cannot evaluate what management tells them about AI. One-third do not discuss it. The satisficing pattern identified by Simon in 1947 is operating, measurably, in the risk category that the WEF[75] identifies as showing the sharpest increase in perceived severity between the short and long term.

Structural Defect 1: Episodic Engagement

Boards engage with risk on a periodic cycle, marked by the quarterly report, the annual risk review, and the strategy day. Between these episodes, risk evolves continuously while oversight is dormant. Bounded rationality ensures that even when boards do engage, they process what is presented rather than seeking what is missing. The result is governance by snapshot in a world of continuous motion.

3.2. Noise and the Variability of Professional Judgement

In 2021, Daniel Kahneman, Olivier Sibony, and Cass Sunstein published *Noise: A Flaw in Human Judgment*,[35] a work that identified a problem in professional decision-making that had been hiding in plain sight.

The authors distinguish between two types of error in judgement:

Bias is systematic directional error i.e., a consistent tendency to err in the same direction.

Noise is unwanted variability i.e., different professionals reaching materially different conclusions when presented with identical information.

Bias has been extensively studied. Noise, the authors argue, has been largely ignored despite contributing at least as much to total judgement error.

The evidence is striking. In one of the book's most arresting findings, a study of insurance underwriters asked experienced professionals to set premiums for the same five fictitious customers. The median difference between any pair of underwriters' quotes was 55%. When executives were asked to predict the variability, they estimated 10%.

Kahneman, Sibony, and Sunstein document comparable noise across medicine (psychiatric diagnoses agreed in only 50% of cases for the same patients), criminal sentencing, forensic science, patent evaluation, and personnel selection. The pattern is consistent. Wherever

professionals exercise judgement, the variability in their conclusions is far greater than the professionals themselves believe.

3.2.1. Application to board-level governance

Board decisions are acts of professional judgement under uncertainty. Directors assess strategy proposals, evaluate risk exposures, approve capital allocations, and form views on management performance. These are precisely the kinds of complex, multi-dimensional judgements in which noise is most prevalent.

Consider two boards of equivalent competence, presented with the same strategic proposal, the same risk data, and the same management recommendation. If the noise findings apply (and there is no theoretical reason they would not) those two boards may reach materially different conclusions. The outcome depends not on the quality of the information but on who speaks first, how the question is framed, what recent events are salient in directors' minds, and whether the prevailing mood in the room favours caution or ambition.

The practical implication is that board decisions are less reliable than boards believe them to be. A board that approves a strategy by consensus may be experiencing the comfort of agreement without the assurance of rigour. A different board, on a different day, with a different seating arrangement and a different opening speaker, might have reached a different conclusion, and either conclusion might be correct.

Kahneman, Sibony, and Sunstein propose a remedy they call *"decision hygiene"*, structured processes designed to reduce noise in the same way that medical hygiene reduces contamination. Their specific mechanism is the Mediating Assessments Protocol (MAP), which can be summarised to a three-step process: first, define the key dimensions of the decision independently before discussion begins; second, have each assessor rate each dimension independently, grounded in evidence, before seeing others' assessments; third, integrate the independent assessments into a final decision only after all dimensions have been scored.

The MAP is designed to prevent the social dynamics that amplify noise, including anchoring to the first opinion expressed, conformity pressure, halo effects from strong personalities, and the substitution of overall impression for structured analysis. It is, in essence, an adversarial process, one that forces independent, evidence-based judgement before allowing group synthesis.

Structural Defect 2: Consensus Dependency

Board decision-making is structurally biased toward consensus. Directors operate under social pressure to agree, under time pressure to conclude, and under cognitive pressure to satisfice. Without a structured mechanism to force independent, evidence-based judgement (a decision hygiene function) boards are subject to the same noise that produces 55% variability in insurance underwriting. The result is decisions that feel rigorous but may be artefacts of group dynamics rather than structured analysis.

3.3. The Three Lines Model and the Missing Challenge Function

The Three Lines Model, updated by the Institute of Internal Auditors in July 2020, is the dominant governance architecture in medium-to-large organisations, particularly in financial services and professional firms. It provides a framework of layered assurance.

The first line (management) owns and manages risk; the second line (risk management, compliance) provides oversight and monitoring; and the third line (internal audit) provides independent assurance.

The model has clear strengths. It defines ownership of risk across the organisation, establishes the principle of independent assurance, and provides a common language for governance architecture. It is, however, a model designed for assurance, providing confidence that controls are operating and risks are being managed. What it was not designed for and does not provide, is a resilient mechanism for continuous, adversarial challenge of strategic decisions and governance architecture at board level.

3.3.1. The Academic Critique

Michael Power, Professor of Accounting at the London School of Economics, has argued in *Organized Uncertainty*[56] that the intensification of risk management has produced a paradoxical outcome. Organisations invest heavily in demonstrating accountability *for* risks rather than in actually reducing risk exposure. Power's thesis, building on his earlier *The Audit Society*,[57] is that governance frameworks become rituals of verification, systems that produce the appearance of control without necessarily delivering its substance.

This critique applies with particular force to the Three Lines Model. The model creates an architecture of assurance in which each line produces reports, assessments, and opinions that flow upward to the board. But the model does not create a function whose purpose is to *break* the assurance, to challenge whether the reports reflect reality, whether the assessments withstand scrutiny, or whether the governance framework itself is fit for purpose.

Bantleon et al.[2] provided empirical evidence for these structural weaknesses in a peer-reviewed study published in the *International Journal of Auditing*. Their survey of Chief Audit Executives across Austria, Germany, and Switzerland found significant variance in coordination challenges between governance stakeholders, with the second line's focus on stakeholder management creating a silo mentality that leads to duplication of risk areas, gaps in coverage, and conflicting assurance opinions reaching the board.

The Financial Stability Institute, a body of the Bank for International Settlements, acknowledged the structural limitations of the three-lines approach as early as 2015,[1] publishing a formal "Four Lines of Defence Model" in response to high-profile banking scandals that had exposed deficiencies in the framework. The FSI's fourth line consists of external auditors and regulatory supervisors, an acknowledgement that the internal three lines are insufficient but a response that adds periodic external assurance rather than continuous adversarial challenge. The structural gap identified by the FSI remains open.

3.3.2. The Operational Reality

The academic critique is reinforced by the operational reality of how the second and third lines function in practice.

Internal audit (the third line) currently spends an average of 75% of its time on routine assurance work‖, including compliance audits, SOX testing, and regulatory obligations. Budget trajectories are deteriorating. Only 23% of internal audit functions received budget increases in 2025, down from 34% the previous year.[32] The third line is structurally consumed by retrospective assurance. It does not have the bandwidth, the mandate, or in many cases the skills to perform forward-looking, adversarial challenge.

‖based on a North America focused survey from IIA

Risk management (the second line) faces an equivalent constraint. The PwC Global Risk Survey[59] found that 73% of risk functions report funding constraints for emerging-risk identification and 75% for advanced monitoring capabilities. The EY Institute of International Finance Global Bank Risk Management Survey 2025[19] (covering 115 banks across 45 countries) found that CRO mandates have expanded significantly to cover AI governance, cyber resilience, ESG, and operational resilience, with no proportional increase in resources. The second line is consumed by monitoring, regulatory reporting, and issue remediation. Strategic, adversarial analysis goes unperformed, not because it is unwanted but because there is no capacity for it.

3.3.3. The Structural Gap

The Three Lines Model was designed for layered assurance. In practice, it produces three lines that are each occupied with their own mandates, with management focused on execution, risk and compliance on monitoring, and internal audit on retrospective review. Between these lines, in the space where continuous, adversarial, forward-looking challenge of governance and strategy should occur, there is a structural gap.

The gap is architectural. Expanding internal audit budgets or hiring additional risk analysts addresses resource constraints within the existing framework; it does not create the function the framework was never designed to include, one whose explicit, full-time purpose is to challenge assumptions, stress-test decisions, and surface failure modes at board level before they materialise.

Structural Defect 3: Absence of Institutionalised Challenge

The dominant governance architecture, the Three Lines Model, provides assurance but not challenge. No permanent function exists in most organisations whose mandate is to act as a structured, adversarial, continuous counterweight to management narratives, board consensus, and governance complacency. Internal audit looks backward. Risk management monitors the present. Nobody is mandated to simulate the future.

3.4. The Three Defects as a Unified Diagnosis

The three structural defects are interconnected and mutually reinforcing.

Episodic engagement means that boards engage with risk only at intervals, processing whatever information management presents during those intervals. **Consensus dependency** means that when they do engage, their decision-making is subject to noise, anchoring, and social pressure that bias outcomes toward agreement with the prevailing narrative. **Absence of institutionalised challenge** means that no function exists to counteract either defect, no mechanism to ensure that engagement is continuous rather than periodic, that decisions are stress-tested rather than consensual, and that governance architecture itself is subjected to adversarial scrutiny.

The result is a governance system that is extensive in its architecture, diligent in its process, and frequently ineffective in its outcomes. It is a system that produces comfort rather than challenge, assurance rather than resilience, and compliance rather than insight.

These defects compound in sequence. Each enables the next in a descending spiral. Episodic engagement creates dormancy between board cycles, rendering the structural gap invisible. Consensus then hardens unchecked into cognitive capture. Agreement feels like rigour; episodic engagement feels sufficient. The cycle restarts from a worse

position. Figure 1 illustrates this dynamic.

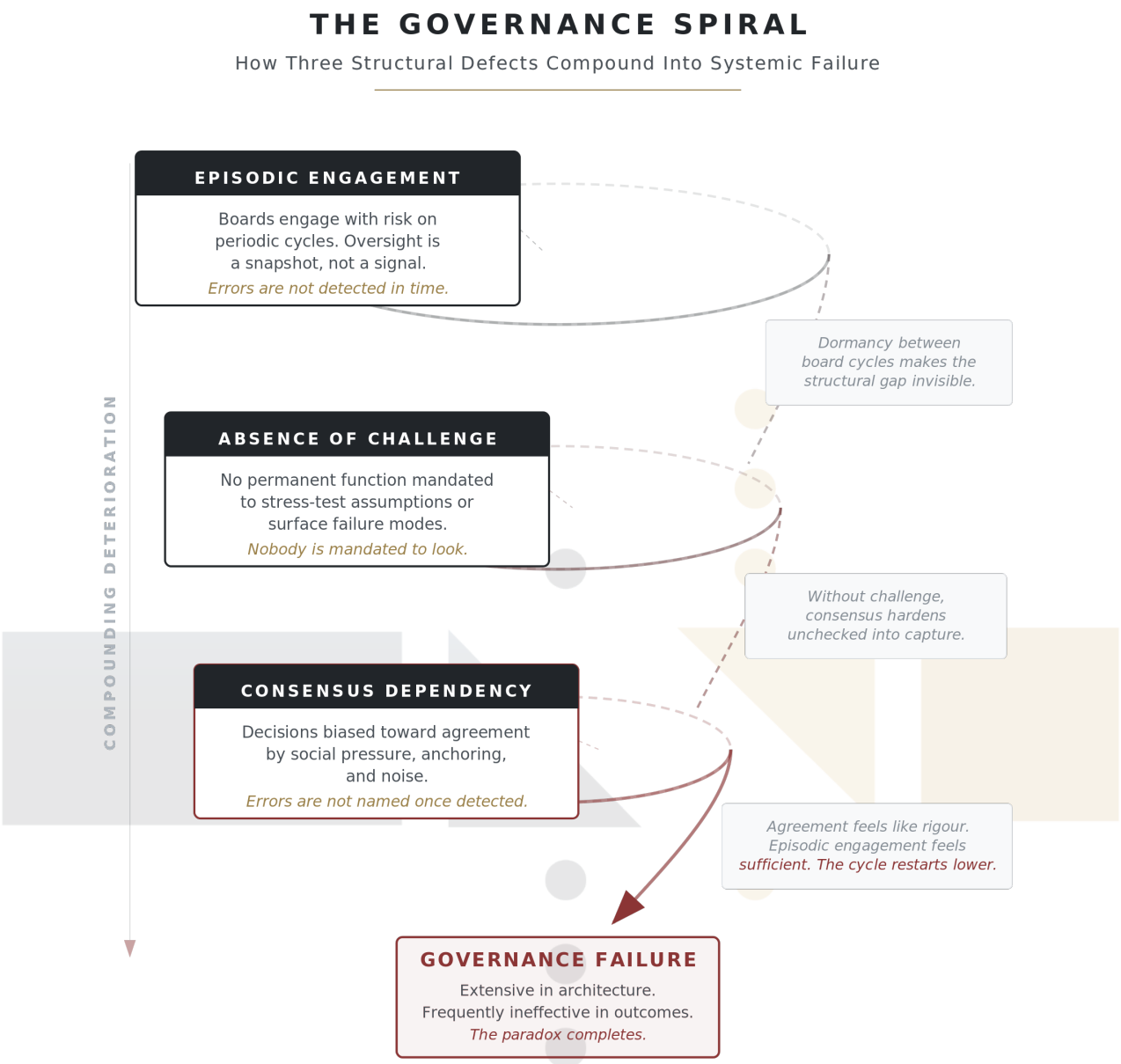


Figure 1. The governance spiral: how the three structural defects compound into systemic failure. Episodic oversight enables architectural absence, architectural absence permits unchallenged consensus, and consensus removes urgency for continuous engagement. Each revolution restarts from a worse position.

Structural Defect	Theoretical Basis	Manifestation	What Is Required
Episodic Engagement	Simon: Bounded Rationality (1947/1957); Kahneman: System 1/System 2 (2011)	Boards engage with risk quarterly or annually; oversight is a snapshot, not a signal	Continuous oversight: a function that monitors and challenges between board cycles
Consensus Dependency	Kahneman, Sibony & Sunstein: Noise (2021); the 55% variability finding	Board decisions biased toward agreement; noise hidden by the comfort of consensus	Decision hygiene: structured, adversarial challenge that forces independent, evidence-based judgement
Absence of Challenge	Power: Organized Uncertainty (2007); Bantleon et al. (2021); FSI Fourth Line paper (2015)	No function mandated to break assumptions, simulate failure, or challenge governance architecture	An institutionalised challenge function: permanent, adversarial, principal-led, operating at board level

Table 3. The three structural defects of governance: theoretical basis, manifestation, and response required

The rightmost column of Table 3 describes three requirements: continuous oversight, adversarial decision hygiene, and an institutionalised challenge function. These are not separate prescriptions. They are different facets of a single architectural response.

The following sections trace these defects through documented case evidence, regulatory convergence, and the value gap in the Three Lines Model.

4 The Evidence of Failure

The three structural defects are not abstractions. They have surfaced repeatedly and observably, in some of the most consequential governance failures of the past two decades.

This section examines five cases: Boeing 737 MAX, Wirecard, Silicon Valley Bank, Credit Suisse and The Post Office Horizon scandal. Each has been subject to public inquiry, regulatory post-mortem, legal proceedings, or some combination of all three. The governance failures in each case are matters of record, not inference.

> **A note on counterfactuals.** This paper does not claim that any governance intervention would have prevented these failures. It claims something more modest and more defensible, that a continuous, adversarial challenge function, operating with independence, access, and a mandate to stress-test assumptions, could have changed the information available to decision-makers, and might have changed the timing and nature of their response. The counterfactual offers option value, not certainty.

4.1. Boeing 737 MAX: The Absence of Safety at Board Level

On 29 October 2018, Lion Air Flight 610 crashed into the Java Sea, killing all 189 passengers and crew. Less than five months later, on 10 March 2019, Ethiopian Airlines Flight 302 crashed near Addis Ababa, killing all 157 on board. Both crashes were caused by the same system, the Maneuvering Characteristics Augmentation System, or MCAS, a flight-control software designed to prevent aerodynamic stall by automatically pushing the aircraft's nose down. In both accidents, MCAS activated erroneously based on data from a single faulty angle-of-attack sensor and pushed the nose down repeatedly, a failure mode that Boeing's safety analysis had not adequately considered.

A U.S. House Committee investigation[69] found systemic failures in Boeing's design process and the FAA's delegation of certification authority. Boeing had been permitted to certify the majority of its own work through the FAA's Organization Designation Authorization programme, creating an inherent conflict of interest in which the manufacturer was, in effect, its own regulator.

4.1.1. The governance failure.

The Boeing board's failure was not primarily one of competence. It was a failure of architecture. Prior to August 2019, after both crashes, no Boeing board committee charter assigned responsibility for aircraft safety oversight.[11,69] Safety, the most mission-critical risk in commercial aviation, sat outside the governance framework entirely. When a Boeing engineer wrote to factory leaders in the summer of 2018, "I'm sorry to say that I'm hesitant about putting my family on a Boeing airplane,"[69] no mechanism existed for that concern to reach the board.

After the first crash, Boeing management waited ten days before notifying the board. The CEO then reported that the 737 MAX was safe. At the February 2019 board meeting, one month before the second crash, the board decided to defer any internal investigation to regulatory processes, even though several directors were aware of internal communications

concerning MCAS deficiencies and the withholding of information from the FAA.

The consequences were extraordinary. Three hundred and forty-six people died. Boeing agreed to a $2.5 billion settlement with the U.S. Department of Justice in January 2021,[68] with additional settlements totalling $1.1 billion in 2025. The board paid $237.5 million to settle a Caremark derivative claim,[11] the largest Caremark cash settlement in Delaware Chancery Court history, based on the court's finding that the board had failed to monitor a "mission critical" operational risk.

4.1.2. Mapping to the structural defects.

Episodic engagement. The board engaged with aircraft safety only after catastrophic failure. Between scheduled board meetings, safety-critical concerns, including the engineer's warning and the MCAS design evolution, were filtered through management channels that had every incentive to minimise them. Oversight was periodic but the risk was continuous.

Consensus dependency. The board deferred to management's reassurance that the aircraft was safe and to the FAA's certification process. The consensus, between management, the regulator, and the board, that the 737 MAX was airworthy was accepted without independent, adversarial examination. When the consensus was wrong, 346 people paid the price.

Absence of institutionalised challenge. No function existed to challenge the board's assumption that safety could be left outside committee charters. No mechanism existed for technical experts to escalate safety concerns directly to the board. No structured process subjected MCAS design assumptions to adversarial review at governance level.

The Counterfactual

A continuous challenge function with a mandate to review governance architecture might have identified the absence of safety from board committee charters as a structural defect before either crash. A red team protocol applied to the MCAS programme might have surfaced the single-sensor dependency and repeated-activation failure mode that Boeing's own safety analysis missed. None of this guarantees a different outcome, but it changes the information available to decision-makers, and the timing at which it arrives.

4.1.3. The Caremark significance.

The Boeing settlement extended the Caremark doctrine in a direction with profound implications for governance. In *In re Caremark* (1996),[9] the Delaware Chancery Court established that directors have a duty to implement information and reporting systems. In *Marchand v. Barnhill* (2019),[12] the Delaware Supreme Court held that the board of ice cream manufacturer Blue Bell had breached its Caremark duties by failing to monitor food safety, a "mission critical" risk. Boeing confirmed the principle:[11] boards can be held liable for failing to build governance architecture around their organisation's most critical operational risks, an extension beyond traditional compliance monitoring.

The trajectory is clear. Courts are no longer asking whether boards had governance frameworks. They are asking whether those frameworks were designed to address the risks that actually mattered.

4.2. Wirecard: When Every Line of Defence Fails Simultaneously

On 18 June 2020, Wirecard AG announced that €1.9 billion in cash balances, purportedly held in trustee accounts in the Philippines, could not be verified. Four days later, the company admitted that the funds "probably never existed." Three days after that, Wirecard filed for insolvency. The company's share price, which had peaked at a market capitalisation of approximately €24 billion following its entry to the DAX 30 in September 2018, collapsed to near-zero within days.

Wirecard is the case in which *every* layer of the governance architecture failed simultaneously. Langenbucher and Leuz[41] identified the collapse of five distinct governance layers, namely internal controls, supervisory board oversight, external audit, auditing oversight bodies, and the market supervisor. The KPMG special investigation,[39] commissioned by Wirecard's own supervisory board, and the subsequent Bundestag parliamentary inquiry[14] documented the scale and mechanism of these failures in detail.

4.2.1. The internal failure.

Wirecard's fraud was sustained through fictitious "Third-Party Acquiring" partnerships in Asia that generated €1.9 billion in fake revenue over five or more years.[39] Internal controls did not detect the fabrication. Risk management rated the trustee account receipts as low risk. Internal audit did not perform independent verification of overseas partner transactions.[14]

4.2.2. The external failure.

EY, Wirecard's external auditor, accepted screenshots and PDF bank statements as evidence of cash balances for three consecutive audit cycles without requesting independent third-party bank confirmations.[14,39] BaFin, the German market supervisor, treated Wirecard as a technology company rather than a financial institution, exempting it from banking-level supervisory scrutiny.[14] When the Financial Times published evidence of fraud, sourced from internal whistleblower Pav Gill, BaFin's response was to file a criminal complaint against the journalists and ban short-selling of Wirecard shares.[14]

4.2.3. The suppression of challenge.

In March 2018, more than two years before the collapse, Gill reported evidence of illegal money flows through Wirecard's Singapore office to COO Jan Marsalek. Marsalek immediately quashed the investigation and removed the whistleblower from the inquiry. Gill was forced to go to external media because internal escalation had been actively suppressed.

4.2.4. Mapping to the structural defects.

Episodic engagement. The supervisory board engaged with Wirecard's Asian operations on a quarterly and annual cycle, processing management presentations that described a high-growth fintech success story. The board did not establish continuous monitoring of the Third-Party Acquiring partnerships that constituted the fraud's mechanism.

Consensus dependency. The consensus, shared across the supervisory board, EY, and BaFin, was that Wirecard was a legitimate technology company disrupting the payments industry. Short-seller reports and journalistic investigations were characterised as motivated attacks rather than evidence requiring investigation. The consensus was so strong that the regulator actively punished those who challenged it.

Absence of institutionalised challenge. Wirecard had no protected mechanism for dissent.

When the whistleblower raised evidence of fraud internally, the function that should have escalated it instead suppressed it. The supervisory board had no independent capability to verify the financial claims on which its oversight depended. No adversarial function existed to stress-test the revenue figures, examine the Asian partnerships, or challenge the narrative that made the supervisory board comfortable.

The Counterfactual

A continuous, adversarial challenge function operating independently of management might have applied fraud-scenario wargaming to the Third-Party Acquiring revenue stream, asking, before any whistleblower came forward, what evidence would be required to confirm that this revenue was real. A structured challenge process might have asked why €1.9 billion in cash sat in Philippine trustee accounts rather than in directly auditable bank deposits. A function with a mandate to protect dissent might have given Pav Gill a route to the supervisory board rather than to the Financial Times.

4.3. Silicon Valley Bank: The Risk That Everyone Saw and Nobody Escalated

Silicon Valley Bank failed on 10 March 2023. The proximate cause was a bank run. Depositors withdrew $42 billion in a single day on 9 March, approximately 25% of total deposits. However, the underlying cause was a governance failure that had been accumulating, visibly, for years. The failure did not remain contained to SVB. Within 48 hours, Signature Bank also failed. First Republic Bank followed in May 2023 with approximately $229 billion in assets, surpassing SVB as the largest U.S. bank failure since Washington Mutual. The cascading crisis spread to Europe, delivering the final blow to Credit Suisse, which became the largest distressed bank rescue in world history.[48]

SVB's business model was built on concentration, with heavy exposure to venture capital deposits, technology-sector clients, and long-duration investment securities. At year-end 2022, the bank held $117 billion in investment securities, approximately 56% of total assets, with roughly $91 billion classified as held-to-maturity, carrying an average duration of approximately six years.[483] This meant that for every 100-basis-point increase in interest rates, the bank faced approximately 6% in unrealised losses on its HTM portfolio. Between March and December 2022, the Federal Reserve raised rates by approximately 425 basis points.[3] By year-end, the bank's unrealised losses on its securities portfolio had reached approximately $17 billion, exceeding its entire book-value equity capital of $15 billion.[48]

The Federal Reserve's post-failure review was unusually candid.[3] It acknowledged that supervisors "did not fully appreciate the extent of the vulnerabilities" at SVB. Fed examiners had identified interest rate risk deficiencies in the 2020, 2021, and 2022 CAMELS examinations but did not issue a formal supervisory finding until November 2022, four months before the bank failed. SVB had received "satisfactory" ratings on management and governance from 2017 through 2021, despite documented weaknesses.[3]

4.3.1. The CRO vacancy.

In April 2022, SVB removed its Chief Risk Officer.[3] The position remained vacant for nine months, from April 2022 to January 2023, during precisely the period in which the Federal Reserve was raising interest rates at the fastest pace in four decades and the bank's unrealised losses were accumulating at extraordinary speed. During the most critical

period of risk exposure in the bank's history, the function responsible for independent risk oversight had no appointed leader.

4.3.2. Mapping to the structural defects.

Episodic engagement. SVB's board engaged with risk on a quarterly cycle, though meetings increased to eighteen annually in 2022. The Federal Reserve Bank of San Francisco examined SVB 26 times and its holding company a further 17 times between February 2018 and March 2023.[52] Neither cadence was sufficient. Between examinations, unrealised losses accumulated continuously. The CRO vacancy meant that no one was continuously monitoring the emerging risk during the most volatile nine months of the bank's existence. The disconnect extended inside the regulator itself. In June 2022, the Federal Reserve Board's own surveillance team issued a special topic report identifying SVB as one of the institutions with the highest levels of unrealised losses in the system and placed it on the Systemwide holding company watch list with a "high adverse change probability" warning.[52] Two months later, the San Francisco examiners responsible for day-to-day supervision of SVB issued a supervisory letter describing the bank's balance sheet structure as *mitigating* the risks associated with its rapid growth.[52] The Board's analytical function caught the risk. The examination function, operating on its own periodic cycle, did not act on it.

Consensus dependency. The consensus, shared between SVB management, the board, and the Federal Reserve, was that SVB's concentration in venture capital deposits was a strategic advantage rather than a systemic risk. Management's assurance that interest rate risk was manageable through liability management was accepted without independent verification. The FDIC's subsequent civil lawsuit against 17 former SVB directors and officers alleges that this was not passive complacency. According to the FDIC's complaint, management "repeatedly breached its own interest-rate risk policies and metrics" and then "manipulated assumptions in one of the risk models to cover up the breaches".[20,73] The complaint further alleges that management removed interest-rate hedges on the securities portfolio to boost short-term profits, increasing the bank's exposure at the precise moment rates were rising, and approved dividends to the parent company months before the bank failed.[20] Neither the board nor the regulator challenged any of these actions. If the allegations are substantiated, the consensus provided cover for the active concealment of internal policy violations.

Absence of institutionalised challenge. During the nine-month CRO vacancy, no formal mechanism existed for independent risk escalation to the board. Fed examiners identified the interest rate risk deficiency three years running but did not escalate their findings to a formal supervisory action until it was too late. The cost to the FDIC's Deposit Insurance Fund was an estimated $16.1 billion.

The quantified regulatory record makes the absence of challenge measurable. The Basel Committee's interest-rate risk in the banking book (IRRBB) standard, implemented in the United Kingdom, Canada, and the Euro area but never fully adopted in the United States, would have identified SVB's asset-liability strategy as an outlier requiring remedial action *ten quarters* before the bank failed.[21] The liquidity coverage ratio (LCR), from which U.S. regulators had explicitly exempted banks of SVB's size, would have required the bank to hold tens of billions of dollars more liquidity *four quarters* before failure. Had SVB been subject to the Basel Committee's total loss-absorbing capacity (TLAC) standard, the FDIC would have saved an estimated $13.6 billion.[21] The risk was quantifiably actionable more than two years before the bank collapsed, under standards that peer jurisdictions already applied.

The Counterfactual

A continuous challenge function might have identified the CRO vacancy as a governance defect requiring immediate board escalation, rather than allowing it to persist for nine months. A pre-mortem diagnostic applied to SVB's interest rate exposure might have asked: "If rates rise 400 basis points in twelve months, what happens to this portfolio?" A structured adversarial review with access to internal risk reports might have identified what the FDIC now alleges, namely that management removed interest-rate hedges not to manage risk but to boost short-term earnings, and that subsequent changes to risk model assumptions were concealing, rather than correcting, breaches of the bank's own policies.[20] The risk was visible in SVB's own financial statements, quantifiably actionable under established Basel standards more than two years before failure,[21] and flagged by the Federal Reserve's own surveillance team eight months before the collapse.[52] What *was* missing was a function mandated to ensure that visible risks received commensurate governance attention.

4.4. Credit Suisse: The Limits of Internal Reform

On 19 March 2023, Credit Suisse ceased to exist as an independent institution after 167 years. The Swiss government, the Swiss National Bank, and FINMA negotiated a forced merger with UBS over a single weekend, mobilising CHF 259 billion in liquidity support and loss guarantees to prevent uncontrolled failure.

The proximate cause was a deposit run. In the fourth quarter of 2022, clients withdrew CHF 138 billion in deposits from a base of approximately CHF 370 billion held at the end of Q3, the largest share leaving in October as media speculation and loss of client confidence reinforced each other.[64] Over the same three months, the wealth and asset management businesses recorded CHF 111 billion in net asset outflows, closing a year that totalled CHF 123 billion in AUM outflows. A few short months later, the bank was gone.

The underlying cause was not a 2023 event. The Swiss Financial Market Supervisory Authority's post-failure review[64] traces the failure to a decade of governance reform that could not establish substance. Successive interventions, new chief executives, new chief risk officers, new chairs, new committee structures, did not change how Credit Suisse made decisions. By the fourth quarter of 2022, eleven of the thirteen members of the Executive Board had been newly appointed within a short period. Senior management was unable, FINMA concludes, "to reinforce the risk culture throughout the bank in a significant and sustainable manner."[64] Repeated changes in senior personnel had not successfully addressed the shortcomings of the underlying architecture.

4.4.1. The governance failure.

FINMA identifies a cluster of structural defects. Risk appetite limits and accountability for risks taken were "often not clear enough, namely in the allocation between the front-office units and the control functions".[64] The corporate structure was complex enough to prevent "clear allocation of responsibilities and thus rigorous decision-making." The Chair of the Risk Committee departed in April 2021, leaving an interim dual-reporting arrangement that contributed to documented breaches of supervisory obligations across the Archegos, Greensill, and Mozambique exposures.[64]

The pattern is consistent across each documented loss event. Risk was visible inside the firm. Internal challenge functions reported into the same chain of authority that had created the exposure. The architecture preserved the form of governance, the committees,

the charters, the reporting lines, while the substance, the willingness and capacity to challenge consensus, eroded. By the time market confidence broke in October 2022, the governance machinery had been failing for years.

4.4.2. Mapping to the structural defects.

Episodic engagement. Credit Suisse engaged with risk through scheduled board cycles and the supervisory cycle imposed by FINMA. Between cycles, exposures accumulated and warning signals propagated through internal channels that had every incentive to filter them. The Archegos and Greensill events were not failures of risk identification at the desk level; they were failures of escalation and accountability at the architecture level. Each event, examined post-hoc, surfaced structural weaknesses that had been visible to internal participants long before they reached the board.

Consensus dependency. The consensus, sustained across two decades of management changes, was that Credit Suisse's governance challenges were a personnel problem. New chief executives, new chief risk officers, and new chairs were appointed on the expectation that fresh leadership would restore discipline. FINMA's finding contradicts the premise. The issue was not the people occupying the roles but the architecture that determined what the roles could achieve. The consensus that internal reform would suffice survived every operational loss until the deposit run made it unsustainable.

Absence of institutionalised challenge. Credit Suisse had a Risk Committee, internal audit, compliance, a Chief Risk Officer, and external auditors. None operated outside the chain of authority they were meant to challenge. When the Risk Committee Chair departed in April 2021, the interim arrangement created the very dual-reporting opacity that FINMA later identified as a contributing factor to the supervisory breaches at Archegos, Greensill, and Mozambique. No function existed at board level whose mandate was independent challenge, independent of management, independent of the chain of appointments, and independent of the consensus its presence was meant to test.

The Credit Suisse case is the clearest illustration in this paper of the limit of internal reform. Twelve years and four chief executives could not establish what FINMA calls "tone from the top" because the function tasked with tone was always inside the organisation it was meant to challenge.

4.5. Post Office Horizon: Twenty Years of Institutional Consensus Against Individual Evidence

The Post Office Horizon scandal is the longest-running governance failure examined in this paper, and arguably the most instructive. It demonstrates what happens when institutional consensus is maintained, unchallenged, for two decades, and when the people who could have broken that consensus had no route to decision-makers.

Beginning in 1999, Fujitsu's Horizon IT system was deployed across Post Office branches throughout the United Kingdom. The system contained software bugs that caused discrepancies in branch accounts. These discrepancies were attributed not to the technology but to the sub-postmasters who operated the branches. Between 1999 and 2015, over 900 sub-postmasters were prosecuted for theft, fraud, and false accounting, approximately 700 of those prosecutions conducted by The Post Office itself.[74] At least 236 individuals were imprisoned.

The human cost defies summary. Sub-postmasters lost their livelihoods, their homes, and their reputations. Families were destroyed. At least thirteen people took their own lives.[74]

The Criminal Cases Review Commission[8] subsequently described the Horizon cases as the "most widespread miscarriage of justice" in its history, the largest single series of wrongful convictions in British legal history. In May 2024, Parliament passed the Post Office (Horizon System) Offences Act 2024,[70] quashing convictions en masse. As of March 2026, over £1.44 billion in compensation had been paid out, with more than 11,300 individual claimants identified.

4.5.1. The governance failure.

The Post Office board did not establish independent verification of the Horizon system's reliability despite accumulating reports of errors. It accepted management's assurance that the system was robust without commissioning independent technical audit. It had no mechanism to review criminal prosecution decisions. The authority to prosecute sub-postmasters was delegated to an operations team with a financial incentive to preserve the Horizon narrative, since the cost of admitting system failure would have been enormous.

Fujitsu's role compounded the failure. Fujitsu employees gave evidence in court that the Horizon system was "robust" and "could not have caused" the shortfalls for which sub-postmasters were being prosecuted, despite internal knowledge of software bugs dating to the system's deployment. The Post Office Horizon System Inquiry,[74] chaired by Sir Wyn Williams, documented systematic failures spanning more than two decades across Post Office management, legal counsel, Fujitsu, and government oversight.

4.5.2. Mapping to the structural defects.

Episodic engagement. The Post Office board engaged with the Horizon system at its initial deployment and thereafter episodically, through annual reports and management summaries rather than through continuous monitoring of system reliability. No real-time feedback mechanism existed between the sub-postmasters who used the system daily and the board responsible for overseeing it. For twenty years, the board's understanding of Horizon was mediated entirely through management.

Consensus dependency. The organisational consensus, that the system was reliable and that discrepancies were caused by dishonest individuals, was shared across management, the board, legal counsel, the external auditor, and the government department responsible for Post Office oversight. This consensus held for more than two decades despite hundreds of sub-postmasters independently reporting the same types of errors. The pattern was not invisible. It was visible and dismissed. The ITV drama *Mr Bates vs The Post Office*, broadcast in January 2024, generated the first sustained public attention the scandal had received in twenty-five years, a measure of how effectively institutional consensus can suppress individual evidence.

Absence of institutionalised challenge. No function existed within The Post Office to independently verify the Horizon system's accuracy. No protected mechanism existed for sub-postmasters to escalate system errors to the board. No independent technical committee assessed system reliability. Complaints were filtered through management channels with every incentive to suppress them. The legal function, rather than protecting the accused's right to challenge system reliability, actively supported the prosecution narrative.

The Counterfactual

A continuous challenge function might have identified, within the first years of deployment, that hundreds of independent operators reporting identical types of shortfalls constituted a statistical anomaly requiring investigation rather than prosecution. A structured adversarial review of the Horizon system might have asked: "What evidence exists that this system is accurate, independent of the vendor's own assertions?" A function with a mandate to provide adversarial challenge might have given sub-postmasters concerns more visibility to the board. The Post Office scandal is the clearest illustration in this paper of the cost of consensus without challenge, twenty years of institutional certainty, and the lives broken by it.

4.6. Patterns Across the Evidence

Five cases spanning aviation, financial technology, US regional banking, Swiss systemic banking, and public services. Four jurisdictions, five industries, and, in each case, the same three structural defects operating in recognisable patterns.

	Boeing 737 MAX	Wirecard	Silicon Valley Bank	Credit Suisse	Post Office Horizon
Episodic Engagement	Safety not monitored between board cycles; engineer's warning filtered through management	Quarterly engagement; no real-time monitoring of Asian partnerships that constituted the fraud	Annual/quarterly exams insufficient; nine-month CRO vacancy during peak risk period	Scheduled cycles only; Archegos and Greensill exposures escalated late through filtered internal channels	Initial deployment then episodic annual oversight; no continuous feedback from system users
Consensus Dependency	Board deferred to management and FAA consensus; "aircraft is safe" accepted without challenge	Board, EY, and BaFin shared consensus; short-sellers punished for dissent	Fed and board consensus: "satisfactory" ratings despite documented weaknesses (2017–2021)	Two-decade consensus that governance failure was a personnel problem; survived every operational loss until the deposit run	System "robust" consensus held for 20+ years; hundreds of individual reports dismissed
Absence of Challenge	No committee charter covered safety; no escalation channel for engineers	Whistleblower suppressed; no adversarial review of revenue claims	No independent escalation during CRO vacancy; Fed findings not escalated as urgent	All challenge functions internal to the chain of authority; Risk Committee Chair gap from April 2021	No independent technical audit; no protected channel for sub-postmasters or staff
Consequences	346 deaths; >$3.8 billion in settlements; $237.5M Caremark claim	€1.9B fabricated; €24B market value destroyed; criminal proceedings ongoing	$42B bank run; $16.1B FDIC cost; second-largest US bank failure at the time; third after First Republic (May 2023)	CHF 138B Q4 deposit run; CHF 123B annual AUM outflow; CHF 259B state support; forced merger with UBS	900+ wrongful prosecutions; 236+ imprisoned; £1B+ in compensation; 13+ suicides

Table 4. Structural defects mapped across five governance failure case studies

Several observations emerge from this mapping.

First, every organisation that failed had a governance framework. Boeing had board committees. Wirecard had a supervisory board, external auditors, and a market regulator. SVB was supervised by the Federal Reserve. Credit Suisse was supervised by FINMA and operated a Risk Committee, internal audit, compliance, and a Chief Risk Officer. The Post Office was overseen by a government department. In every case, the architecture existed and was insufficient to surface the risks that destroyed value, lives, or both.

Second, the warnings existed. In each case, information that could have changed the trajectory was available before catastrophe struck. Boeing's engineers raised concerns.

Wirecard's whistleblower reported fraud. SVB's interest rate exposure was visible in its public filings. Credit Suisse's risk culture failures were documented across the Archegos, Greensill, and Mozambique exposures. Hundreds of sub-postmasters reported Horizon errors over two decades. The problem was not that the signals did not exist, it was that no function was mandated to receive them, analyse them adversarially, and escalate them to decision-makers with the authority to act.

Third, consensus was the mechanism of failure. In each case, the prevailing narrative ("the aircraft is safe," "the company is a fintech success," "the bank's model is sound," "the new leadership will restore discipline," "the system is robust") was maintained by consensus long after evidence to the contrary was available. Consensus is not inherently dangerous, but without a structured mechanism for challenge, consensus becomes the means by which organisations convince themselves that what is comfortable is also true.

Fourth, the cost of inaction dwarfs the cost of challenge. The cumulative direct financial cost of these five cases exceeds $50 billion, before accounting for the CHF 259 billion in Swiss state intervention required to prevent uncontrolled failure of Credit Suisse, the human cost of 346 aviation deaths, the destruction of over 900 livelihoods, and the broader systemic effects. The cost of a continuous, adversarial challenge function operating at board level is a fraction of the value at risk.

Fifth, these cases are the extremes, not the norm. The failures examined here sit at the catastrophic end of a distribution. As Section 2 established, the more common manifestation of the same structural defects is strategic drift, the failed acquisition that was never stress-tested, the technological pivot that the board discussed but never mandated, the slow erosion of competitive position that no function was tasked with challenging. The Hunziker et al. data confirms that eight in ten value-destroying corporate crises originate in strategy and external-risk categories, not in the preventable-risk space that compliance governance targets. The case studies above demonstrate what unchecked structural defects produce at their terminal extreme. For most organisations, the defects operate at lower amplitude but with the same mechanism, namely episodic oversight that misses evolving risk, consensus that suppresses challenge, and an absence of any function mandated to ask whether the current strategy still holds. The economic case (Section 11) is built on both, the catastrophic tail and the chronic middle.

Sixth, the establishment voice now confirms the pattern. The Committee of Sponsoring Organizations of the Treadway Commission, the consortium that authored the dominant ERM framework cited above, conceded the diagnosis directly in 2026.[43] A global survey of risk leaders reported in COSO's *From Guidance to Action* found that 54% of ERM programmes are perceived as compliance or assurance functions, 28% as strategic partners, only 7% are fully integrated into strategy decisions, and 98% of respondents believe ERM should play a more strategic role. COSO frames the recurring failure mode as "scoring theater" and reports that registers, heat maps, and self-assessments consume significant effort without affecting choices. The case studies in this section are the catastrophic terminus of that pattern. The COSO data quantifies the chronic middle, the organisations operating on the same defective architecture without yet generating a public failure event.

The next sections turn from evidence to response, examining the regulatory convergence and the value gap that together create the structural space for a new function.

5 The Regulatory Direction

Regulators are converging on requirements the current model cannot meet. Across multiple jurisdictions, independently and without coordination, regulatory frameworks are moving toward continuous oversight, adversarial testing, personal accountability, and independent challenge. Regulators are not using the language of Strategic Governance as a Service. But the direction of travel is unmistakable.

Independent regulators, responding to the same evidence, have converged on the same set of requirements without coordination. The evidence they share is consistent. Governance frameworks that looked complete on paper failed in practice. The result is a regulatory environment that is, progressively and from multiple directions, creating the conditions in which a continuous, adversarial, independent governance function is structurally necessary.

5.1. The UK Corporate Governance Code: From Periodic Establishment to Continuous Maintenance

The Financial Reporting Council published the updated UK Corporate Governance Code,[23] effective 1 January 2025. The revisions are, in places, linguistically subtle while structurally they are anything but.

Principle O, the foundation of the Code's risk and controls framework, was revised to require that boards not merely "establish" but "maintain" effective risk management and internal control frameworks. The addition of "maintain" is a shift from a one-time act of design to a continuous obligation of oversight. It implies that a board which builds a framework and then relies on periodic review is no longer meeting the Code's expectations.

Provision 28 was revised to require boards to explain the procedures they have in place for identifying and managing emerging risks (risks that do not yet appear on conventional risk registers and may not yet have a defined owner). This is a requirement for forward-looking, horizon-scanning governance, precisely the kind of activity that is crowded out when the second and third lines are consumed by monitoring and retrospective assurance.

Most significantly, Provision 29 (effective 1 January 2026) requires boards to make an annual declaration on the effectiveness of the organisation's material internal controls. The scope is explicit, covering financial, operational, reporting, and compliance controls. It extends well beyond financial reporting. Boards must take personal, public ownership of control effectiveness across all four dimensions of the business.

The practical implication is that boards will need independently validated evidence that their material controls are effective. The question the Code implicitly raises, and does not answer, is: who provides that independent validation on a continuous basis, across the full scope of material controls, with a mandate that extends beyond the retrospective assurance provided by internal audit?

5.2. The Caremark Doctrine: From Compliance to Mission-Critical Risk

While the UK's governance evolution is principles-based, the United States has developed a parallel, and in some respects more consequential, trajectory through case law. The Caremark doctrine, originating in a 1996 Delaware Chancery Court decision, has evolved over three decades from a narrow compliance-monitoring duty into an expansive fiduciary obligation that now reaches the heart of operational governance.

The original *In re Caremark* decision (1996) established that directors have a duty to implement information and reporting systems. *Stone v. Ritter* (2006)[13] affirmed and codified this as a two-prong test, under which liability arises where directors either utterly fail to implement any reporting system, or, having implemented one, consciously fail to monitor its operation.

For over two decades, Caremark claims were virtually impossible for plaintiffs to win. The doctrine was real but dormant. That changed in 2019.

Marchand v. Barnhill (2019) revitalised the doctrine in a case involving Blue Bell Creameries, an ice cream manufacturer whose products were linked to a listeria outbreak. The Delaware Supreme Court held that the board had breached its Caremark duties by failing to monitor food safety, an operational risk that was "mission critical" to the company's business, extending the oversight obligation beyond legal compliance. The court introduced a new principle. Where a risk is intrinsically critical to the company's operations, the board's oversight obligation is heightened.

Boeing confirmed and extended *Marchand*. The $237.5 million Caremark cash settlement (the largest in Delaware history) was based on the finding that Boeing's board had established no committee-level oversight of aircraft safety, the single most mission-critical operational risk in commercial aviation.

In January 2023, the Delaware Court of Chancery took the doctrine further still. In *In re McDonald's Corporation* (2023),[10] the court extended Caremark duties from directors to corporate officers. The standard is identical. Officers face personal liability for bad-faith failure to oversee matters within their remit. The effect is to create personal accountability at every level of the governance hierarchy for mission-critical oversight.

> **The trajectory.** Caremark has evolved from a duty to build compliance systems (1996) to a duty to monitor those systems (2006) to a duty to build governance architecture specifically around mission-critical operational risks (2019–2022) to personal officer-level liability for oversight failures (2023). The direction is consistent. Courts are no longer asking whether boards had governance frameworks. They are asking whether those frameworks were designed to address the risks that actually mattered and whether anyone was mandated to challenge the assumption that they did.

5.3. DORA: The Adversarial Principle in Regulation

The European Union's Digital Operational Resilience Act,[18] fully effective from 17 January 2025, introduces a regulatory concept with implications beyond its immediate scope, namely the principle that critical functions should be subjected to structured, adversarial challenge as a governance-level control.

DORA requires significant financial entities to conduct threat-led penetration testing (TLPT)

of critical IT functions at least every three years, based on bespoke threat intelligence tailored to the entity's risk profile. The framework aligns with the European Central Bank's TIBER-EU methodology, which provides governance-level guidance on red teaming as a structured control framework.

An epistemological distinction is necessary. DORA's TLPT operates in the technical domain. A penetration test either breaches a system's defences or it does not. The outcome is empirically verifiable. Strategic governance challenge operates in a different domain. A board's M&A thesis, its technology investment case, or its strategic assumptions about competitive positioning cannot be empirically broken before the fact. What can be tested is not the assumption itself but the quality of evidence supporting it, in particular whether the proxies are weak, the reasoning motivated, or the cognitive biases documented in Section 3 are operating on the decision. Technical testing delivers a binary verdict. Strategic falsification delivers a calibrated assessment of evidentiary fragility.

The significance of DORA for this paper's argument lies not in a claim of equivalence between technical and strategic testing. It lies in the regulatory recognition that critical functions should be subjected to structured adversarial scrutiny, not as a voluntary exercise in risk maturity, but as a governance obligation. The governance function that oversees it is accountable for ensuring that the testing produces actionable intelligence. That principle, the principle that adversarial challenge is a governance-level control, applies with equal force in the strategic domain, where the consequences of unchallenged assumptions are no less severe and the evidentiary basis is often more fragile.

DORA applies to credit institutions, investment firms, payment institutions, insurance undertakings, and other financial entities across the EU. Its TLPT requirement applies to systemically significant entities. The principle it embeds, that critical functions require structured adversarial scrutiny, extends naturally from technical infrastructure to strategic governance, provided the epistemological distinction is maintained. SGaaS maintains it. The methodology described in Section 9 applies Popperian falsification to governance assumptions, dismantling the evidence that supports strategic positions rather than claiming to break the positions themselves.

5.4. SM&CR: Personal Accountability as a Governance Accelerant

The UK's Senior Managers and Certification Regime,[22] implemented progressively from March 2016 for banks and building societies and extended to all FCA-regulated firms from December 2019, represents a different dimension of the regulatory convergence, the creation of personal consequences for governance failure.

Under SM&CR, each Senior Management Function holder has a statutory Duty of Responsibility. If the firm breaches a regulatory requirement, the senior manager responsible for that area faces personal enforcement action unless they can demonstrate they took "reasonable steps" to prevent or stop the breach. The burden is on the individual and the consequences are personal, including financial penalties, restrictions, and reputational damage that follow the individual personally.

SM&CR does not prescribe how senior managers should discharge their duty, nor does it mandate any particular governance structure. What it creates is a powerful incentive (or more precisely, a powerful fear) that drives demand for demonstrable, independently validated governance assurance. A senior manager whose Statement of Responsibilities includes risk oversight has a personal interest in ensuring that an independent function is continuously challenging the governance framework within which they operate. If

the framework fails, "I relied on internal audit's annual assurance" may not satisfy the "reasonable steps" test. "I commissioned continuous, adversarial, independent review and acted on the findings" is a materially stronger defence.

The FCA and PRA initiated a review of SM&CR in March 2023, examining whether the regime adequately promotes governance accountability and challenge functions. The review signals regulatory awareness that personal accountability, while necessary, may not be sufficient without the structural governance mechanisms that give senior managers the information they need to discharge their duties.

5.5. Operational Resilience: From Risk Registers to Disruption Tolerances

A further dimension of convergence is visible in the operational resilience frameworks emerging across multiple jurisdictions. These frameworks share a common departure from traditional risk management. They ask organisations to go beyond listing risks and quantify their tolerance for disruption, and to demonstrate, continuously, that they can operate within those tolerances.

In the UK, the PRA and FCA's operational resilience rules required firms to demonstrate by 31 March 2025 that they can operate within defined impact tolerances for their important business services. This is a fundamentally different governance requirement from maintaining a risk register. It requires boards to make quantified commitments about the maximum disruption their organisation can withstand and to test, on an ongoing basis, whether their operations would remain within those bounds under adverse conditions.

In Australia, APRA's Prudential Standard CPS 230, effective 1 July 2025, establishes that the board is "ultimately accountable" for operational risk management. The standard requires boards to set disruption tolerances for critical operations, approve business continuity plans, and continuously monitor operational risk profiles.

In Canada, OSFI's Guideline E-21, published in final form in August 2024, mandates continuous monitoring, reporting, and escalation of operational risks to the board, with disruption tolerances set and actively monitored at board level.

The pattern is consistent across jurisdictions. Regulators are requiring boards to move from passive receipt of periodic assurance reports to active, continuous governance of operational resilience. The boards that can demonstrate this level of oversight (with independent validation and adversarial challenge) will satisfy regulatory expectations. Those that continue to rely on periodic internal assurance will face increasing scrutiny.

5.6. The Wider Convergence

The regulatory developments described above are not isolated. They are part of a broader, multi-jurisdictional convergence toward the same set of governance requirements.

The Basel Committee's Corporate Governance Principles for Banks (BCBS 328) require independent risk management functions with sufficient stature to challenge business line decisions, direct reporting to the board, and explicit authority to escalate risk concerns without management veto.

The EU's Corporate Sustainability Due Diligence Directive,[15] entered into force in July 2024, extends board-level accountability to human rights and environmental risks across the entire value chain, requiring continuous identification and assessment of impacts that

go far beyond traditional financial governance. Member states are required to transpose the Directive into national law by July 2026, with phased applicability for companies by size thereafter.

The SEC's cybersecurity governance rules, evolving since 2023, require public companies to disclose board-level cybersecurity oversight practices and the processes through which the board oversees cybersecurity risk, creating strong practical incentives for boards to receive regular briefings on risk assessments and tabletop exercises.

The Japan Financial Services Agency's Corporate Governance Reform 2025 principles[24] require boards to "persistently assess the appropriateness of current allocation of resources" and strengthens board independence.

The Monetary Authority of Singapore[51] updated its outsourcing notices in December 2023 to mandate board-level governance frameworks for third-party risk with continuous executive oversight.

Regulatory Requirement	Jurisdictions	Traditional Response	Structural Requirement
Continuous oversight of risk and controls	UK (Principle O), Australia (CPS 230), Canada (E-21), Singapore (MAS)	Quarterly board reports; annual risk review	A function providing continuous, real-time governance intelligence to the board
Adversarial testing of critical functions	EU (DORA TLPT), ECB (TIBER-EU), SEC (tabletop exercises)	Periodic technical penetration testing; compliance audits	Structured adversarial challenge extended from technical infrastructure to strategic governance assumptions through falsification of evidentiary support
Mission-critical risk governance architecture	US (Caremark: Marchand, Boeing, McDonald's), UK (Provision 29)	Generic risk committee with broad remit	Dedicated governance architecture around the organisation's most consequential risks
Personal accountability for oversight	UK (SM&CR), US (Caremark officer liability), Australia (CPS 230 board accountability)	Collective board responsibility; "I wasn't told" defence	Demonstrable evidence that the individual took reasonable steps, including commissioning independent challenge
Independent challenge functions	BCBS 328, FSI Fourth Line, UK SM&CR, APRA CPS 230	Internal audit's periodic assurance	A permanent, independent function mandated to challenge management narratives and board assumptions

Table 5. Multi-jurisdictional regulatory convergence: requirements, traditional responses, and structural gaps

The convergence is not only regulatory. The Committee of Sponsoring Organizations of the Treadway Commission, the consortium of the AAA, AICPA, FEI, IMA, and IIA whose 2017 framework defines the global ERM standard, published *From Guidance to Action* in 2026.[43] The paper restates the requirement that risk management be embedded in strategy and

decision rhythms rather than reported alongside them, and concedes that most ERM programmes produce documentation without affecting choices. The framework authors have therefore moved, on their own analysis, from the assurance-centric model toward the continuous, decision-led, adversarially tested governance the regulatory developments above are converging on. The direction of travel is regulatory and normative at the same time.

5.7. What Regulators Are Asking For and What Does Not Yet Exist

The regulatory convergence described in this section creates a set of requirements that are clear in their direction and challenging in their implementation.

Regulators are asking for continuous, not periodic, governance oversight. They are requiring adversarial testing of critical functions and assumptions. They are creating personal accountability for governance failures at board and officer level. They are demanding independent challenge functions with the authority to escalate without management veto. And they are extending governance obligations beyond financial compliance to mission-critical operational risks across the full scope of the business.

These requirements describe a function that does not currently exist within most organisations' governance architecture. Internal audit provides retrospective assurance. Risk management monitors the present, but often does not have the bandwidth to look to the future. External audit provides periodic certification. The board itself meets periodically and is remote from day to day business activity.

The Financial Stability Institute recognised this structural gap as early as 2015,[1] proposing a "fourth line of defence" to supplement the three-lines model. But the FSI's fourth line consisted of external auditors and regulatory supervisors, entities that provide additional periodic assurance rather than the continuous, adversarial, principal-led challenge that regulators are now, by logical implication, increasingly requiring.

> **The regulatory gap.** Regulators across multiple jurisdictions are converging on a consistent set of governance requirements: continuous oversight, adversarial challenge, mission-critical risk architecture, personal accountability, and independent escalation. These requirements describe a function that the existing governance architecture (the Three Lines Model, supplemented by external audit and regulatory supervision) was not designed to provide. The regulatory direction is clear and this paper proposes a structural response: Strategic Governance as a Service.

The following sections examine the value gap this creates and the structural response it demands.

6 The Value Gap in the Three Lines Model

Internal audit spends 75% of its time on routine assurance.[31] This single statistic captures the value gap at the heart of the Three Lines Model. The model, updated by the Institute of Internal Auditors in July 2020, remains the dominant governance architecture in medium-to-large organisations. Its structural limitations were examined theoretically in Section 3. This section examines the empirical reality, the measurable gap between what the second and third lines are asked to do and what they have the capacity to deliver.

The Three Lines Model does what it was designed to do. The problem is that what it was designed to do, layered assurance in an environment of bounded complexity, falls short of what the current risk environment demands, where risk velocity, regulatory volume, and stakeholder expectations have long outpaced its design assumptions. The characterisation is not rhetorical. The World Economic Forum's Global Risks Report,[75] drawing on the Global Risks Perception Survey of over 1,300 senior risk experts, names the defining feature of the current environment as "the accelerating scale, interconnectedness and speed of global risks" and frames 2026 as "an age of competition". The Three Lines Model, last revised by the Institute of Internal Auditors in July 2020, was not designed for that environment. The result is a value gap, a structural space between what governance functions are mandated to provide and what they can actually deliver, that no existing function fills.

6.1. The Third Line: Internal Audit's Capacity Trap

Internal audit, the third line, occupies a paradoxical position in most organisations. It is mandated to provide independent assurance to the board. It is increasingly expected to deliver strategic advisory services, forward-looking risk assessment, and insights on emerging threats. And it spends three-quarters of its time doing neither.

The IIA's Vision 2035 report,[31] based on a survey of over 7,000 respondents, found that internal audit currently allocates an average of 75% of its capacity to routine assurance work, including compliance audits, Sarbanes-Oxley testing, and regulatory obligations. The remaining 25% encompasses everything else, including advisory work, strategic risk assessment, emerging risk identification, and stakeholder engagement. The IIA's own target is to shift this balance to 59% assurance and 41% advisory by 2035. That target implicitly acknowledges that the current allocation is failing to deliver the value that stakeholders require.

For functions with SOX responsibilities, the constraint is even more acute. Only 15% of their time is allocated to advisory work.[31] SOX compliance, by its nature, is retrospective, process-driven, and non-negotiable. It consumes capacity with limited room for strategic reallocation. Yet 55% of CFOs and 50% of audit committees report that they want more risk-focused work from internal audit. The demand exists, but the capacity does not.

The resource trajectory is deteriorating. The 2025 North American Pulse of Internal Audit[32] found that only 23% of internal audit functions received budget increases, down from 34% the previous year, and 19% reported outright cuts. Simultaneously, 42% of functions report lacking the skill sets they need, with data analytics, cybersecurity, and AI governance cited as the most critical gaps.

The result is a function that is simultaneously over-committed and under-resourced. Internal audit cannot perform routine assurance, strategic advisory, emerging risk identification, and continuous governance challenge with 75% of its capacity locked in compliance cycles and shrinking budgets. Something has to give, and what gives is the forward-looking, adversarial, strategic work that boards and regulators are increasingly demanding.

The outsourcing data confirms the structural nature of the gap. A KPMG SOX survey[40] found that 58% of organisations rely on outsourced providers for more than 20% of their SOX programme efforts, a structural dependence on external resources to perform work that internal functions cannot absorb. The outsourcing addresses routine compliance, not strategic challenge.

> **The capacity trap.** Internal audit is asked to be a trusted strategic advisor to the board while spending 75% of its time on routine assurance, operating with shrinking budgets, and lacking the skills its stakeholders demand. The IIA's own 2035 target acknowledges the problem. But even if the target is met, and current budget trajectories suggest it will not be, a 59/41 split still leaves no dedicated capacity for continuous, adversarial, board-level governance challenge. The capacity trap is an architectural problem, not simply a resourcing one.

6.2. The Second Line: Mandate Expansion Without Capacity

If internal audit's problem is a capacity trap, the second line, risk management and compliance, faces an equivalent challenge from the opposite direction, an expanding mandate with no proportional increase in resources.

A PwC Global Risk Survey[59] found that 73% of risk functions report funding constraints for emerging-risk identification, and 75% lack sufficient funding for advanced monitoring capabilities. These are not requests for incremental improvement. Emerging-risk identification and advanced monitoring are core components of what regulators are now requiring (as Section 5 demonstrated). Yet three-quarters of risk functions report that they cannot afford to do the work regulators are demanding.

An EY and Institute of International Finance survey,[19] covering 115 banks across 45 countries, found that CRO mandates have expanded significantly to encompass AI governance, cyber resilience, ESG, and operational resilience, risk categories that barely existed a decade ago and now command board attention. The survey found no proportional increase in resources.

The operational reality of the second line in most organisations is a function consumed by monitoring, regulatory reporting, issue remediation, and maintaining risk registers. These activities are necessary. They are also largely backward-looking or present-focused. Strategic, forward-looking analysis of governance architecture, decision-making quality, and systemic failure modes goes unperformed, not because it is unwanted, but because there is no capacity for it after the mandatory work is complete.

The consequence is a second line that satisfies regulatory expectations for risk monitoring while leaving the board without the strategic risk intelligence it needs. Boards receive risk reports. They do not receive adversarial challenge of the assumptions those reports are built on.

6.3. Between the Lines: Coordination Failures and Information Loss

Coordination failures between the lines compound the gap beyond what any individual line's shortfall would suggest.

Bantleon et al.[2] lay out these coordination challenges empirically in a peer-reviewed study covering Chief Audit Executives across Austria, Germany, and Switzerland. Their detailed work paints a picture of governance architecture operating in silos rather than as an integrated system, with inconsistent and multiple reporting to the board, gaps in risk coverage between the lines, siloed risk functions duplicating effort in some areas while leaving others unmonitored, business fatigue from overlapping requests, confusion about the organisation's aggregate risk profile, and layers of redundant controls that add cost without adding assurance.

The IIA itself acknowledged these structural weaknesses in its 2020 revision,[33] noting that the original model's "defence" framing had reinforced separation rather than collaboration, and that role ambiguity from overlapping responsibilities had blurred accountability. The revision emphasised that "independence does not imply isolation." But the structural incentives of the model, where each line reports through different channels, operates on different cycles, and measures success by different metrics, continue to produce the isolation the revision sought to address.

Academic critics have gone further. The "defence" terminology, as several scholars have noted, implies a reactive, compliance-driven posture focused on protection rather than on proactive risk-taking and resilience. It fosters what Power[56] has characterised as a "tick-box mentality", a focus on demonstrating compliance with process rather than delivering substance.

In cybersecurity governance, the coordination failure is particularly acute. Internal auditors typically review cyber-risk components annually on three-to-five-year audit cycles, a cadence that hinders internal audit's capacity to provide comprehensive and timely assessment in an environment where threats evolve daily. The gap between the velocity of cyber risk and the periodicity of third-line assurance is structural. The model was designed for an environment where risk moved slowly enough to be reviewed on annual cycles. Cyber threats do not.

6.4. The Board Perspective: What Is Expected and What Is Delivered

Research on board risk reporting consistently finds a persistent disconnect between what boards receive and what they need. In practice, risk reporting for many boards amounts to standardised templates of backward-looking data with limited forward-looking situational analysis. Boards receive data. They do not receive the contextualised, adversarial analysis that would enable them to challenge management narratives and test governance assumptions.

The advisory industry reached the same conclusion over a decade earlier. In a 2010 McKinsey working paper written for boards, Brodeur et al.[6] asked why risk processes had failed to raise the alarm during the 2008 financial crisis and identified three structural reasons: the risk assessments "often miss large company-wide risks; they do not uncover the fundamental drivers of the large risks identified; and they fail to consider how multiple risks can operate in tandem." The authors' conclusion was unambiguous: "such processes

fail to generate insight that management or boards can act on." The defect is that the reports the second and third lines produce, by the advisory industry's own assessment, do not give boards what boards need.

The same paper is equally direct on where risk oversight should sit within the board. Brodeur et al.[6] observed that many directors park risk oversight with the audit committee and stated that this is "likely a mistake, and might result from a deep-seated underestimation of the value and importance of risk oversight to the company's performance and health. It could also result from a too-casual working definition of risk, leading directors to confuse the audit committee's compliance-related approach to risk with a true ERM approach." McKinsey, in 2010, was telling boards that parking risk with the audit committee produces a compliance frame rather than a risk frame, and that the two are categorically different. The architectural critique this paper advances is not a fringe position. It has been the advisory industry's own diagnosis for over a decade.

AI governance provides a present-day test of whether that diagnosis has been acted on, and it is clear it has not. A Deloitte survey,[44] covering 695 board members and C-suite executives across 56 countries in January and February 2025, found that 31% of boards do not have AI on the agenda at all. Only 17% address it at every meeting; 19% take it up once a year. The pattern is episodic by any definition. And it is not explained by indifference. Some 53% of respondents say their organisations need to accelerate AI adoption, and only 3% consider AI irrelevant. The board recognises the strategic weight of AI. The governance architecture does not equip it to oversee AI continuously. Sixteen years after McKinsey told boards their oversight was superficial, the most commercially significant emerging technology is governed on an annual or semi-annual cycle by two-thirds of respondent boards.

The framework authors have now confirmed the same diagnosis. COSO, the consortium of the AAA, AICPA, FEI, IMA, and IIA whose 2017 framework defines the global ERM standard, published *From Guidance to Action* in 2026.[43] A global survey of risk leaders reported in that paper found that 54% of ERM programmes are perceived as compliance or assurance functions, 28% as strategic partners, and only 7% are fully integrated into strategy decisions. Yet 98% of respondents believe ERM should play a more strategic role. The 7%-to-98% spread measures the value gap in COSO's own data. The diagnosis is therefore consistent across the consortium that authored the framework, the firms that most frequently advise on its implementation, and the boards on the receiving end of its outputs. What is missing is not awareness of the gap. It is a function whose explicit mandate is to close it.

The expectations gap extends to the relationship between audit committees and internal audit leadership. Audit committee chairs consistently report that they expect their Chief Audit Executive to be a "trusted advisor", someone comfortable sharing perspectives informally, raising uncomfortable truths, and providing strategic insight beyond the audit plan. Yet practitioners acknowledge that "there is often an unfortunate gap between audit committee expectations and internal audit's performance."[49]

The result is predictable. Organisations that cannot obtain strategic governance intelligence from their internal functions turn to external providers. Big Four advisory revenues have surpassed their audit services revenues since the mid-2010s,** with the consulting segment growing rapidly across all four firms as demand for AI governance and transformation advisory has accelerated.

**Based on individual firm revenue disclosures. Advisory and consulting lines now exceed assurance revenues for each of the four firms.

Michael Power's analysis in *Organized Uncertainty* provides the theoretical frame for this dynamic. Organisations invest heavily in demonstrating accountability for risks, the apparatus of governance, rather than in reducing actual risk exposure. The Three Lines Model produces assurance reports, risk registers, and audit opinions. What it does not produce, because this fell outside its design mandate, is continuous, adversarial intelligence about whether the governance framework itself is functioning as intended.

6.5. The Automation Paradox: Technology That Could Free Capacity But Hasn't

A reasonable objection to the value gap argument is that technology should be solving it. Robotic process automation can perform routine audit work such as reconciliations, confirmations, and document reviews at speeds substantially faster than manual processes, enabling full-population testing rather than statistical sampling. AI adoption among internal auditors is expected to double significantly over the next two years.[31] Continuous auditing has been adopted by a growing minority of firms,[32] with further adoption planned.

If these technologies were deployed at scale, they could, in principle, free 30–40% of the capacity currently consumed by routine assurance work. That freed capacity could be redirected toward the advisory, strategic, and challenge functions that stakeholders demand.

In practice, this has not happened. The barriers are organisational rather than purely technological. Internal audit functions lack the data science and AI skills required to implement and govern these tools. The technology exists, but organisational capability to deploy, validate, and maintain it at scale has not kept up with the pace of technical development.

This creates what might be called the automation paradox. The tools to release capacity from routine work are available, but the skills required to use those tools are the same skills the function lacks for its strategic mandate. Automation highlights the value gap rather than resolving it.

The paradox extends beyond the audit function to the board itself. A Deloitte survey,[44] covering 695 board members and C-suite executives across 56 countries in early 2025, found that only 12% of boards engage with their Chief Risk Officer on AI, compared with 72% who engage with the CIO or CTO.[44] The board discusses AI as a technology opportunity through the technology function, not as a risk-bearing strategic commitment through the risk function. Deloitte's companion research on generative AI enterprise adoption[44] reinforces the point. Organisational preparedness in technology infrastructure and strategy has improved, but preparedness has not improved in the critical area of risk and governance.

The gap requires the right people, with the right mandate and the right independence, to perform work of a fundamentally different character to anything in the existing lines.

6.6. The Structural Space: What the Value Gap Creates

The evidence presented in this section describes a governance architecture with a measurable and widening gap between mandate and capacity.

The rightmost column of Table 6 describes a consistent gap across every dimension of the governance architecture, namely the absence of a function that provides continuous,

Function	Mandate	Operational Reality	Gap
Third Line (Internal Audit)	Independent assurance; strategic advisory; emerging risk identification; continuous governance intelligence	75% on routine assurance; 15–21% advisory; shrinking budgets; 42% skill gaps; 3–5 year audit cycles for cyber	No capacity for continuous, forward-looking, adversarial challenge at board level
Second Line (Risk & Compliance)	Risk monitoring; emerging-risk identification; advanced analytics; strategic risk intelligence	73–75% funding constraints; CRO mandates expanding without resources; 61% talent barriers; consumed by monitoring and reporting	No capacity for adversarial stress-testing of governance assumptions and strategic decisions
Coordination (Between Lines)	Integrated risk coverage; consistent reporting; unified risk profile; efficient resource allocation	Silos; duplicated effort; gaps in coverage; inconsistent reporting; business fatigue; confusion on aggregate risk	No function mandated to ensure the governance architecture itself is coordinated, complete, and effective
Board Interface	Contextualised, forward-looking, adversarial governance intelligence; trusted advisory relationship	Stale data in standardised templates; expectations gap between audit committees and IA leadership	No function providing the continuous, challenging, strategic governance insight boards require

Table 6. The Three Lines value gap: mandate, operational reality, and the missing function

adversarial, forward-looking governance challenge at board level.

This is not a gap that can be closed by expanding internal audit budgets, hiring additional risk analysts, or deploying automation. These measures address resource constraints within the existing architecture. The gap is architectural. The Three Lines Model does not include a function whose explicit, full-time, permanent mandate is to challenge the governance framework itself, to ask whether the assurance is real, whether the risk intelligence is complete, whether the coordination is effective, and whether the board is receiving what it needs rather than what the existing functions are configured to produce.

The Financial Stability Institute recognised this gap in 2015, proposing a fourth line of defence.[1] But the FSI's fourth line consisted of external auditors and regulatory supervisors, entities that add periodic assurance rather than continuous challenge. The gap the FSI identified remains open.

The value gap thesis

The value gap thesis. The Three Lines Model was designed for layered assurance in a governance environment of bounded complexity. It now operates in an environment where risk velocity, regulatory volume, and stakeholder expectations exceed its design capacity. The result is a structural gap between what governance functions are mandated to provide and what they can deliver, a gap that is architectural rather than incremental, and one that no existing function within the model fills. This is the structural space that Strategic Governance as a Service occupies.

Section 8 defines the function that can fill it.

7 Why Traditional Advisory Models Under-Deliver

A natural question follows from the preceding analysis. If a structural gap exists between assurance and adversarial challenge, why hasn't the established multi-centi billion dollar management consulting market closed it?

The global management consulting market exceeds USD 700 billion annually. Big Four advisory revenues alone surpassed their traditional audit services revenues around 2014 and have continued to grow. Governance, risk, and compliance advisory is one of the fastest-growing segments. Organisations are clearly spending money on external governance support. Yet the structural gap persists.

The gap persists by design. Traditional advisory models are built in ways that reproduce the same structural defects that cause governance failure rather than resolve them.

7.1. The Episodic Engagement Problem

The dominant model for governance advisory is project-based. A firm identifies a governance concern, commissions an external review, receives a report, implements recommendations, and the engagement ends. Average engagement duration for governance and risk advisory projects ranges from eight to sixteen weeks, and fewer than 15% extend beyond six months.

This model is, by design, episodic. The consultancy team arrives, analyses, recommends, and departs. Between engagements, the organisation's governance environment continues to evolve. New risks emerge, strategic decisions are taken, board composition changes, and regulatory requirements shift. The consultant has no visibility into these changes. When the next engagement begins, if there is one, the consultant must rebuild context from scratch, often with an entirely different set of team members.

The structural defect this reproduces is obvious. Section 3 identified episodic engagement as the first of three governance defects, the tendency for boards to engage with risk only at intervals, processing whatever is presented during those intervals. Project-based consulting operates on the same model. It provides a snapshot of governance effectiveness at a point in time, not a continuous signal. The value of the snapshot degrades from the moment the engagement ends.

The FSI's fourth line of defence (external audit and regulatory supervision) operates on the same episodic logic. Annual audit cycles, periodic regulatory examinations, and project-based consulting reviews all share a common architectural limitation. They provide assurance at intervals in a world where risk is continuous.

7.2. The Institutional Memory Problem

A governance review conducted over twelve weeks generates deep understanding of the organisation's culture, power dynamics, information flows, decision-making patterns, and structural vulnerabilities. This understanding lives in the minds of the consulting team. It

is not transferable in a report. Reports capture findings and recommendations. They do not capture the pattern recognition, contextual judgement, and relational knowledge that informed those findings.

The consequence is a perpetual restart. Each new engagement begins with weeks of context-building. Each new consulting team must learn what the previous team learned and forgot. The organisation pays, repeatedly, for the same discovery process.

A continuous governance function, by contrast, accumulates institutional memory. It observes how decisions are made over quarters and years, not weeks. It tracks whether recommendations are implemented, diluted, or quietly abandoned. It notices when the same structural weaknesses recur under different labels. This cumulative knowledge is one of the most valuable assets a governance challenge function can build, and it is, by definition, unavailable to a project-based engagement model.

7.3. The Consensus Incentive

Section 3 identified consensus dependency as the second structural defect of governance, the tendency for board decisions to be biased toward agreement, amplified by social pressure, anchoring, and the comfort of collective assent. Traditional advisory models are subject to this defect rather than counteracting it.

The commercial reality of consulting is that engagements end and relationships continue. A consulting firm that delivers findings uncomfortable to management risks losing future engagements. A firm that challenges the board's preferred narrative risks being perceived as adversarial rather than collaborative. The incentive structure favours findings that are rigorous enough to be credible but palatable enough to be acceptable.

Bazerman, Morgan, and Loewenstein[4] demonstrated that self-serving bias is unconscious and structural. Even well-intentioned professionals cannot fully eliminate the influence of financial relationships on their professional judgement. The effect requires no conscious corruption to operate. The effect is that the commercial relationship creates a gravitational pull toward consensus, toward findings that the client can accept without disruption.

For the Big Four specifically, the incentive is compounded. These firms provide audit, advisory, tax, and consulting services to overlapping client bases. While independence restrictions limit the advisory services an audit firm can provide to its audit clients, the broader commercial incentive to maintain multi-service relationships remains. A governance advisory engagement that produces findings challenging to the audit relationship creates institutional tension. The structural pressure, however subtle, is toward findings that preserve the overall commercial ecosystem.

An adversarial governance function requires the opposite incentive structure. Its value lies precisely in its willingness to surface uncomfortable truths, challenge prevailing narratives, and report findings that management may not welcome. This requires structural independence from the commercial dynamics that govern project-based advisory, an independence that is easier to design into a retained, principal-led model than into a fee-per-engagement one.

7.4. The Prescription and the Delivery Model

The clearest evidence that traditional advisory cannot close the governance gap comes from traditional advisory itself. In 2010, four McKinsey partners published a board-facing working paper that prescribed, with considerable precision, the capabilities boards require,

namely continuous integration of risk into strategic planning and capital allocation; a risk dialogue "centered on specific business issues, rather than a discussion of high-level generalities"; direct board interaction with the handful of executives who understand the key risks best; a "board culture that promotes dialogue and constructive challenge"; and identification of the three to five "big bets" on which the organisation actually depends.[6] These are the operating capabilities the authors identify as the difference between governance that works and governance that does not.

Every capability on that list is continuous, specific, and relational. None of them can be delivered through a twelve-week engagement by a rotating team of consultants on a deliverable-based billing model. The prescription and the commercial model are architecturally incompatible. The advisory industry has been able to describe what boards need for over fifteen years. It has not been able to sell it, because the capabilities it prescribes cannot be packaged as projects, scoped as deliverables, or priced by the hour.

The pattern repeats in 2025, with a different firm and a different risk domain but the same structural contradiction. A Deloitte survey[44] covering 695 board members and C-suite executives across 56 countries concluded that boards must oversee AI strategy execution and risk management continuously, "challenging management to identify when and how the strategy may need to be adapted in response to risks and opportunities". The report prescribes seven thematic areas of permanent board-level inquiry, namely strategy, risk appetite, governance structure, board education, performance measurement, talent, and culture. Each requires sustained engagement, not a periodic check-in. Yet the vehicle for the prescription is a Deloitte Global Boardroom Program survey report, a deliverable that boards read once and file. Deloitte, like McKinsey fifteen years earlier, prescribes an architectural capability from a commercial position that delivers episodic advisory. The gap between what the advisory industry prescribes for boards and what it is structurally able to deliver is the gap that SGaaS is designed to close, through a commercial model (retained, principal-led, independent, outside the audit-tax-consulting ecosystem) that is compatible with the continuous adversarial capabilities the prescription requires.

The pattern repeats a third time, in 2026, with a non-commercial author and the same architectural contradiction. COSO's *From Guidance to Action*,[43] written by the framework consortium of the AAA, AICPA, FEI, IMA, and IIA, prescribes an ERM operating system built from forums where risk-informed decisions are actually made, a cadence aligned to operating reviews, triggers that convert awareness into action, and short, decision-ready artefacts that travel with the schedule. The prescription is the same continuous, embedded, decision-led discipline McKinsey described in 2010 and Deloitte described in 2025. The author this time is the consortium that wrote the framework rather than a firm that sells advisory hours. The delivery vehicle is, once again, a published report that boards read once and file. Even the framework authors cannot escape the architectural problem. They can articulate what good ERM looks like; they cannot deliver it. The ERM operating system COSO describes does not exist as a product, and the same paper's fallback proposal of a five-hour-a-week minimum operating rhythm for resource-constrained risk leaders is a tacit admission that internal capacity is structurally insufficient. The prescription has now been issued by a consultancy, by a peer consultancy, and by the framework consortium itself. None of the three has been able to deliver it. SGaaS is the delivery vehicle the prescription requires.

7.5. The Deliverable Substitution Problem

Michael Power's concept of "organised uncertainty"[56] describes a dynamic in which organisations substitute auditable artefacts for substantive assurance (the appearance of control for its reality). Project-based advisory is particularly susceptible to this substitution.

A governance review produces a report. The board receives the report, notes the findings, and approves the recommendations. It then files the report. The *report* becomes the evidence of governance, the artefact that demonstrates the board took action. Whether the recommendations are implemented, whether the implementation is effective, and whether the governance environment has changed since the report was written are questions the report cannot answer and the consulting engagement does not address.

Kahneman, Sibony, and Sunstein's work on decision hygiene reinforces the point. Reducing noise in professional judgement requires sustained, structured, repeated intervention, not a one-off diagnostic. A single governance review can identify problems. It cannot sustain the decision discipline required to prevent them from recurring. That requires continuous presence, not periodic visitation.

7.6. The Structural Comparison

The following table maps the three structural defects identified in Section 3 against the traditional advisory model and the requirements for a function that could address the value gap.

Dimension	Traditional Advisory	Structural Defect Reproduced	What Is Required
Engagement model	Project-based; 8–16 weeks; defined deliverable; engagement ends	Episodic engagement: snapshot governance in a world of continuous risk	Continuous, retained engagement with ongoing access, visibility, and accountability
Institutional memory	Knowledge leaves with the team; each engagement restarts context-building	No longitudinal intelligence; governance history lost between engagements	Cumulative knowledge of organisational culture, decision patterns, and governance dynamics
Independence	Commercial incentive to maintain client relationships; self-serving bias (Bazerman et al.)	Consensus dependency: findings gravitationally pulled toward palatability	Structural independence from commercial dynamics; mandate to challenge, not to please
Deliverable	Report, framework, or set of recommendations; filed after presentation	Deliverable substitution: the report becomes the artefact of governance, not its substance	Continuous intelligence feed; ongoing challenge and accountability for implementation
Challenge function	Advisory: recommends improvements within client's preferred parameters	Absence of institutionalised challenge: no mandate to break assumptions or stress-test decisions	Adversarial by design: mandated to surface failure modes, challenge narratives, and simulate scenarios the organisation prefers not to consider

Table 7. Traditional advisory models mapped against the three structural governance defects

The pattern is consistent. Traditional advisory models reproduce the same structural defects, including episodic engagement, consensus dependency, and absence of institutionalised challenge. These are root causes of governance failure. They address governance symptoms through periodic intervention rather than governance architecture through continuous presence.

7.7. What the Gap Requires

The regulatory direction described in Section 5 makes the inadequacy of traditional models increasingly consequential. Provision 29 of the UK Corporate Governance Code requires

boards to declare on the effectiveness of material internal controls across financial, operational, reporting, and compliance dimensions. This requires continuous evidence, not periodic review. The Caremark doctrine requires governance architecture specifically around mission-critical risks. This requires permanent structural commitment for which project-based intervention will not work. SM&CR creates personal accountability for senior managers. This requires demonstrable evidence of "reasonable steps". A twelve-week consulting engagement, however excellent its report, may not provide this evidence.

The gap requires a function that is:

Core Principle

Continuous: Present across board cycles, not between engagements.
Adversarial: Mandated to challenge, not to recommend within acceptable parameters.
Independent: Structurally separated from the incentives that pull findings toward consensus.
Cumulative: Building institutional memory of governance dynamics over time, not restarting context with each engagement.
Principal-led: Delivered by experienced governance professionals, not by teams of junior analysts supervised remotely by a partner.

Section 8 defines this function and gives it a name.

8 Defining Strategic Governance as a Service

If the problem is structural, the response must be structural. The preceding sections have documented the defects, the evidence, the regulatory convergence, and the value gap. This section defines the response.

8.1. The Formal Definition

Definition

Strategic Governance as a Service (SGaaS) is a continuous, adversarial, principal-led governance function, delivered at board level on a retained basis, whose mandate is to challenge assumptions, stress-test decisions, and surface failure modes in governance architecture before they materialise as organisational loss.
SGaaS carries authority to challenge rather than merely advising. It operates continuously rather than episodically. It is human-led rather than platform-delivered. And it complements rather than replaces internal governance functions, occupying the structural gap between the lines that the existing architecture was never designed to fill.

This definition rests on five design principles, each of which responds directly to the structural defects and evidence presented in this paper.

Continuous: SGaaS operates on a retained basis across board cycles, rather than sporadic project engagements. It accumulates institutional memory of the organisation's governance dynamics, decision patterns, and risk evolution over quarters and years. It addresses the first structural defect, episodic engagement, by ensuring that governance challenge is always present, not periodically available.

Adversarial: SGaaS challenges, not confining recommendations within parameters inoffensive to the consensus. Its methodology is grounded in structured adversarial techniques (red teaming, scenario simulation, pre-mortem analysis) that force organisations to confront the assumptions they would prefer not to examine. It addresses the second structural defect, consensus dependency, by providing the decision hygiene function that Kahneman, Sibony, and Sunstein identified[35] as essential to reducing noise in professional judgement.

Principal-led: SGaaS is delivered by experienced governance professionals operating at board level, not by teams of junior analysts supervised remotely. The principal is the engagement. They build the relationships, develop the institutional knowledge, and carry the authority to challenge effectively. The model is deliberately craft-based, and its value depends on the quality and seniority of the principal. The analytical work, assumption mapping, document review, adversarial scenario construction, and coordination with the second and third lines, is conducted asynchronously by the principal alongside the organisation's existing governance rhythm. The board receives distilled, high-signal adversarial intelligence, not raw analytical burden. The cognitive load on part-time directors is managed by design. The methodology asks them to commit independent positions and engage

in structured debate, not to conduct the red team exercise themselves.

Independent: SGaaS operates outside the incentive structures that compromise traditional advisory independence. It is structurally separated from audit, assurance, and multi-service commercial relationships. Its mandate is to surface uncomfortable truths, not to protect client relationships across adjacent service lines. It addresses the third structural defect, the absence of institutionalised challenge, by creating a function whose independence is architectural, not aspirational.

Complementary: SGaaS does not replace internal audit, risk management, compliance, or any other governance function. It occupies the space between them, the value gap documented in Section 6, performing the continuous, adversarial, forward-looking work that overstretched internal functions cannot deliver. It works alongside the Three Lines Model, not instead of it.

8.2. Distinguishing SGaaS from Existing Models

The term "Governance as a Service" is already used in IT, cybersecurity, and data governance markets, typically describing compliance monitoring platforms, outsourced policy management, or cloud-based governance dashboards. Strategic Governance as a Service is a fundamentally different concept. The distinction rests on four pillars.

Pillar	Existing GaaS Market	Strategic Governance as a Service
Scope	IT compliance, data governance, cybersecurity controls, policy management	Board-level strategic risk and governance architecture
Delivery	Advisory, technology platform, or outsourced operations; typically delivered by junior teams	Principal-led: the provider operates at CRO level with authority to challenge board and management
Methodology	Compliance monitoring, framework assessment, control testing, training	Adversarial by design: red teaming, risk simulation, pre-mortem diagnostics
Commercial model	Project fees, SaaS subscription, or hourly rates; engagement ends when deliverable is complete	Tiered retainer architecture designed for continuity, progression, and cumulative institutional knowledge

Table 8. Strategic Governance as a Service distinguished from existing GaaS market offerings

The distinction matters. Compliance-focused GaaS platforms address whether an organisation's IT policies meet a defined standard. Strategic Governance as a Service addresses whether the organisation's governance architecture is capable of preventing catastrophic failure. These are different problems, requiring different methodologies, different seniority of engagement, and fundamentally different commercial structures.

8.3. Relationship to the Three Lines Model

Section 6 documented a structural gap in the Three Lines Model, a space between the assurance the model provides and the adversarial challenge that boards, regulators, and fiduciary law require. SGaaS occupies that gap.

It is important to be precise about what SGaaS is *not* within the governance architecture. It is not a fourth line of defence. The Financial Stability Institute proposed a fourth line in 2015,[1] consisting of external auditors and regulatory supervisors. That proposal adds

periodic external assurance to the architecture. SGaaS adds something different, namely continuous, adversarial, internal-facing challenge that operates alongside the existing three lines.

The first line (management) owns risk. The second line (risk and compliance) monitors risk. The third line (internal audit) provides assurance. SGaaS challenges. It challenges the assumptions underlying management's risk decisions, the completeness of the second line's monitoring, the rigour of the third line's assurance, and the effectiveness of the governance architecture that connects them.

This distinction matters operationally. Internal audit functions are sometimes concerned that external governance services may encroach on their mandate. SGaaS explicitly does not. It produces no audit opinions, performs no compliance testing, and issues no assurance reports. It produces challenge, namely structured, adversarial, documented challenge that is designed to make the existing lines more effective, not to replace them.

SGaaS also differs from the networked governance models proposed by governance theorists who have recognised the same structural gap. Shann Turnbull's "Watchdog Board" concept[38] envisions a permanent internal supervisory body with independent information channels and veto power over decisions that could harm stakeholders. John Carver's Policy Governance method separates "ends" (outcomes) from "means" (methods), with the board governing proscriptively, defining what management may not do rather than prescribing what it must. Both frameworks recognise the need for institutionalised challenge. SGaaS provides the same functional outcome through a different architectural response, one that is external and retained rather than internally constituted, principal-led rather than committee-based, and deployable within existing governance frameworks without requiring changes to articles of association, board composition, or regulatory approval. The two approaches are not mutually exclusive. SGaaS can serve as a bridge, providing the challenge function immediately while an organisation builds toward deeper structural change if appropriate.

8.4. Theoretical Foundations

SGaaS rests on established theoretical foundations, each addressing a specific structural defect.

From bounded rationality to continuous oversight. Herbert Simon demonstrated that decision-makers under conditions of cognitive constraint satisfice rather than optimise. Boards, operating part-time with limited information and processing capacity, are structurally prone to accepting the first adequate option rather than seeking the best. SGaaS counteracts this by maintaining continuous governance intelligence across board cycles, ensuring that the information environment in which directors satisfice is as complete, current, and adversarially tested as possible.

From noise to decision hygiene. Kahneman, Sibony, and Sunstein demonstrated that professional judgement exhibits far greater variability than professionals believe, and that reducing this noise requires structured processes (decision hygiene) applied consistently over time. SGaaS operationalises this through its adversarial methodology. The Mediating Assessments Protocol's requirement for independent, evidence-based judgement before group synthesis is the theoretical ancestor of SGaaS's red teaming and pre-mortem techniques.

From organised uncertainty to substantive challenge. Michael Power demonstrated that governance frameworks tend to produce the appearance of control rather than its

substance, rituals of verification that satisfy the need for demonstrable accountability without necessarily reducing risk. SGaaS is designed to be the function that breaks through the ritual, not another layer of assurance, but a challenge to the assurance itself.

From requisite variety to architectural design. W. Ross Ashby's Law of Requisite Variety, a foundational principle of cybernetics, states that a control system must possess at least as much variety (complexity, response capacity) as the system it seeks to govern. Koenig[38] applies this principle to corporate governance. A board operating on quarterly cycles with standardised risk reports lacks the variety to match a risk environment characterised by velocity, interconnection, and fat-tailed distributions. The Three Lines Model, with its periodic cadence and assurance focus, is a low-variety control system governing a high-variety environment. SGaaS adds requisite variety by introducing a continuous, adversarial function that operates on a different cadence, with a different methodology, and from a different vantage point than the existing lines.

From military doctrine to governance application. The adversarial methodology at the core of SGaaS draws on established traditions of structured challenge. Red teaming, as developed by the U.S. Army's Red Team Leader Program and documented by Bryce Hoffman,[28] provides the doctrinal basis for systematic adversarial analysis. Klein's pre-mortem technique,[37] published in the Harvard Business Review, provides the framework for failure-first analysis of governance decisions. Schwartz's scenario planning methodology,[60] developed at Royal Dutch Shell and documented in *The Art of the Long View*, provides the intellectual architecture for structured exploration of alternative futures.

What is novel about SGaaS is not any individual technique. It is the combination, the application of these established methodologies, at board level, on a continuous and retained basis, by an independent principal, within a commercial architecture designed for the specific governance gap documented in this paper.

8.5. Regulatory Alignment

Section 5 documented a multi-jurisdictional regulatory convergence toward five requirements, namely continuous oversight, adversarial testing, mission-critical risk architecture, personal accountability, and independent challenge. SGaaS is designed to satisfy all five.

Regulatory Requirement	Key Regulations	How SGaaS Responds
Continuous oversight of risk and controls	UK CGC Principle O; APRA CPS 230; OSFI E-21	Retained engagement providing continuous governance intelligence across board cycles
Adversarial testing of critical functions	DORA TLPT; TIBER-EU; SEC tabletop exercises	Red Team Protocol, Risk Simulation Lab, and Pre-Mortem Diagnostic: the adversarial principle applied to strategic governance assumptions through falsification of evidentiary support
Mission-critical risk architecture	Caremark: Marchand, Boeing, McDonald's; UK Provision 29	Dedicated governance architecture around the organisation's most consequential risks
Personal accountability for oversight	SM&CR; Caremark officer liability; CPS 230	Documented, independent challenge providing evidence of "reasonable steps" for senior managers
Independent challenge functions	BCBS 328; FSI Fourth Line; SM&CR	Structurally independent principal with mandate to challenge management narratives and board assumptions

Table 9. SGaaS regulatory alignment: requirements, key regulations, and how SGaaS responds

SGaaS does not claim to be the only way to satisfy these regulatory requirements. It claims to be a structurally coherent response that addresses them as an integrated set rather

than individually. An organisation that commissions continuous, adversarial, independent, principal-led governance challenge is better positioned, across all five requirements simultaneously, than one that relies on periodic internal assurance supplemented by episodic consulting reviews.

8.6. The Three-Layer Architecture of SGaaS

Marentis Labs delivers SGaaS through three interdependent layers: a governance brand, an adversarial methodology, and a commercial architecture. Each layer is addressed in subsequent sections of this paper; this section provides an overview of how they integrate.

Layer 1: The Governance Brand. "Strategic Governance as a Service. Adversarial by Design." The brand communicates the core proposition, that governance challenge is a permanent, architecturally designed function. It speaks to boards, audit committees, and senior managers, the individuals who commission governance functions and who bear personal accountability for their effectiveness.

Layer 2: The Adversarial Methodology. Three structured tools (the Red Team Protocol, the Risk Simulation Lab, and the Pre-Mortem Diagnostic) provide the operational substance of SGaaS. These are not proprietary inventions from scratch. They are established adversarial techniques, drawn from military doctrine, decision science, and scenario planning, adapted and integrated for board-level governance application. Section 9 details the methodology.

Layer 3: The Commercial Architecture. A four-tier retainer model (Diagnostic, Retained, Embedded, and Pre-Exit) designed for continuity and progression. The commercial structure is integral to the governance proposition. The tiered retainer ensures that SGaaS engagements are continuous (not episodic), cumulative (building institutional knowledge over time), and structurally aligned with the client's governance maturity. Section 10 details the architecture.

Originator Statement

Marentis Labs developed Strategic Governance as a Service and coined the term to describe a specific governance architecture combining board-level scope, principal-led delivery, adversarial methodology, and tiered retainer structure. The novelty lies in the integrated model, the application of established adversarial techniques, at board level, on a continuous basis, by an independent principal, within a commercial architecture designed for the structural governance gap that this paper has documented. This paper serves as the foundational description of the concept.

The following sections detail the adversarial methodology, the four-tier commercial architecture, and the economic case.

9 The Adversarial Methodology

Three tools constitute the adversarial methodology at the core of SGaaS: the Red Team Protocol, the Risk Simulation Lab, and the Pre-Mortem Diagnostic. Each draws on an established intellectual tradition and adapts it for a specific purpose, the delivery of structured, continuous, board-level governance challenge. What distinguishes their application within SGaaS is their integration, their governance context, and their sustained deployment on a retained basis rather than as episodic exercises.

The methodology's lineage runs through Karl Popper's account of how reliable knowledge is produced. No theory, however well-supported, can be proven correct by accumulated confirming evidence; it can only be provisionally corroborated, held open to further testing. What separates rigorous knowledge from its alternatives is not the evidence that supports it but the disciplined search for evidence that would refute it. "The criterion of the scientific status of a theory," Popper wrote, "is its falsifiability, or refutability, or testability."[54] The three tools below are instruments of that discipline applied to governance. They challenge the assumption that a strategy is sound, that a governance framework is working, or that a board decision is correct. They seek the conditions under which each would fail. A governance function that only accumulates confirming evidence produces comfort. A governance function that systematically attempts refutation produces resilience.

An epistemological distinction matters here. Technical systems can be tested empirically. A penetration test either breaches a firewall or it does not. Strategic assumptions cannot be broken empirically before the fact. An M&A valuation, a market-entry thesis, or a technology investment case depends on judgements about a future that has not yet arrived. What can be tested is not the assumption itself but the quality of the evidence supporting it, in particular whether the proxies are weak or strong, whether the reasoning is motivated or disciplined, and whether the cognitive biases documented by Kahneman are operating on the decision. SGaaS applies Popperian falsification to governance not by claiming to break strategic futures but by systematically dismantling the evidentiary basis on which those futures rest. The service produces a structured, adversarial examination of the evidence, the reasoning, and the cognitive conditions under which a strategic decision was reached. Where technical testing delivers a binary verdict, strategic falsification delivers a calibrated assessment of evidentiary fragility. Both are adversarial. They are not the same kind of test, and this paper does not claim otherwise.

9.1. The Red Team Protocol

9.1.1. Intellectual Origin

Red teaming has its modern origins in military and intelligence practice. The U.S. Army established its Red Team Leader Program[72] at the University of Foreign Military and Cultural Studies, Fort Leavenworth, in 2004, following intelligence failures that contributed to the Iraq War. The programme trains officers in structured adversarial analysis, the discipline of rigorously challenging plans, policies, and assumptions by adopting the perspective of an adversary or sceptic. The methodology has since been adopted by the CIA, FBI, UK Ministry of Defence, and NATO.

Bryce Hoffman, the first civilian graduate of the programme, documented its corporate

application in *Red Teaming* (2017),[28] demonstrating that the same techniques used to stress-test military operations can be applied to business strategy, organisational design, and governance architecture. Micah Zenko's *Red Team* (2015)[77] provided further evidence across military, intelligence, and corporate contexts.

The regulatory environment has begun to codify the adversarial principle itself. DORA's requirement for threat-led penetration testing of critical IT functions in financial services establishes that structured adversarial challenge is a governance-level expectation. The analogy is directional, not equivalential. DORA tests technical infrastructure empirically; SGaaS tests strategic and governance assumptions through the falsification of their evidentiary support. What regulators have recognised in the technical domain, that critical functions should be subjected to structured adversarial scrutiny, applies with equal force to the strategic domain, where the consequences of unchallenged assumptions are no less severe.

The board-advisory literature has travelled in the same direction. Brodeur et al.[6] identified "a board culture that promotes dialogue and constructive challenge" as a defining feature of effective risk oversight, and recommended that boards concentrate governance attention on the three to five "big bets" on which the organisation actually depends. The concept is not novel. What has been missing is the architecture to deliver it consistently. The Red Team Protocol operationalises constructive challenge as a permanent function rather than as an aspirational cultural trait, and focuses that challenge on the specific strategic assumptions the board has the least appetite to question.

The 2026 COSO review of practical ERM provides the empirical case for that architecture. *From Guidance to Action*[43] reports that only 20% of risk practitioners surveyed perceive high psychological safety in leadership discussions, and identifies the most damaging risks as those that are known internally but never voiced. COSO frames candour as a capability that leaders must deliberately practise, reinforce, and protect. The diagnosis is correct. The remedy is incomplete. Candour cannot be willed into existence by the same leaders whose authority creates the social cost of dissent, and culture-based interventions inherit the same chain-of-authority constraints that suppress challenge in the first place. The 80% of organisations operating below the COSO candour threshold are not failing through inattention; they are subject to the structural pressures any internal challenge function inherits. The Red Team Protocol externalises the challenge function rather than asking culture to bear the load. The principal sits outside the chain of authority being questioned. Dissent is not a personal act of professional courage. It is the principal's contracted output.

9.1.2. Definition and Operation

The Red Team Protocol is a structured adversarial assessment of strategic plans, governance frameworks, and board decisions. The SGaaS principal, operating independently of management, systematically identifies the assumptions on which a decision, strategy, or governance architecture depends and then subjects their evidentiary basis to falsification, testing whether the proxies are weak, the reasoning motivated, or the supporting evidence thinner than the confidence it carries.

In practice, a Red Team Protocol engagement proceeds through a defined sequence, with the analytical burden carried by the SGaaS principal rather than the board.

Phase 1: Asynchronous analysis. The principal maps the decision architecture, capturing what has been decided, by whom, on what evidence, with what assumptions, and with what alternatives considered or dismissed. This mapping is conducted through document

review, management interviews, observation of governance processes, and coordination with the second and third lines. The principal then constructs adversarial scenarios, the conditions under which the key assumptions fail, the evidence is incomplete, or the dismissed alternatives prove correct. The principal performs this analytical work asynchronously, alongside the organisation's existing governance rhythm. The board does not conduct the red team exercise. The board receives its distilled, high-signal output.

Phase 2: Forced independent deliberation. Before the principal reveals the Challenge Memo, each director independently submits a structured pre-deliberation assessment, recording their confidence in the key assumptions underlying the decision, their view of the two or three most material risks, and the conditions under which they would change their position. The principal collects these assessments anonymously and aggregates the results. This step is not optional. It is the mechanism through which the Red Team Protocol operationalises Kahneman, Sibony, and Sunstein's Mediating Assessments Protocol at board level. Independent, evidence-based judgement must precede group synthesis. Without it, the board becomes a passive consumer of the principal's analysis, and the decision hygiene the methodology depends on collapses into exactly the consensus dynamics it was designed to prevent.

Phase 3: Adversarial disclosure and structured debate. The principal then presents the Challenge Memo alongside the aggregated pre-deliberation data, revealing where directors' prior confidence aligns with the adversarial findings and where it diverges. The board debates the decision with three inputs that no conventional governance process provides, namely their own independently committed positions, a structured adversarial assessment of the evidentiary basis, and a map of the divergence between the two. The board retains the authority to decide. The Red Team Protocol ensures that the decision is made with adversarial intelligence, cognitive self-awareness, and structured debate.

The forced deliberation step addresses a specific vulnerability in the original design. If the principal simply presents a completed Challenge Memo, the board's role is reactive, limited to reading, discussing, and deciding. The pre-deliberation assessment reverses this. Directors commit their own positions before seeing the adversarial analysis, which means they engage cognitively with the assumptions rather than deferring to the principal's conclusions. The resulting debate is a genuine contest between the board's prior judgement and the adversarial evidence, not a presentation followed by questions.

Absence of institutionalised challenge
Primary defect addressed: Absence of institutionalised challenge. The Red Team Protocol creates a permanent function whose explicit mandate is to challenge the assumptions underlying governance decisions. It does not replace the board's judgement. It ensures that judgement is exercised against the widest possible range of adversarial intelligence.

9.2. The Risk Simulation Lab

9.2.1. Intellectual Origin

Scenario planning as a structured discipline emerged at Royal Dutch Shell in the 1970s, where Pierre Wack and his team developed a methodology for exploring alternative futures that enabled Shell to anticipate the 1973 oil crisis and respond more effectively than

competitors who relied on single-point forecasts. Peter Schwartz, a former head of Shell's scenario planning group, subsequently documented and extended the methodology in *The Art of the Long View* (1991), establishing scenario planning as a recognised tool for strategic decision-making under uncertainty.

The Risk Simulation Lab extends this tradition from strategic planning into governance. Where traditional scenario planning asks "what might happen?", the Risk Simulation Lab asks "how would our governance respond?" It shifts the unit of analysis from the external environment to the organisation's own decision-making architecture.

9.2.2. Definition and Operation

The Risk Simulation Lab is a scenario-based stress test of governance and leadership behaviour under crisis conditions. The SGaaS principal designs and facilitates simulated crises that are calibrated to the organisation's specific risk profile, governance architecture, and strategic context.

The design draws on Taleb's analysis of narrative fallacy,[65] the human tendency to construct coherent stories from incomplete evidence. The simulations deliberately violate the organisation's preferred narratives, presenting scenarios in which the growth strategy fails, the key assumption proves to be wrong, the regulatory environment shifts, or the reputational crisis arrives from an unexpected direction. By forcing participants to navigate conditions that challenge their mental models, the Lab reveals the assumptions on which governance depends. These assumptions are invisible under normal operating conditions.

In practice, a Risk Simulation Lab engagement is a facilitated exercise involving board members, senior management, or both, depending on the scenario's scope. The principal constructs the scenario, manages its evolution in real time (depending on the scenario), and observes the governance response, noting who takes charge, what information is sought, what assumptions are tested or accepted, how dissent is handled, and where the decision-making architecture breaks down.

The output is observed evidence of how the organisation's governance actually functions under adversarial conditions, evidence unavailable from any other source. Risk registers describe risks. The Risk Simulation Lab reveals how the organisation would actually respond to them.

Tetlock and Gardner's research[66] on expert judgement reinforces the design rationale. The best forecasters are those who systematically challenge their own assumptions. Surowiecki's work[63] on collective intelligence demonstrates that group judgement outperforms individual expertise only under conditions of diversity, independence, and structured aggregation. The Risk Simulation Lab creates precisely these conditions, providing diverse perspectives, forced independent assessment, and structured observation of the governance response.

Consensus dependency

Primary defect addressed: Consensus dependency. The Risk Simulation Lab forces decision-making under adversarial conditions that prevent the social dynamics (anchoring, conformity pressure, deference to seniority) that produce consensus without rigour. It reveals whether governance decisions are products of structured analysis or artefacts of group dynamics.

9.3. The Pre-Mortem Diagnostic

9.3.1. Intellectual Origin

The pre-mortem technique was developed by Gary Klein and published in the *Harvard Business Review*.[37] Klein's method inverts the conventional post-mortem. Instead of analysing why something failed after the fact, participants imagine that a project or decision has already failed catastrophically and work backward to identify the most likely causes.

The technique exploits a cognitive phenomenon known as prospective hindsight. Research by Mitchell, Russo, and Pennington[50] demonstrated that imagining an event has already occurred increases the ability to identify its causes. The pre-mortem transforms a question of prediction ("what could go wrong?") into a question of explanation ("why did it fail?"). The human mind is significantly better at explanation than prediction.

The technique also serves a social function that is directly relevant to governance. In a conventional risk discussion, raising concerns about a proposed strategy can feel adversarial. The person raising the concern is challenging the consensus and may face social pressure to conform. In a pre-mortem, the failure is stipulated. Every participant is asked to explain it. Dissent becomes the task, not the exception. The pre-mortem gives permission to speak truth to power.

9.3.2. Definition and Operation

The Pre-Mortem Diagnostic applies Klein's technique to governance decisions before major capital commitments, strategic shifts, or structural changes. The SGaaS principal facilitates a series of structured sessions in which participants are told: "It is twelve months from now. This decision has failed catastrophically. What happened?"

Participants work independently before group discussion, a direct application of Kahneman, Sibony, and Sunstein's decision hygiene principle that independent assessment must precede group synthesis. Each participant identifies the most plausible causes of failure from their own perspective and expertise. The principal then aggregates and structures the responses, identifying clusters of concern, areas of divergence, and failure modes that no single participant identified but that emerge from the collective analysis.

The output is a structured failure-mode map, a documented catalogue of the ways in which the decision might fail, weighted by frequency of identification and assessed for plausibility. This map does not tell the board what to decide. It tells the board what it is risking, and it does so with the benefit of the 30% improvement in causal reasoning that prospective hindsight provides.

Within the SGaaS model, the Pre-Mortem Diagnostic is a decision prerequisite, not a periodic review exercise. It is embedded into the governance process at the point of maximum leverage. This timing is what addresses the structural defect of episodic engagement. By activating risk engagement at the decision point itself, rather than in post-decision review, the Pre-Mortem Diagnostic shifts governance from periodic compliance to decision discipline.

Episodic engagement

Primary defect addressed: Episodic engagement. The Pre-Mortem Diagnostic makes risk engagement a prerequisite of significant decisions, not a periodic review conducted between them. It ensures that governance challenge occurs at the moment of maximum leverage (before the decision is made) rather than at the moment of minimum leverage (after the decision has been implemented and the organisation is committed).

9.4. The Integrated Methodology

The three tools are designed to operate best as an integrated system, but the use, scale and prominence of each tool is bespoke for each client.

Tool	Function	Primary Defect	Timing	Output
Red Team Protocol	Adversarial assessment of plans, frameworks, and decisions	Absence of challenge	Continuous: applied on a retained basis across governance cycles	Structured challenge briefs; assumption maps; adversarial intelligence
Risk Simulation Lab	Scenario-based stress test of governance behaviour under crisis	Consensus dependency	Periodic: calibrated exercises at defined intervals or ahead of strategic inflections	Observed evidence of governance response; decision-making diagnostics
Pre-Mortem Diagnostic	Failure-first analysis before major decisions	Episodic engagement	Event-driven: deployed before significant capital, strategic, or structural decisions	Failure-mode maps; weighted risk catalogues; decision-readiness assessments

Table 10. The three SGaaS adversarial tools: function, primary defect addressed, deployment timing, and output

In a typical retained SGaaS engagement, the three tools interact as follows. The Red Team Protocol operates continuously, providing ongoing adversarial intelligence on the organisation's governance architecture, strategic assumptions, and decision quality. The Risk Simulation Lab is deployed at defined intervals (typically quarterly or semi-annually) or ahead of significant strategic inflections, stress-testing the governance response under controlled adversarial conditions. The Pre-Mortem Diagnostic is deployed as decisions approach, ahead of major capital commitments, strategic shifts, and structural reorganisations.

The three tools share a common design philosophy with two operational principles. First, the analytical burden is carried by the SGaaS principal, not the board. Assumption mapping, adversarial scenario construction, document review, and coordination with the second and third lines are conducted asynchronously alongside the organisation's existing governance rhythm. Part-time directors receive distilled, high-signal adversarial intelligence rather than raw analytical workload. Second, directors are not passive consumers of that intelligence. Forced independent deliberation (anonymous pre-deliberation assessments of confidence and risk) precedes every structured challenge output, ensuring that the board engages cognitively with the decision before receiving the adversarial analysis. The tools differ in their scope (architecture vs. behaviour vs. decision), their timing (continuous vs. periodic vs. event-driven), and their primary target (the third, second, and first structural defects respectively). Together, they constitute a comprehensive challenge methodology that addresses all three structural defects simultaneously while respecting the cognitive constraints of board-level governance.

> **The methodology in summary.** SGaaS does not rely on a single technique. It deploys three integrated tools, each grounded in established intellectual traditions, each addressing a specific structural defect, and each operating on a different cadence. The Red Team Protocol provides continuous challenge. The Risk Simulation Lab stress-tests governance behaviour at defined intervals. The Pre-Mortem Diagnostic embeds risk engagement into the decision process itself. Together, they provide the sustained, adversarial, evidence-based challenge that the preceding sections have shown is missing from conventional governance architecture.

Section 10 presents the four-tier retainer model through which this methodology is delivered.

10 The Four-Tier Architecture

SGaaS operates through four tiers, each serving a different organisational entry point and building toward a natural progression path. The delivery architecture is integral to the governance proposition.

The structural defects this paper has identified cannot be addressed by a methodology alone. They require a delivery model that ensures the methodology is applied continuously, that institutional knowledge accumulates over time, and that the engagement deepens as the organisation's governance maturity develops.

The four tiers (Diagnostic, Retained, Embedded, and Pre-Exit) provide structured entry points for different organisational needs and a natural progression path from initial assessment to deep, board-level governance partnership.

10.1. Tier 1: Diagnostic GaaS

Diagnostic GaaS

Purpose: A structured adversarial assessment of the organisation's governance architecture, identifying structural defects, value gaps, and capability shortfalls.
Duration: Typically 4–8 weeks.
Entry point: The low-risk starting point for organisations that recognise the governance gap but want evidence before committing to ongoing engagement.

Who it serves. The Diagnostic tier is designed for organisations at a governance inflection point. Typical clients include a new chair or CEO seeking to understand the governance environment they have inherited, a board responding to a near-miss or regulatory finding, a private equity sponsor assessing governance readiness across a portfolio, and an audit committee that senses a gap between what it receives and what it needs.

What it delivers. The Diagnostic produces a Governance Architecture Assessment, a structured, adversarial evaluation of the organisation's governance framework. It examines the quality and independence of board-level decision-making, the effectiveness of the Three Lines Model as operationally implemented, the organisation's capacity for institutionalised challenge, and the gap between governance aspiration and governance reality.

The assessment is deliberately adversarial. Unlike a conventional governance review, which typically evaluates compliance with a code or framework, the Diagnostic asks whether this governance architecture is capable of surfacing the information the board needs to prevent catastrophic failure. If not, where are the structural weaknesses, and what would it take to address them?

How it integrates. The Diagnostic operates alongside existing governance functions. It does not replicate internal audit's work or duplicate the risk function's assessments. It assesses the *architecture* within which those functions operate, asking whether the board is receiving what it needs, whether the lines are coordinated, whether challenge is present or absent, and whether the governance framework is designed for the risks the

organisation actually faces.

Commercial structure. The Diagnostic is delivered on a fixed-fee basis. It is designed to be commercially accessible, with a defined scope, a defined timeline, and a defined deliverable. For the client, it is an investment in governance intelligence. For the SGaaS practice, it is the foundation of the institutional knowledge that makes retained engagement valuable.

10.2. Tier 2: Retained GaaS

Retained GaaS

Purpose: Continuous, adversarial governance challenge delivered on a retained basis across board cycles.
Duration: Ongoing; typically engaged on annual retainer with quarterly review points.
Entry point: The core SGaaS offering for organisations committed to closing the governance value gap on a sustained basis.

Who it serves. The Retained tier serves organisations where governance is a strategic priority and the cost of failure is consequential. Typical clients include regulated financial institutions, mid-market companies with complex risk profiles, organisations navigating strategic transformation, and boards that have completed a Diagnostic and want to act on its findings.

What it delivers. The Retained tier provides three categories of output, delivered on a continuous cycle:

Governance Pulse Reports: periodic assessments of the governance environment, identifying emerging risks, shifting dynamics, and areas where the board's information may be incomplete or stale. These reports provide the continuous governance intelligence that bridges the gap between board meetings.

Board Challenge Memos: structured adversarial briefs prepared ahead of significant board decisions, delivered through the forced deliberation protocol described in Section 9. Before the memo is presented, each director independently submits an anonymous pre-deliberation assessment, recording their confidence in the decision's key assumptions and the risks they consider most material. The principal then presents the Challenge Memo alongside the aggregated director assessments, revealing where prior confidence aligns with the adversarial findings and where it diverges. This protocol ensures that directors engage cognitively with the decision before receiving the adversarial analysis, preventing the passive consumption that would undermine the decision hygiene the methodology depends on.

Pre-Mortem Diagnostics and Risk Simulation Labs: deployed at defined intervals or ahead of strategic inflections, as described in Section 9. The retained relationship ensures that these exercises are calibrated to the organisation's specific context, informed by cumulative institutional knowledge, and connected to the ongoing governance narrative rather than conducted as isolated events.

How it integrates. The SGaaS principal operates alongside the CRO, head of internal audit, and compliance leadership. The principal attends governance committee meetings as an observer with a defined challenge mandate. They have access to board papers, risk reports, and audit findings, not to duplicate the work of internal functions, but to

assess whether the governance architecture is producing the outcomes those functions are designed to deliver. The relationship is collaborative in tone and adversarial in function.

Commercial structure. The Retained tier is delivered on an annual retainer, structured to provide continuity across board cycles. The retainer model is essential to the governance proposition. It eliminates the episodic engagement problem that characterises project-based advisory and aligns the commercial incentive with sustained governance improvement rather than with discrete project deliverables.

For senior managers operating under SM&CR or equivalent personal accountability regimes, the Retained tier provides documented, continuous, independent governance challenge, the evidence of "reasonable steps" that strengthens their personal defence. For boards facing Provision 29's declaration requirement, it provides the ongoing evidence base to support annual statements on control effectiveness.

10.3. Tier 3: Embedded GaaS

Embedded GaaS

Purpose: Permanent integration of the SGaaS principal into the organisation's governance architecture as an Independent Board Observer or Mandated Advisor, with contractual authority to challenge.
Duration: Ongoing; typically multi-year commitment.
Entry point: For organisations where the governance challenge function requires the permanence, visibility, and access that comes with a standing board-level presence.

Who it serves. The Embedded tier serves organisations where the governance challenge is significant enough to require a permanent, structurally embedded function with defined access and contractual challenge authority. Typical contexts include organisations navigating major transformation (merger integration, business model pivot, regulatory remediation); firms with heightened regulatory scrutiny requiring demonstrable, continuous, board-level governance; and complex organisations where the governance architecture spans multiple entities, jurisdictions, or regulatory regimes.

What it delivers. The Embedded tier provides everything in the Retained tier, plus permanent board-level presence. The SGaaS principal attends board and committee meetings as a contracted Independent Board Observer with a defined adversarial mandate. They provide real-time challenge during board deliberations, contribute to agenda-setting to ensure that governance-critical issues are not omitted, and serve as a standing adversarial voice in the room.

How it integrates. The Embedded tier preserves the SGaaS principal's independence from fiduciary liability by design. The principal does not take a formal directorial appointment. This is a deliberate architectural choice. Under corporate law in mature jurisdictions, fiduciary duties are holistic, collective, and non-delegable. A director cannot ring-fence liability to an adversarial function without assuming full responsibility for the board's strategic decisions. Formal appointment would compromise the independence that makes the function valuable.

Instead, the Embedded tier operates through one of two structures:

Independent Board Observer with contractual challenge authority. The SGaaS principal holds a permanent, contracted observer role with board and committee access, the right to

speak, the right to table challenge papers, and the right to require management response to findings. The principal does not vote and owes no fiduciary duties to the company. This is the default structure for Embedded engagements.

Mandated Advisor to the Risk or Audit Committee. The principal serves as a standing advisor to the relevant board committee, with a defined reporting line to the committee chair and, through the committee, to the full board. This structure provides institutional standing and a formal governance channel without creating direct fiduciary exposure.

Both structures cleanly separate the SGaaS principal from directorial liability while preserving the access, authority, and permanence that make the Embedded tier effective. The principal does not make governance decisions; they provide the adversarial intelligence that the actual fiduciaries need to discharge their duties under frameworks such as the Caremark doctrine or the UK Corporate Governance Code. A board that has embedded a continuous, independent, adversarial governance function through this structure demonstrates a level of oversight commitment that strengthens its position in any future Caremark analysis.

Commercial structure. The Embedded tier is delivered on a multi-year retainer, reflecting the depth of integration and the commitment required from both parties. The commercial structure reflects the premium value of board-level presence and the principal's investment in deep institutional knowledge.

10.4. Tier 4: Pre-Exit GaaS

Pre-Exit GaaS

Purpose: Governance uplift and exit-readiness assessment for private equity portfolio companies approaching a sale, IPO, or other liquidity event.
Duration: Typically 12–24 months before the anticipated exit event.
Entry point: For PE sponsors and portfolio company boards seeking to maximise governance-driven exit value.

Who it serves. The Pre-Exit tier serves private equity portfolio companies in the final phase of value creation before exit. Governance quality is a recognised factor in M&A diligence. Buyers assess financial performance alongside the maturity, resilience, and independence of the governance architecture that produced it. A portfolio company with demonstrably strong governance, one that can show continuous, independent, adversarial challenge at board level, presents a lower-risk acquisition target and a smoother diligence process.

What it delivers. The Pre-Exit tier combines the Diagnostic's assessment capability with the Retained tier's continuous challenge, focused specifically on exit readiness. The principal conducts a governance maturity assessment benchmarked against buyer expectations, identifies and remediates governance gaps that could create diligence friction, and provides an independent governance opinion that the seller can present to prospective buyers as evidence of governance quality.

The Pre-Exit tier provides the PE sponsor with a rigorous, adversarial assessment of how the portfolio company's capital allocation and risk governance will perform under intense buy-side due diligence and ensures that the evidence base supporting the existing competitive advantage period (CAP) is mathematically and operationally bulletproof.[45] This protects the seller from buy-side model compression, where acquirers exploit unstructured

risk reporting to underwrite a rapid, aggressive fade rate (f) to chip the transaction price during exclusivity.

How it integrates. The Pre-Exit principal works alongside the portfolio company's management team, the PE sponsor's value creation team, and any other advisors involved in exit preparation. The function is specifically designed to be independent of the management team preparing the business for sale, providing the buyer with confidence that the governance assessment was not self-serving.

Commercial structure. The Pre-Exit tier is delivered on a structured retainer basis across the 12–24 month engagement period. Commercial terms reflect the defined scope of governance assessment, remediation, and exit-readiness work, and are agreed in detail during the initial scoping conversation.

10.5. The Progression Logic

The tiers are designed as a progression, rather than a menu.

	Diagnostic	Retained	Embedded	Pre-Exit
Duration	4–8 weeks	Annual retainer, ongoing	Multi-year, ongoing	12–24 months pre-exit
Depth	Assessment and architecture mapping	Continuous challenge; ongoing governance intelligence	Board-level presence; real-time challenge authority	Exit-focused assessment, remediation, and opinion
Primary tools	Red Team Protocol (architecture assessment)	All three tools on continuous/periodic cycle	All three tools with direct board application	Diagnostic + Retained tools, exit-focused
Integration	Alongside existing functions; observer access	Governance committee observer; access to board papers and risk reports	Permanent Board Observer or Mandated Advisor; contractual challenge authority	Works with management, PE sponsor, and deal advisors
Commercial model	Fixed fee	Annual retainer	Multi-year retainer	Structured retainer

Table 11. The four-tier SGaaS architecture: duration, depth, tools, integration, and commercial model

The natural progression for most organisations is Diagnostic → Retained → Embedded. The Diagnostic builds the institutional knowledge and establishes the trust that makes the Retained tier valuable. The Retained tier deepens the relationship and demonstrates the value of continuous challenge, creating the conditions under which Embedded becomes a natural evolution. For PE portfolio companies, the path is typically Diagnostic → Pre-Exit, or Retained → Pre-Exit where the retained relationship pre-dates the exit timeline.

This progression logic is what distinguishes the SGaaS architecture from project-based advisory. Each tier is a stage in an evolving governance partnership, where cumulative institutional knowledge makes each subsequent tier more valuable than it could be as a standalone engagement.

> **The flywheel.** The four-tier architecture creates a governance flywheel. The Diagnostic builds knowledge that makes the Retained tier effective; the Retained tier builds trust and institutional depth that makes the Embedded tier a natural evolution; and the Pre-Exit tier converts governance maturity into measurable exit value. Each tier feeds the next. The result is a commercial architecture that is structurally aligned with the governance proposition, delivering continuity, progression, and cumulative challenge.

Section 11 makes the economic case.

11 The Economic Case

Do the economics work? Every figure cited below traces to a primary or authoritative source. Where evidence is suggestive rather than definitive, that limitation is acknowledged. The aim is to demonstrate that the economic logic of continuous governance challenge is sound, and that the cost of not having it is quantifiable and severe.

11.1. The Cost of Governance Failure

The case studies examined in Section 4 are quantifiable demonstrations of what governance failure costs. The figures are substantial enough to make the economic argument on their own terms.

Case	Financial Impact	Key Components
Boeing 737 MAX	~$20 billion total	$237.5M Caremark settlement; $2.5B DOJ Deferred Prosecution Agreement (Jan 2021); $1.1B additional settlements (2025); $1.77B airline compensation; $200M SEC penalty; 71% stock decline; 1,200+ cancelled orders
Wirecard	approximately €24 billion in shareholder value destroyed	€1.9B missing funds; €3.1B bank losses; share price collapse from €193 to €0.30[††]
Silicon Valley Bank	$16.1 billion FDIC fund cost	$42B single-day deposit flight; $100B queued withdrawals; $209B in total assets
Post Office Horizon	>£1.44 billion in compensation (as of March 2026) and legal costs	£250M legal fees[‡‡]; 900+ wrongful prosecutions; 20+ years of governance failure
Wells Fargo	>$7 billion in cumulative penalties	$3.7B CFPB order; $3B DOJ settlement; $2 trillion asset cap (lifted in June 2025)

Table 12. Quantified financial cost of governance failure across five documented cases

These are not outliers. They are the documented consequences of the structural defects this paper has identified, with oversight gaps that missed accumulating risk, suppressed internal challenge, and left boards without adversarial intelligence.

The headline cases sit inside a broader empirical pattern. Hunziker et al.[30] classified the underlying risk drivers behind 395 severe corporate crises in the DACH region between 2018 and 2024 using the Kaplan and Mikes (2012) framework.[36] Strategy risks accounted for 40.8% of events, external risks for a further 40.0%, and preventable (internal) risks for 19.2%. Eight in ten value-destroying events in a seven-year window originated in the two categories that rule-based, compliance-oriented governance was not designed to handle, namely strategic misjudgement and external shock. The point is not that compliance

[††] trading was terminated on the Frankfurt exchange in Jan 2021, with all delistings completed by November 2021.

[‡‡] as reported by the Guardian on 21st August 2024 (https://www.theguardian.com/uk-news/article/2024/aug/21/post-office-law-firms-payouts-horizon-it-scandal)

governance is failing at its own job; preventable-risk controls reduce the frequency of the events they target. The point is that the failures that matter most are happening in the space compliance governance was never built to cover, and that is the space an adversarial challenge function is designed to occupy.

The common thread across these cases is that governance structures were present and insufficient. Every organisation had boards, risk committees, internal audit functions, external auditors, and regulatory oversight. What each lacked was a mechanism for continuous, independent, adversarial challenge, the function that might have surfaced the risks before they became catastrophes. The economic question is whether the cost of providing that function is proportionate to the cost of not having it.

11.2. The Strategic Drift Cost

Catastrophic failures command the headlines, but routine value erosion is the more common economic consequence of the same structural defects. Failed M&A integrations, missed technological pivots, and unchallenged strategic assumptions produce damage that is chronic rather than acute, and, for mid-market firms, no less consequential over time.

The McKinsey finding that approximately 70% of mergers fail to achieve their stated value targets[47] is a strategy-risk statistic, not a compliance-risk statistic. Acquisitions fail because no function stress-tested the thesis, no one challenged the integration assumptions, and no adversarial mandate existed to ask what would need to be true for the deal to destroy value rather than create it. These are the same structural defects, episodic engagement and consensus dependency, operating at a lower amplitude than Boeing or Wirecard but with cumulative effects that compound across years.

The investor-side evidence reinforces the scale of the problem. Mauboussin and Callahan's analysis of nearly 24,000 US public companies from 1926 to 2025 found that 70% produced lifetime earnings insufficient to justify their IPO price. A mere 0.7% of listed companies created more than 75% of aggregate shareholder wealth, measured at $91 trillion.[45] The default trajectory for most companies is value erosion. Returns on invested capital regress toward the sector mean at an average annual fade rate of approximately one-fifth.[45] The question is how long a company can resist that gravitational pull. Governance challenge is one of the mechanisms that determines the answer, because the assumptions that accelerate the fade (unchallenged strategy, unexamined competitive position, unquestioned capital allocation) are precisely the assumptions an adversarial function is designed to surface.

For a mid-market firm, the twelve-percentage-point recovery gap that Hunziker et al. document translates directly. A £500 million enterprise that suffers a severe governance-driven value event and then underperforms its sector benchmark by twelve points for two or more years has lost £60 million or more in relative market position. That loss does not appear in a single write-down. It appears in the price achieved at the next fundraise, the multiples available at exit, and the competitive ground ceded while the board was reviewing backward-looking reports.

The economic case for SGaaS does not depend on preventing the next Wirecard. It depends on the proposition that continuous, adversarial governance challenge prevents the quiet accumulation of strategic risk that, left unchallenged, produces either a catastrophic event or a slow bleed of competitive position. The catastrophic cases prove the mechanism. The strategic drift cost proves the frequency.

11.3. The Recovery Gap

The most under-recognised element of the cost of governance failure is not the initial share-price drop. It is the divergence that persists long after the crisis itself has passed.

Hunziker et al.[30] tracked the post-crisis performance of the 213 DACH-listed companies in their sample that suffered a monthly share-price decline of 25% or more, benchmarked against the average of the Austrian Traded Index total return, the German Prime All Share performance index, and the Swiss Performance Index total return over the 24 months following each event. Two findings carry the argument.

First, the initial shock is severe. Affected firms fall to roughly 60% of their pre-crisis value in the event month, an approximate 40% loss of market capitalisation at the moment of impact.

Second, and more consequentially, the recovery is illusory. Twenty-four months later, the average affected firm has regained only its starting point, approximately 103% of pre-crisis value. Over the same period, the DACH benchmark indices have advanced to approximately 115%. The resulting gap, around twelve percentage points, is not a delayed rebound. It is market position that was forfeited at the event and never recovered. The authors' conclusion is explicit. "Severe firm-specific shocks leave long-lasting scars, not only in value destruction at the event but also in missed participation in subsequent market upswings".

The finding is not isolated. Hunziker et al. follow the methodology of the 1998 Mercer Management Consulting study of the US Fortune 1000, which documented the same recovery lag in a different market, different period, and different regulatory regime. Two independent datasets, separated by twenty-seven years and an ocean, find the same structural signature. Severe firm-specific shocks produce a permanent relative loss of market position, not a temporary write-down that subsequent performance erases.

This changes the economic framing of governance investment. The cost of a governance failure is not the write-down in the month it occurs. It is the write-down plus two-plus years of missed market participation plus the relative underperformance that, on the evidence, does not recede. Governance challenge, measured against this frame, is a value-preservation investment measured against a documented, persistent, and quantified gap.

The mechanism behind that persistence is stakeholder amplification. Grimwade,[27] drawing on McKinsey's analysis of approximately 350 operational risk incidents at European and North American financial institutions, documents that total shareholder returns over the 120 working days following disclosure were impacted more than twelve times the actual monetary losses from fines, settlements, and direct costs. The initial write-down is the trigger; the amplification chain, through share price decline, credit rating downgrade, increased funding costs, and customer attrition, is what makes the damage permanent. For investment-grade institutions, a one-notch downgrade typically widens debt spreads by 10 to 50 basis points,[26] a penalty that persists long after the operational loss itself has been absorbed; UBS's Fitch downgrade following the 2011 rogue-trader incident took five years to recover to 'A' and a further fifteen months to reach 'AA–'[26] . At Credit Suisse, the amplification accelerated past recovery. In the fourth quarter of 2022, clients withdrew CHF 138 billion in deposits, the largest share leaving in October as media speculation and loss of client confidence reinforced each other; over the same three months, the wealth and asset management businesses recorded CHF 111 billion in net asset outflows, closing a year that totalled CHF 123 billion in AUM outflows.[64] Share price decline and client withdrawal compounded into a self-amplifying loop that ended in forced rescue.

The recovery gap Hunziker et al. document is the aggregate signature of this amplification. Markets price the cascade, and the cascade outlasts the event.

The Recovery Gap

Two years after a severe corporate crisis, DACH-listed firms had, on average, returned only to their pre-crisis share price. The broader market had advanced approximately 15% over the same period.[30] The resulting twelve-point gap is not an initial write-down. It is a permanent loss of market position. The economic case for continuous governance challenge is measured against this gap, not against the event itself.

11.4. The Cost Positioning of SGaaS

SGaaS occupies a deliberate position in the governance cost spectrum. It sits below the cost of building a permanent internal capability, above the cost of episodic advisory, and is structured for continuity rather than project-based engagement.

To contextualise this positioning, consider the alternatives. A full-time Chief Risk Officer at a mid-market financial institution commands base compensation of £180,000–£225,000 in the UK, with total compensation (including bonus, pension, and benefits) typically reaching £270,000–£400,000 annually. In the United States, the range is $171,000–$275,000 in base salary, with total packages at larger institutions exceeding $400,000. Beyond the CRO, a functioning internal governance capability requires supporting staff, technology, and operational budget, costs that escalate rapidly with organisational complexity.

At the other end of the spectrum, project-based governance reviews from major advisory firms provide episodic assessment but no continuity. They address the question of the moment but do not build institutional knowledge, do not provide ongoing challenge between engagements, and create the very episodic engagement problem this paper has identified as a structural defect.

The SGaaS Retained tier (the core offering) provides continuous, principal-led governance challenge at a fraction of the fully-loaded cost of an internal CRO function, while delivering something no internal function can provide, namely structural independence. The principal is not employed by the organisation, does not report to the CEO, and has no career incentive to moderate challenge. The retainer model ensures continuity; the adversarial methodology ensures rigour; and the principal-led delivery model ensures that the challenge comes with the authority and experience to be taken seriously at board level.

11.5. The Value Creation Argument

The strategic drift evidence above established the gravity that governance must resist. ROIC regresses toward sector means at fade rates averaging one-fifth, and 70% of US public companies produce lifetime earnings insufficient to justify their IPO price.[45] The CAP framework decomposes the resistance. Terminal value, which accounts for more than 70% of firm value in standard DCF, is a function of three variables, namely investment magnitude, ROIC-WACC spread, and competitive advantage period.[45] SGaaS provides the rigorous capital allocation governance and risk hedging frameworks that allow these three variables to be defended under transaction conditions. By aligning internal project hurdle rates with today's macroeconomic realities and hardening interest-rate and supply-chain hedges, SGaaS ensures that the historical ROIC spread is structurally defensible and that

the buyer cannot credibly model an accelerated reversion to the mean. The question that follows is what governance does to those three variables.

Koenig[38] answers it directly. Governance is an organisational design discipline that determines how much risk the firm can take and how well it allocates capital across the risks it does take. Strong governance lifts the mean of the firm's outcome distribution and widens the range of upside the board can credibly underwrite.

The first mechanism is risk-taking capacity. A board with structured adversarial challenge can authorise larger and longer-horizon investments because it has a mechanism for detecting when a thesis is breaking. A board without that mechanism rations capital below the available opportunity set, because the oversight architecture cannot distinguish good risk from bad. Koenig[38] frames this as an application of Ashby's Law of Requisite Variety to corporate governance, observing that a control system must possess at least as much variety as the system it governs to regulate it. A board whose oversight architecture lacks the variety to match its risk environment will, predictably, under-invest in the spread-creating opportunities available to it. The cost of weak governance shows up in the foregone investment that was never made.

The second mechanism is capital allocation quality. Mauboussin and Callahan's analysis of nearly a century of US public company data establishes the scale of the variable. A mere 0.7% of listed companies created more than 75% of the $91 trillion in aggregate shareholder wealth.[45] McKinsey's finding that approximately 70% of mergers fail to achieve their stated value targets[47] reinforces the same conclusion in transaction form. The distribution is heavily skewed. A small minority of allocation decisions accounts for the bulk of value created, which is direct evidence that allocation discipline, the cumulative quality of the capital decisions a firm makes year after year, is the dominant variable in long-run value creation. Adversarial governance challenge is the mechanism by which weak theses are killed before capital follows them, with strategic assumptions tested, integration logic stress-checked, and unexamined consensus interrogated.

Both mechanisms compound through the CAP identity. Risk-taking capacity expands investment magnitude and extends CAP duration. A board that can safely authorise more growth investment funds more spread-creating opportunities, and one that detects early when a thesis is fading buys additional years before regression sets in. Capital allocation quality widens the spread itself. Every avoided value-destructive acquisition, every challenged growth assumption, every reconsidered capital deployment increases the gap between ROIC and WACC. SGaaS operates directly on the three variables that drive the majority of firm value.

This reframes the proposition for upper-tier clients. For Embedded and Pre-Exit engagements, where the principal is integrated into the strategic and capital-allocation cadence of the organisation, the economic case rests on governance being the condition under which a longer CAP, a higher spread, and a larger investment programme are credibly sustainable. The price of the engagement is measured against the value created.

The value-creation logic of SGaaS

Governance challenge expands the upside the board can credibly underwrite while it tightens the downside the board can absorb. Risk-taking capacity and capital allocation quality are the two variables Koenig[38] identifies as the governance contribution to value creation. They map directly onto the investment magnitude, spread, and CAP duration that drive the majority of firm value in standard valuation.[45] The case for the

upper tiers rests on the value-creation arithmetic above. The case for the lower tiers rests on the loss-avoidance arithmetic that follows.

11.6. The Loss Avoidance Argument

The most straightforward economic case for SGaaS is loss avoidance. This paper does not claim that SGaaS would have prevented every failure documented in Section 4. Counterfactual certainty is not available, and claiming it would undermine the intellectual discipline this paper seeks to maintain. What the evidence supports is a more measured proposition, that a continuous, adversarial, independent governance function, had one been in place, might have surfaced the risks earlier, challenged the assumptions more forcefully, and given the board the information it needed to intervene before the damage became irreversible.

The value of that 'might have' is economically significant even at modest probabilities. If a retained governance challenge function costing £200,000–£400,000 per year reduced the probability of a catastrophic governance failure by even a single percentage point for an organisation facing £100 million or more in potential loss exposure, the expected value calculation is overwhelmingly positive.

The logic is the same that underlies insurance, internal audit, and compliance expenditure. Organisations invest in preventive functions not because they guarantee that losses will not occur but because they reduce the probability and severity of losses to a degree that justifies the investment. SGaaS extends this logic to the governance architecture itself, the layer that oversees all other risk management functions creating, in effect, a form of strategy insurance.

11.7. Exit Value Creation

For private equity portfolio companies, the economic case for SGaaS has an additional dimension, namely exit value. Governance quality is a recognised factor in M&A diligence, and demonstrable governance maturity can reduce diligence friction, accelerate transaction timelines, and strengthen buyer confidence.

McKinsey research[47] documents that approximately 70% of mergers fail to achieve their stated value targets, with governance and integration capability identified as key differentiators in successful transactions. Due diligence limitations can overlook significant proportions of potential merger value, and governance maturity is among the factors that can reduce transaction friction.

Recall the CAP decomposition introduced earlier in this section. At the exit moment, the buyer's central forecasting question is how long the target firm can sustain its current ROIC spread before regression sets in. Mauboussin and Callahan's analysis of ROIC persistence, drawing on 55 years of data, shows five-year fade rates averaging 0.21, with sector-specific variation from 0.10 (consumer staples) to 0.30 (utilities).[45] Every year of additional CAP a buyer can justify in their valuation model lifts the exit multiple, because terminal value compounds at the spread the buyer is willing to underwrite for the duration the buyer is willing to underwrite it.

Governance architecture is one of the factors that determines whether that CAP assumption is credible. A portfolio company with 12–24 months of documented, continuous, independent governance challenge (governance pulse reports, board challenge memos,

red team assessments, and a governance maturity scorecard) gives the buyer evidence that the conditions sustaining ROIC above the cost of capital are being actively managed. Strategic assumptions are stress-tested, emerging risks are surfaced early, and decision-making at board level is subject to structured adversarial review.

A buyer's underwriting team seeks any structural, regulatory, or operational governance gap to justify modeling a faster fade rate (f), which translates directly into a late-stage purchase price deduction. In a congested 2026 exit market where average hold periods exceed six years, assets are highly vulnerable to these price-chipping tactics.A company whose governance documentation consists of annual board minutes and an internal audit plan offers no such basis.

The Pre-Exit tier is structured so that the principal's engagement is oriented toward exit value defense. The commercial model is agreed in advance and tied to the defined scope of governance work, creating a shared interest in the quality of the governance evidence base presented to prospective buyers.

11.8. Regulatory and Compliance Efficiency

The regulatory direction documented in Section 5 creates economic pressure as well as legal pressure. Boards facing Provision 29 declarations, SM&CR personal accountability, DORA resilience testing requirements, and Caremark-driven fiduciary duties must invest in governance capability regardless of whether they engage SGaaS. The decision is how to invest most effectively, not whether.

PwC research[58] identifies 20% cost reduction potential through the transition from periodic to continuous risk and compliance monitoring. While this figure relates to compliance functions broadly rather than to SGaaS specifically, the underlying principle is directly applicable: continuous governance challenge, by identifying issues earlier and maintaining a current understanding of the governance environment, reduces the cost of remediation, regulatory response, and crisis management.

The compliance cost literature reinforces this logic. Research by the Ponemon Institute,[53] conducted in the context of data protection compliance, found that organisations spend on average 2.71 times more on the consequences of non-compliance than on building and maintaining compliance programmes. While this finding is specific to data protection regulations, the underlying cost dynamic, namely that reactive management of compliance failure substantially exceeds the cost of proactive investment, applies with comparable logic to governance challenge investment: the documented costs of governance failure in the cases above dwarf any plausible preventive expenditure.

11.9. Insurance and Risk Transfer

Directors' and officers' liability insurance is priced, in significant part, on underwriters' assessment of governance quality. Willis Towers Watson research[76] documents that D&O underwriters scrutinise governance structures, risk management frameworks, and board oversight capability as primary factors in premium determination.

While the D&O market softened in 2024, with 81% of clients experiencing premium decreases averaging 5.2%, this cyclical trend does not diminish the structural relationship between governance quality and insurance pricing. As emerging risks (AI-related shareholder claims, economic insolvency, ESG litigation) enter the D&O market, underwriters are likely to differentiate more sharply between organisations with demonstrable governance

challenge capability and those without.

An organisation that can present evidence of continuous, independent governance challenge (documented through SGaaS deliverables) is better positioned in D&O renewal negotiations than one relying solely on standard governance structures. The insurance premium benefit alone does not justify SGaaS engagement; but as one component of a comprehensive economic case, it contributes to the overall cost-effectiveness of the model.

11.10. The Governance : Performance Relationship

The broader academic evidence supports the economic logic of governance investment. A meta-analysis conducted by Clark, Feiner, and Viehs,[7] examining over 200 academic studies on ESG and sustainability practices, found that 90% demonstrated a positive relationship between strong sustainability practices and lower cost of capital, while 88% showed a positive correlation between ESG quality and operational performance. Given that governance constitutes a core pillar of the ESG framework, these findings are relevant to the governance investment argument, though they should be understood as applying to ESG broadly rather than to governance in isolation.

These findings do not prove that SGaaS specifically will deliver financial returns. No honest analysis can make that claim for any governance investment. What they establish is that governance quality is an economically significant variable. Organisations with stronger governance architectures demonstrably perform better on cost of capital, operational efficiency, and long-term value creation. SGaaS strengthens the governance architecture; the economic evidence suggests that doing so has measurable financial consequences.

> **The economic case for SGaaS rests on three pillars.**
> First, the cost of governance failure is quantifiably catastrophic, measured in the billions across documented cases.
> Second, the cost of continuous governance challenge is modest by comparison: measured in the hundreds of thousands annually.
> Third, the broader evidence consistently links governance quality to financial performance, lower cost of capital, and more effective risk management.
> The question facing boards is starker: can they quantify the cost of not having it?

12 Objections and Responses

Six objections deserve direct answers. Governance professionals, from board directors to risk committee chairs to chief risk officers, are trained to interrogate propositions and probe their potential weaknesses. This section subjects SGaaS to the scrutiny its own methodology demands.

The objections addressed below are the questions that emerge consistently when the model is presented to governance practitioners, raising matters of independence, adoption willingness, scalability, fiduciary conflict, and intellectual originality. Each deserves a direct and honest response.

12.1. "If SGaaS Is Paid for by the Company, How Is It Independent?"

This is the most important objection, and the paper acknowledges it directly. Any externally provided governance function that is paid by the entity it serves faces a structural tension between commercial interest and independent judgement. This tension is real, and no amount of rhetorical framing can eliminate it.

But the objection, taken to its logical conclusion, would eliminate every externally provided assurance and governance function. External auditors are paid by the companies they audit. Credit rating agencies are paid by the issuers they rate. Management consultants are paid by the management teams they advise. The question is not whether a commercial relationship exists. It does, in every case. But the structural safeguards are sufficient to preserve functional independence despite it.

The SGaaS model addresses independence through four structural mechanisms:

First, the mandate. The SGaaS principal reports to the board or committee chair, not to management. The engagement terms are approved by the board. Management cannot direct, constrain, or veto the SGaaS function's findings. This reporting structure is fundamentally different from consulting engagements, where management typically controls scope, access, and deliverable acceptance.

Second, the methodology. The adversarial methodology (red teaming, risk simulation, premortem analysis) is structurally designed to produce challenge. A red team that does not challenge has failed, regardless of the commercial relationship. The methodology creates institutional pressure toward independence that complements the structural safeguards.

Third, the commercial model. The retainer structure eliminates the project-by-project revenue dependency that creates the most acute independence risk in traditional advisory. The SGaaS principal is not competing for the next project; the engagement is continuous by design. This removes the incentive (identified by Bazerman and colleagues in their analysis of auditor independence) to moderate findings to secure future work.

Fourth, the market discipline. SGaaS is a reputational business. A governance challenge function that fails to challenge (that tells boards what they want to hear rather than what they need to hear) will be exposed by the first governance failure it fails to prevent. The commercial incentive, properly understood, runs toward rigour rather than away from it.

> **The honest answer**: SGaaS cannot claim perfect independence. No externally provided function can. What it can claim is that its structural design (mandate, methodology, commercial model, and market incentive) creates stronger independence safeguards than any existing alternative for governance challenge at board level.

12.2. "Boards Won't Voluntarily Adopt a Function Designed to Challenge Them"

Some won't. This paper does not pretend otherwise. Boards that are satisfied with their governance architecture, that believe their existing oversight mechanisms are sufficient, or that are simply unwilling to subject themselves to structured adversarial challenge will not engage SGaaS. That is their prerogative.

But three forces are making voluntary adoption increasingly rational.

The regulatory direction is unmistakable. Provision 29 requires boards to declare on the effectiveness of material internal controls (a declaration that requires evidence of continuous monitoring, beyond the existence of governance structures). The Caremark doctrine's evolution through Marchand and Boeing has increased personal director liability for oversight failures of mission-critical risks. SM&CR imposes personal accountability on senior managers. Boards that recognise this trajectory understand that proactive governance investment is preferable to regulatory-forced remediation.

The case studies are compelling. Every governance failure documented in Section 4 (Boeing, Wirecard, SVB, Credit Suisse and The Post Office) occurred in an organisation that had a full complement of governance structures. The failures were not failures of framework but failures of challenge. Boards that have studied these cases, or that have experienced near-misses in their own organisations, are precisely the audience for whom SGaaS is designed.

The entry point is low-risk. The tiered architecture is specifically designed to address adoption resistance. The Diagnostic tier offers a four-to-eight-week assessment with defined scope and deliverables (a low-commitment engagement that allows boards to experience the value of independent governance challenge before committing to an ongoing relationship). It is an invitation to test the proposition before making any permanent structural commitment.

12.3. "How Does This Scale Without Diluting Quality?"

SGaaS does not scale in the conventional sense. That is a deliberate design choice.

SGaaS is a principal-led model. The governance challenge is delivered by the principal (a senior practitioner with the authority, experience, and institutional knowledge to engage credibly at board level). Unlike audit fieldwork, compliance monitoring, or consulting analysis, the governance challenge requires a senior principal and cannot be delegated to a junior team. A pyramid model (in which junior analysts perform the work and a partner reviews it) would reproduce the deliverable substitution problem this paper identified in Section 7, where the organisation pays for senior judgement but receives junior analysis.

Scalability in the SGaaS model comes from three sources. First, the **tiered architecture** itself creates natural segmentation. The Diagnostic tier is relatively scalable (it is a defined-scope assessment), while the Embedded tier is deliberately capacity-constrained

(it requires deep, ongoing engagement). Second, **the practice model** is built around principals, not around a single individual. As the practice grows, it adds senior practitioners (each capable of leading engagements independently) rather than building a pyramid of juniors supporting a small number of partners. Third, **institutional knowledge tools** (governance pulse reports, challenge memos, maturity assessments) create a cumulative evidence base that reduces the start-up cost of each new engagement.

The honest constraint is that SGaaS is designed for organisations where governance is a strategic priority and the cost of failure is existential. That market is substantial, but it is not unlimited, and the model does not pretend otherwise.

12.4. "Board-Level Presence Creates Fiduciary Conflicts"

This objection anticipates a real problem, but the Embedded tier was designed to avoid it, not to manage it after the fact.

Under corporate law in mature jurisdictions (the UK Companies Act 2006, Delaware General Corporation Law, and their equivalents), fiduciary duties are holistic, collective, and non-delegable. A director who accepts a formal board appointment cannot confine liability to a single function. Any attempt to "ring-fence" an adversarial mandate within a directorial role would expose the principal to the full spectrum of fiduciary obligation, compromising the independence that makes the challenge function valuable in the first place.

The Embedded tier therefore excludes formal directorial appointment by design. The SGaaS principal operates exclusively as an Independent Board Observer or as a Mandated Advisor to the Risk or Audit Committee. Neither structure creates fiduciary duties. Both structures preserve the access, permanence, and authority the tier requires.

The separation is clean. The principal does not make governance decisions. The principal provides the adversarial intelligence, the stress-tested assumptions, surfaced failure modes, and challenged consensus positions, that the actual fiduciaries need to discharge their own duties. For directors operating under the Caremark doctrine's evolving standard for mission-critical risk oversight, or under the UK Corporate Governance Code's expectations for effective board challenge, the Embedded tier strengthens their position. It provides documented, continuous, independent governance intelligence that supports the "reasonable steps" defence.

Appropriate professional indemnity and contractual terms are required for both structures. The legal structuring is straightforward precisely because the architecture resolves the fiduciary question at the design stage rather than managing it contractually.

12.5. "Red Teaming and Pre-Mortems Are Established Techniques: What's New?"

The individual techniques have well-documented intellectual origins, and this paper has acknowledged them throughout. Red teaming traces its lineage from the Vatican's advocatus diaboli through military intelligence to contemporary business applications. The pre-mortem technique was formalised by Gary Klein and has been widely adopted in project management contexts. Scenario planning has roots in military strategy and was developed for business use at Royal Dutch Shell in the 1970s.

The claim of this paper is not that these techniques are new. The claim is that their

structured, continuous application at board level as a governance function is new, and that this application addresses a specific set of structural defects that no existing model adequately addresses.

The distinction matters. A one-off red team exercise conducted as part of a consulting engagement is not SGaaS. A pre-mortem analysis performed by the project team before a single decision is not SGaaS. A scenario planning workshop facilitated by an external consultant every two years is not SGaaS. What distinguishes the SGaaS methodology is the *synthesis*: the integration of these techniques into a continuous, principal-led, adversarial governance architecture that builds institutional knowledge over time and operates with the independence and authority to challenge at the highest level of the organisation.

The same is true at the architectural level. Governance theorists have recognised the need for an institutionalised challenge function for decades. Turnbull's Watchdog Board and Carver's Policy Governance method[38] both propose structural responses to the absence of independent challenge. The governance profession has long had the diagnosis. The delivery model has been missing, a commercially viable, externally retained architecture that makes continuous, independent challenge available within existing governance frameworks. The individual tools are acknowledged building blocks. The governance need is established theory. The architecture, the way the tools are combined, delivered, and sustained as a retained service, is what SGaaS contributes.

12.6. "Our Internal Audit and Risk Functions Already Provide This"

The evidence examined in Section 6 suggests otherwise, not because internal audit and risk functions are failing, but because they are structurally unable to provide what SGaaS delivers. Internal audit spends 75% of its time on routine assurance and compliance. Risk functions face material funding constraints for emerging-risk identification. Both functions report through management hierarchies that create inherent limitations on the independence and adversarial nature of their challenge.

These functions are essential. The question is whether they can, within their current structural constraints, provide continuous, adversarial, independent governance challenge at board level. The IIA's Vision 2035 report[31] implicitly acknowledges they cannot. Its projection that internal audit should shift from 75% assurance to 59% assurance is an admission that the current model is inadequate for the strategic challenge governance increasingly requires.

SGaaS does not replace these functions. It fills the structural gap they cannot fill, the space between what the Three Lines model is supposed to deliver and what it actually delivers in practice. The integration architecture described in Section 13 is specifically designed to ensure that SGaaS complements rather than competes with existing governance functions.

12.7. The Limits of Independence: Why SGaaS Can Still Fail

To apply the exact mandate of SGaaS (stress-testing logic and identifying failure modes) to the model itself, this paper must preemptively acknowledge its own operational vulnerabilities. While SGaaS is designed to mitigate the structural defects of traditional governance, it is not immune to the human and organisational realities it critiques. There are three primary ways the model can still fail:

Commercial independence remains aspirational. The paper argues that a retainer model breaks the consensus dependency of project-based consulting. While it mitigates the

pressure, it does not eliminate it. A retained advisor who continually antagonises management or delivers deeply uncomfortable truths still faces the risk of the retainer not being renewed. True structural independence only exists when the challenger cannot be fired by the entity being challenged (such as a regulator), but the gravitational pull of palatability remains a risk.

Continuous oversight is practically constrained. While SGaaS positions itself as continuous rather than episodic, an external principal's visibility is ultimately gated by the information the organisation chooses to share and the meetings they are invited to observe; unless the principal is physically embedded on a near full-time basis, their oversight relies heavily on management's willingness to provide transparent access. The principal can only challenge what they are allowed to see.

Methodology cannot override toxic culture. Techniques like the Pre-Mortem Diagnostic rely on "prospective hindsight" to grant participants permission to dissent. However, in highly autocratic or psychologically unsafe cultures (precisely those most at risk of catastrophic failure), an external facilitator asking executives to imagine a project has failed will not magically produce radical honesty. Executives may simply offer politically safe failure modes that protect their departments and the CEO. The methodology requires a baseline of psychological safety to function; without it, the exercise risks becoming performative.

Acknowledging these limits does not invalidate the model. Rather, it demonstrates the adversarial honesty that SGaaS champions, recognising that no external governance architecture can entirely engineer away human nature or profound cultural dysfunction.

13 Implementation Blueprint

If a board is persuaded, what does it do next?

The implementation blueprint below is actionable without being prescriptive. Every organisation's governance context is different, with a different regulatory environment, different board maturity, different risk profile, and different internal capability. What follows is a structured pathway that can be adapted to any of these contexts while preserving the core principles of SGaaS, namely continuous engagement, adversarial challenge, principal-led delivery, and structural independence.

13.1. When Is SGaaS the Right Answer?

Not every organisation needs SGaaS, and not every moment is the right entry point. The decision to engage an external governance challenge function should be triggered by identifiable conditions, signals that the current governance architecture is insufficient for the risks the organisation faces.

The most common triggers fall into five categories:

Trigger	Indicators
Regulatory pressure	Upcoming Provision 29 declaration; SM&CR personal accountability concerns; DORA resilience testing requirements; heightened Caremark exposure following mission-critical risk identification
Board concern	Risk or audit committee dissatisfaction with quality of challenge; sense that risk reporting is backward-looking; concern that governance structures exist on paper but do not produce genuine oversight
Leadership transition	CRO vacancy or transition; new board chair or committee chair seeking independent assessment; post-CEO change governance review
Post-incident review	Regulatory enforcement action; material risk event; near-miss that exposed governance gaps; reputational crisis revealing oversight deficiency
Transaction preparation	PE portfolio company approaching exit (12–24 month horizon); IPO preparation requiring governance uplift; acquisition integration requiring governance alignment

Table 13. Common triggers for SGaaS engagement and their indicators

The presence of any single trigger is sufficient to warrant a Diagnostic engagement. The presence of multiple triggers, particularly the combination of regulatory pressure and board concern, typically indicates a need for the Retained tier from the outset.

13.2. The Entry Pathway

The recommended entry pathway for all SGaaS engagements, regardless of the eventual tier, is the Diagnostic. This is a deliberate design choice, not a sales tactic. The Diagnostic serves three functions that are prerequisites for effective ongoing governance challenge.

First, the Diagnostic establishes a governance baseline. Using the Marentis Risk Maturity Model, the assessment evaluates the organisation's governance architecture across five dimensions, namely governance structure and mandate clarity, challenge capability and independence, risk information flow and escalation, decision quality processes, and institutional memory and continuity. The output is a composite maturity score benchmarked against sector peers, a factual starting point, not a sales document.

Second, the Diagnostic identifies the specific governance gaps that subsequent SGaaS engagement would address. The Diagnostic maps the organisation's governance architecture against the three structural defects identified in this paper (episodic engagement, consensus dependency, absence of institutionalised challenge), identifying where each defect manifests in the organisation's specific context.

Third, the Diagnostic builds the working relationship between the SGaaS principal and the board. Effective governance challenge requires trust, not the trust that comes from telling people what they want to hear, but the trust that comes from demonstrating rigour, independence, and genuine insight into the organisation's governance dynamics. The Diagnostic creates this foundation before any ongoing commitment is made.

> **Typical Diagnostic pathway**: 4–8 weeks. Interviews with board members, committee chairs, CRO, Head of Internal Audit, and key management. Document review of governance frameworks, risk reporting, board and committee minutes, and internal audit plans. Adversarial assessment of governance capability. Deliverable: Governance Maturity Report with benchmarking, gap analysis, and recommended pathway.

13.3. Mandate Design

The effectiveness of SGaaS depends critically on the mandate under which it operates. A poorly designed mandate (one that subordinates the SGaaS function to management, limits access to information, or constrains the scope of challenge) will produce precisely the kind of compromised governance oversight that the model is designed to replace.

The mandate must address four structural requirements:

Reporting line. The SGaaS principal reports to the board or to a designated committee chair (typically the risk committee or audit committee chair), not to the CEO, CFO, or any management function. This reporting line is non-negotiable. Management-directed governance challenge is a contradiction in terms. It recreates the consensus dependency that SGaaS exists to disrupt.

Scope of challenge. The mandate must define what falls within the SGaaS scope (typically strategic risk oversight, governance architecture effectiveness, decision quality, and board information sufficiency) while explicitly preserving the mandates of existing functions. SGaaS does not replace internal audit, risk management, or compliance. It challenges the governance architecture within which those functions operate.

Access rights. The SGaaS principal requires access to board and committee papers, risk reports, internal audit plans and findings, regulatory correspondence, and critically, the right to attend relevant board and committee meetings as an observer with defined challenge authority. Without information access, the function cannot fulfil its mandate.

Independence protections. The mandate must include structural protections for independence, including a defined term with board-approved renewal; removal only by board

resolution; no management veto over SGaaS deliverables or findings; and clear terms governing the separation of the SGaaS mandate from any other advisory or commercial relationship with the organisation.

13.4. Integration with Existing Functions

SGaaS complements existing functions; it does not compete with them. Its value depends on working effectively alongside, not in place of, the organisation's existing governance functions. The integration architecture defines how this relationship operates in practice.

Function	SGaaS Relationship	Coordination Mechanism
Chief Risk Officer	SGaaS challenges governance architecture and strategic risk oversight; CRO owns risk management operations and reporting	Quarterly alignment meeting; SGaaS receives CRO risk reports; CRO receives SGaaS challenge findings for consideration
Internal Audit	SGaaS provides forward-looking, adversarial challenge; IA provides retrospective assurance and compliance verification	Annual plan coordination; SGaaS Red Team outputs inform IA risk assessment; IA findings inform SGaaS governance evaluation
Compliance	SGaaS assesses governance architecture effectiveness; Compliance ensures regulatory obligation adherence	SGaaS receives regulatory change notifications; Compliance receives SGaaS regulatory alignment assessments
Board / Committees	SGaaS reports directly to board or committee chair; provides independent challenge perspective on all governance matters	Monthly Governance Pulse Report; attendance at key committee meetings; annual governance health assessment
External Audit	No direct coordination mandate; SGaaS may reference external audit findings in governance assessments	Information sharing via audit committee as appropriate; no direct reporting relationship

Table 14. SGaaS integration with existing governance functions and coordination mechanisms

14 Conclusion

This paper began with a paradox. Spending on governance, risk management, and compliance has never been higher. Regulatory requirements have proliferated across every major jurisdiction. Organisations have invested in boards, risk committees, internal audit functions, compliance teams, and external advisers. Yet the evidence, documented across five detailed case studies, two decades, and three continents, shows that governance failures have not diminished in frequency or severity.

The paper has argued that this paradox has an identifiable cause. Governance fails not because frameworks are absent but because of three structural defects in how oversight is delivered: episodic engagement that cannot match the pace at which risks evolve; consensus dependency that suppresses the adversarial challenge boards need; and the absence of institutionalised challenge (no permanent function within most governance architectures whose mandate is to stress-test assumptions, surface failure modes, and challenge decisions before they become irreversible).

These are not theoretical propositions. Boeing's 737 MAX programme killed 346 people while every layer of governance was in place. Wirecard's €1.9 billion fraud survived five layers of oversight for years. Silicon Valley Bank collapsed in 48 hours with its CRO position vacant for nine months. The Post Office prosecuted more than 900 innocent people over two decades while its governance architecture failed to challenge a system it knew to be flawed. In every case, the structures were present. What was absent was the challenge.

Regulators across the United Kingdom, European Union, and United States are converging on the same conclusion, that continuous oversight, effective challenge, and personal accountability are non-negotiable requirements for governance at board level. The Three Lines model (the dominant governance framework) produces a measurable value gap between what it promises and what it delivers, with internal audit consumed by routine assurance and risk functions trapped in business-as-usual monitoring. Traditional advisory models (Big Four consulting, boutique firms, NED networks) address pieces of the problem but none provides the continuous, adversarial, independent challenge that the evidence demands.

Strategic Governance as a Service is the structural response to these structural defects.

SGaaS replaces episodic oversight with continuous engagement. It replaces consensus dependency with adversarial challenge, delivered through a proprietary methodology comprising the Red Team Protocol, the Risk Simulation Lab, and the Pre-Mortem Diagnostic, each addressing a specific structural defect. It replaces the absence of institutionalised challenge with a permanent, principal-led governance function that operates at board level with the independence, authority, and institutional knowledge to make that challenge meaningful.

The model is delivered through a four-tier architecture (Diagnostic, Retained, Embedded, and Pre-Exit) designed for progression. Each tier builds the understanding and trust that makes the next a natural evolution, not a new sale. The economic case is conservative but clear. The cost of continuous governance challenge is measured in the low hundreds of thousands; the cost of governance failure, whether catastrophic or chronic, is measured in multiples of that investment. The catastrophic cases documented in this paper prove the mechanism. The broader evidence, with over 80% of value-destroying corporate

events originating in strategy and external-risk categories, proves the frequency. SGaaS addresses both, the tail-risk explosion that ends careers and the strategic drift that erodes competitive position while the board reviews last quarter's reports. Investors already have empirical tools to measure how long a company's competitive advantage is expected to last, with sector-specific fade rates calibrated against 55 years of return data.[45] Governance architecture is one of the factors that determines whether those expectations are justified, namely whether the board is actively managing the conditions that sustain returns above the cost of capital, or passively watching them erode. SGaaS provides the mechanism through which boards can demonstrate, to investors and to themselves, that the assumptions underpinning their competitive advantage period are being continuously and adversarially tested.

This paper has been disciplined about what it claims and what it does not. SGaaS is not for every organisation. It is for those where governance is a strategic priority and the cost of failure is existential. It is for the board that recognises the gap between its governance architecture and the challenge that architecture should deliver. Some boards will conclude that their existing structures are sufficient. Some will prefer to wait for regulatory direction to force the question. That is their prerogative.

But for boards that have studied the case record, that feel the weight of Provision 29 declarations and Caremark exposure, that know their internal audit function is stretched and their risk committee is receiving backward-looking reports when it needs forward-looking challenge, SGaaS offers a structured, evidence-based, intellectually rigorous answer to a question the governance profession has been asking for two decades; *if the problem is not the absence of governance, what is it, and what do we do about it?*

Marentis Labs developed Strategic Governance as a Service and originated the term to describe a specific governance architecture, comprising board-level scope, principal-led delivery, adversarial methodology, and a tiered retainer structure designed for continuity. This paper is the foundational articulation of that model. The firm exists to deliver it.

Core Thesis

Governance failures are not failures of frameworks. They are failures of challenge, continuity, and independence, and Strategic Governance as a Service is the structural response.

Next Step

Marentis Labs offers a confidential Diagnostic conversation for boards and committee chairs who recognise the governance gap this paper describes. The conversation is without obligation, structured around your organisation's specific governance context, and assesses whether SGaaS is the right response.
To arrange a Diagnostic conversation, contact Marentis Labs at **governance@marentislabs.com**

About the Author

LinkedIn

Owen Vallis is an experienced C-suite leader, Independent Non-Executive Director and the Founder and Managing Director of Marentis Labs, where he originated the concept of Strategic Governance as a Service (SGaaS). With more than twenty years of experience across the global financial services landscape, his career is dedicated to shifting governance from a compliance-led performative ritual toward a model of substantive, adversarial challenge that drives genuine organisational resilience.

His expertise spans the domains of asset management, investment banking, and wholesale banking, at firms including Morgan Stanley, J.P. Morgan and Credit Suisse, with a specialised focus on fiduciary and prudential risk for complex discretionary portfolios. Owen is a subject matter expert in the design and implementation of capital and liquidity frameworks, and institutional investment portfolios across a wide range of asset classes. He possesses a refined capability for the rigorous validation of complex financial models. Owen excels at bridging the gap between technical, quantitative risk data and the strategic narratives required for effective board-level decision-making.

As an executive leader and experienced independent board chairman, Owen addresses the structural defects of episodic oversight and consensus dependency that often lead to governance failure. By integrating this extensive practical experience with technical skills in data analytics, he conducts independent, evidence-driven analysis to inform structured challenge.

Through Marentis Labs, Owen provides boards and senior executives with the continuous, principal-led challenge and decision hygiene necessary to navigate the volatility of modern global markets.

Glossary of Acronyms

APRA	Australian Prudential Regulation Authority; the prudential regulator of the Australian financial services industry.
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht; Germany's Federal Financial Supervisory Authority, responsible for the supervision of banks, insurance undertakings, and securities trading.
BCBS	Basel Committee on Banking Supervision; the primary global standard-setter for the prudential regulation of banks, operating under the auspices of the Bank for International Settlements.
CAMELS	Capital adequacy, Asset quality, Management, Earnings, Liquidity, and Sensitivity to market risk; the supervisory rating system used by US federal banking regulators to assess the overall condition of a financial institution.
CAP	Competitive Advantage Period; the duration over which a company can earn returns on invested capital above its cost of capital on new investment. Used in investor valuation models to quantify the sustainability of excess returns.
CCRC	Criminal Cases Review Commission; the independent body responsible for reviewing potential miscarriages of justice in England, Wales, and Northern Ireland.
CFPB	Consumer Financial Protection Bureau; a US government agency responsible for consumer protection in the financial sector.
CFO	Chief Financial Officer.
CIA	Central Intelligence Agency; the US federal intelligence service, whose red-teaming and adversarial analysis practices informed the methodology underlying the SGaaS Red Team Protocol.
CRO	Chief Risk Officer; the senior executive responsible for managing and overseeing enterprise-wide risk.
D&O	Directors' and Officers' liability insurance; insurance covering personal liability of corporate directors and officers for claims arising from their managerial decisions.
DAX	Deutscher Aktienindex; Germany's benchmark stock market index, comprising the thirty largest companies listed on the Frankfurt Stock Exchange.
DORA	Digital Operational Resilience Act; European Union regulation, fully effective from January 2025, requiring financial entities to manage ICT risk and conduct threat-led penetration testing of critical functions.
DOJ	Department of Justice; the US federal department responsible for law enforcement and the administration of justice.
ECB	European Central Bank; the central bank of the European Union and the primary monetary authority for the euro area.
ESG	Environmental, Social, and Governance; a framework for evaluating

	the non-financial risks and responsibilities of an organisation.
FAA	Federal Aviation Administration; the US national authority with powers to regulate all aspects of civil aviation.
FCA	Financial Conduct Authority; the conduct regulator for financial services firms and financial markets in the United Kingdom.
FDIC	Federal Deposit Insurance Corporation; the US agency providing deposit insurance to depositors in US commercial banks and savings banks.
FRC	Financial Reporting Council; the UK independent regulator responsible for promoting transparency and integrity in business, including oversight of the UK Corporate Governance Code.
FSI	Financial Stability Institute; a body of the Bank for International Settlements that assists financial sector authorities in strengthening their financial systems.
FTSE	Financial Times Stock Exchange; the index series produced by FTSE Russell, a subsidiary of the London Stock Exchange Group, including the FTSE 100 and FTSE 350.
GaaS	Governance as a Service; a broad category of externally delivered governance support. Within this paper, distinguished from Strategic Governance as a Service (SGaaS).
GDPR	General Data Protection Regulation; the European Union's primary legislation governing the processing of personal data.
GRC	Governance, Risk, and Compliance; the integrated approach covering an organisation's governance framework, enterprise risk management, and adherence to regulatory obligations.
HTM	Held-to-Maturity; an accounting classification for debt securities that an entity intends and is able to hold until they mature.
IA	Internal Audit; the function providing independent, objective assurance and consulting activity designed to add value and improve an organisation's operations.
IIA	Institute of Internal Auditors; the international professional association and standard-setting body for the internal audit profession.
IPO	Initial Public Offering; the process by which a private company offers shares to the public for the first time.
IRRBB	Interest Rate Risk in the Banking Book; the risk to a bank's capital and earnings arising from adverse movements in interest rates that affect the bank's non-trading portfolio.
LCR	Liquidity Coverage Ratio; a Basel III requirement that banks hold sufficient high-quality liquid assets to cover net cash outflows over a thirty-day stress period.
M&A	Mergers and Acquisitions.
MAP	Mediating Assessments Protocol; a structured decision-making process developed by Kahneman, Sibony, and Sunstein to reduce noise in professional judgement by requiring independent, evidence-based assessment before group deliberation.

MAS	Monetary Authority of Singapore; the central bank and financial regulatory authority of Singapore.
MCAS	Maneuvering Characteristics Augmentation System; the flight-control software on the Boeing 737 MAX designed to prevent aerodynamic stall, whose malfunction caused the Lion Air and Ethiopian Airlines crashes.
MiFID II	Markets in Financial Instruments Directive II; the European Union legislative framework governing investment services and activities across EU member states.
NATO	North Atlantic Treaty Organisation; the intergovernmental military alliance whose red-teaming and adversarial analysis doctrine provided a foundational methodology for the SGaaS Red Team Protocol.
NED	Non-Executive Director; a member of the board who does not form part of executive management and typically serves in a supervisory and advisory capacity.
OSFI	Office of the Superintendent of Financial Institutions; the federal regulatory agency responsible for supervising and regulating federally registered financial institutions in Canada.
PE	Private Equity; investment in companies not listed on a public stock exchange, typically through leveraged buyouts, growth equity, or venture capital.
PRA	Prudential Regulation Authority; the UK body responsible for the prudential regulation and supervision of banks, building societies, credit unions, insurers, and major investment firms.
ROIC	Return on Invested Capital; net operating profit after taxes divided by invested capital. The core measure of whether a company creates or destroys economic value relative to its cost of capital.
SEC	Securities and Exchange Commission; the US federal agency responsible for enforcing federal securities laws and regulating the securities industry.
SGaaS	Strategic Governance as a Service; the continuous, adversarial, principal-led governance function developed and originated by Marentis Labs, delivered at board level on a retained basis, whose mandate is to challenge assumptions, stress-test decisions, and surface failure modes in governance architecture before they materialise as organisational loss.
SM&CR	Senior Managers and Certification Regime; the UK regulatory framework that assigns individual accountability to senior managers at regulated financial services firms, with a statutory Duty of Responsibility for the areas within their remit.
SOX	Sarbanes-Oxley Act; US federal legislation enacted in 2002 establishing requirements for all US public company boards, management, and public accounting firms in response to the Enron and other accounting scandals.
SPV	Special Purpose Vehicle; a subsidiary entity created to isolate financial risk, commonly used in structured finance and off-balance-sheet arrangements.

SVB	Silicon Valley Bank; the California-based technology-focused bank that failed in March 2023, discussed in this paper as a case study in governance failure.
TIBER-EU	Threat Intelligence-Based Ethical Red-teaming; the European Central Bank's framework for conducting controlled, bespoke, intelligence-led red team tests on the critical live production systems of financial entities.
TLAC	Total Loss-Absorbing Capacity; the Basel Committee standard requiring systemically important banks to hold minimum levels of instruments capable of absorbing losses in the event of resolution.
WACC	Weighted Average Cost of Capital; the blended opportunity cost of a company's debt and equity financing, used as the discount rate in enterprise valuation and as the benchmark against which ROIC is measured.
TLPT	Threat-Led Penetration Testing; adversarial testing of critical functions based on bespoke threat intelligence, required by DORA for significant financial entities.

References

[1] Isabella Arndorfer and Andrea Minto. *The "Four Lines of Defence Model" for Financial Institutions: Taking the Three-Lines-of-Defence Model Further to Reflect Specific Governance Features of Regulated Financial Institutions*. Tech. rep. 11. FSI Occasional Paper No. 11. Basel, Switzerland: Financial Stability Institute, Bank for International Settlements, Dec. 2015. URL: https://www.bis.org/fsi/fsipapers11.htm.

[2] Ulrich Bantleon et al. "Coordination Challenges in Implementing the Three Lines of Defense Model". In: *International Journal of Auditing* 25.1 (2021), pp. 1–16. DOI: 10.1111/ijau.12201.

[3] Michael S. Barr. *Review of the Federal Reserve's Supervision and Regulation of Silicon Valley Bank*. Tech. rep. Washington, DC: Board of Governors of the Federal Reserve System, Apr. 2023. URL: https://www.federalreserve.gov/publications/files/svb-review-20230428.pdf.

[4] Max H. Bazerman, Kimberly P. Morgan, and George F. Loewenstein. "The Impossibility of Auditor Independence". In: *Sloan Management Review* 38.4 (1997), pp. 89–94.

[5] Glynis M. Breakwell. *The Psychology of Risk*. 2nd ed. Cambridge, UK: Cambridge University Press, 2014.

[6] André Brodeur et al. *A Board Perspective on Enterprise Risk Management*. Tech. rep. 18. McKinsey Working Papers on Risk, No. 18. New York, NY: McKinsey & Company, Feb. 2010.

[7] Gordon L. Clark, Andreas Feiner, and Michael Viehs. *From the Stockholder to the Stakeholder: How Sustainability Can Drive Financial Outperformance*. Tech. rep. Oxford, UK: University of Oxford Smith School of Enterprise, the Environment, and Arabesque Partners, Mar. 2015.

[8] Criminal Cases Review Commission. *Post Office Horizon Cases: CCRC Statement*. Criminal Cases Review Commission. Birmingham, UK, Apr. 2021.

[9] Delaware Court of Chancery. *In re Caremark International Inc. Derivative Litigation*. 698 A.2d 959 (Del. Ch. 1996). 1996.

[10] Delaware Court of Chancery. *In re McDonald's Corporation Stockholder Derivative Litigation*. C.A. No. 2021-0324-JTL (Del. Ch. Jan. 25, 2023). 2023.

[11] Delaware Court of Chancery. *In re The Boeing Company Derivative Litigation*. Consol. C.A. No. 2019-0907-MTZ (Del. Ch. Feb. 17, 2022). Settlement approved February 17, 2022; $237.5 million monetary settlement amount. Feb. 2022.

[12] Delaware Supreme Court. *Marchand v. Barnhill*. 212 A.3d 805 (Del. 2019). 2019.

[13] Delaware Supreme Court. *Stone v. Ritter*. 911 A.2d 362 (Del. 2006). 2006.

[14] Deutscher Bundestag, 3. Untersuchungsausschuss. *Abschlussbericht des Dritten Untersuchungsausschusses (Wirecard)*. Tech. rep. Drucksache 19/30900. Final report of the 3rd Parliamentary Committee of Inquiry, 19th electoral period. Berlin, Germany: Deutscher Bundestag, June 2021.

[15] European Parliament and Council of the European Union. *Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on Corporate Sustainability Due Diligence and Amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859*. Official Journal of the European Union, L 2024/1760. Entered into force 25 July 2024; member state transposition required by 26 July 2026. July 2024. URL: http://data.europa.eu/eli/dir/2024/1760/oj.

[16] European Parliament and Council of the European Union. *Directive 2014/65/EU on Markets in Financial Instruments (MiFID II)*. Official Journal of the European Union, L 173/349. Applicable from 3 January 2018. 2014.

[17] European Parliament and Council of the European Union. *Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data (GDPR)*. Official Journal of the European Union, L 119/1. Applicable from 25 May 2018. 2016.

[18] European Parliament and Council of the European Union. *Regulation (EU) 2022/2554 of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector and Amending Regulations (DORA)*. Official Journal of the European Union, L 333/1. Effective 17 January 2025. 2022.

[19] EY and Institute of International Finance. *Global Bank Risk Management Survey*. Tech. rep. EY and Institute of International Finance, 2025.

[20] Federal Deposit Insurance Corporation. *Federal Deposit Insurance Corporation v. Becker et al.* U.S. District Court, N.D. California. Case No. 5:25-cv-569. FDIC complaint as receiver for Silicon Valley Bank. All claims are allegations; no adjudication has occurred as of May 2026. 2025.

[21] Greg Feldberg, Carey K. Mott, and Jill Cetina. "How US Bank Regulation Failed SVB and Its Supervisors". In: *Journal of Financial Crises* 7.2 (2025). Published 25 June 2025, pp. 313–355. DOI: 10.17132/2693-3179.1658.

[22] Financial Conduct Authority and Prudential Regulation Authority. *Senior Managers and Certification Regime (SM&CR)*. Financial Conduct Authority and Prudential Regulation Authority. Extended to all FCA-regulated firms from December 2019. London, UK, 2019.

[23] Financial Reporting Council. *UK Corporate Governance Code*. Financial Reporting Council. Code effective 1 January 2025; Provision 29 effective 1 January 2026. London, UK, Jan. 2024.

[24] Financial Services Agency (Japan). *Action Programme for Corporate Governance Reform 2025*. Tech. rep. Tokyo, Japan: Financial Services Agency, June 2025.

[25] Grand View Research. *Governance, Risk Management and Compliance Market Size, Share & Trends Analysis Report*. Tech. rep. Grand View Research, 2025.

[26] Michael Grimwade. "Approaches for Quantifying the Financial Impacts of Reputational Damage from Climate Change". In: *Journal of Risk Management in Financial Institutions* 16.2 (2023), pp. 138–157. ISSN: 1752-8887.

[27] Michael Grimwade. *How Can Effective Operational Risk Management Genuinely Deliver Commercial Value?* Practitioner article. LinkedIn. 2025. URL: https://www.linkedin.com/posts/michael-grimwade-a0661a17_how-can-op-risk-management-deliver-commercial-activity-7451540211920130048-Lh9L (visited on 04/27/2026).

[28] Bryce G. Hoffman. *Red Teaming: How Your Business Can Conquer the Competition by Challenging Everything*. New York, NY: Crown Business, 2017.

[29] House of Commons Business, Energy and Industrial Strategy Committee and Work and Pensions Committee. *Carillion*. Tech. rep. HC 769-I. First Joint Report of Session 2017–19. London, UK: House of Commons, May 2018.

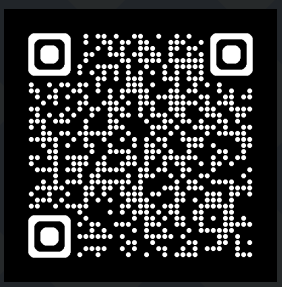
[30] Stefan Hunziker et al. *Corporate Crises in Germany, Austria, and Switzerland: Empirical Evidence on Risk Drivers. ERM Report 2025*. Tech. rep. In cooperation with HAW Kiel (Institut für Controlling) and Swiss GRC. Rotkreuz, Switzerland: Institute of Financial Services Zug IFZ, Lucerne School of Business, 2025.

[31] Institute of Internal Auditors. *Internal Audit Vision 2035: Creating Our Future Together*. Tech. rep. Lake Mary, FL: Internal Audit Foundation, 2024. URL: https://ia-vision2035.org/.

[32] Institute of Internal Auditors. *North American Pulse of Internal Audit 2026*. Tech. rep. Lake Mary, FL: Internal Audit Foundation, 2026. URL: https://www.theiia.org/.
[33] Institute of Internal Auditors. *The IIA's Three Lines Model: An Update of the Three Lines of Defense*. Tech. rep. Lake Mary, FL: Institute of Internal Auditors, July 2020. URL: https://www.theiia.org/.
[34] Daniel Kahneman. *Thinking, Fast and Slow*. New York, NY: Farrar, Straus and Giroux, 2011.
[35] Daniel Kahneman, Olivier Sibony, and Cass R. Sunstein. *Noise: A Flaw in Human Judgment*. New York, NY: Little, Brown Spark, 2021.
[36] Robert S. Kaplan and Anette Mikes. "Managing Risks: A New Framework". In: *Harvard Business Review* 90.5 (May 2012), pp. 48–60.
[37] Gary Klein. "Performing a Project Premortem". In: *Harvard Business Review* 85.9 (2007), pp. 18–19.
[38] David R. Koenig. *Governance Reimagined: Organizational Design, Risk, and Value Creation*. 2nd ed. (b)right governance publications, 2018.
[39] KPMG. *Report Concerning the Independent Special Investigation, Wirecard AG, Munich*. Tech. rep. Commissioned by Wirecard's supervisory board; delivered 28 April 2020. Munich, Germany: KPMG, Apr. 2020. URL: https://web.archive.org/web/20220307204458/https://www.wirecard.com/uploads/Bericht_Sonderpruefung_KPMG_EN_200501_Disclaimer.pdf.
[40] KPMG LLP. *The 2025 SOX Survey*. Tech. rep. KPMG LLP, 2025.
[41] Katja Langenbucher and Christian Leuz. *Wirecard Scandal: When All Lines of Defence Against Corporate Fraud Fail*. Oxford Business Law Blog, University of Oxford. Oxford, UK, Nov. 2020. URL: https://blogs.law.ox.ac.uk/business-law-blog/blog/2020/11/wirecard-scandal-when-all-lines-defense-against-corporate-fraud-fail.
[42] LexisNexis Risk Solutions. *True Cost of Financial Crime Compliance*. Tech. rep. LexisNexis Risk Solutions, 2023.
[43] Ryan Luttenton, Stefany Samp, and Alexa Stone. *From Guidance to Action: Exploring Practical Enterprise Risk Management*. Tech. rep. Content and design contributions by Crowe LLP. Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2026.
[44] Anna Marks, Lara Abrash, and Arno Probst. *Governance of AI: A Critical Imperative for Today's Boards*. Tech. rep. London: Deloitte Global Boardroom Program, 2025.
[45] Michael J. Mauboussin and Dan Callahan. *Competitive Advantage Period: The Neglected Value Driver*. Tech. rep. Consilient Observer series. Counterpoint Global Insights, Morgan Stanley, Apr. 2026.
[46] Maggie McGrath. "Wells Fargo Admits to More Unauthorized Accounts, Increasing Tally to 3.5 Million". In: *Forbes* (Aug. 2017). URL: https://www.forbes.com/sites/maggiemcgrath/2017/08/31/wells-fargo-admits-to-more-unauthorized-accounts-increasing-tally-to-3-5-million/ (visited on 05/14/2026).
[47] McKinsey & Company. *Perspectives on Merger Integration*. Tech. rep. McKinsey & Company, 2010.
[48] Andrew Metrick. "The Failure of Silicon Valley Bank and the Panic of 2023". In: *Journal of Economic Perspectives* 38.1 (2024), pp. 133–152. DOI: 10.1257/jep.38.1.133.
[49] *Mind the Gap: CAE Strategies for Fortifying Audit Committee Relationships*. Practitioner blog post. Optro. 2026. URL: https://optro.ai/blog/mind-the-gap-cae-strategies-fortifying-audit-committee-relationships (visited on 05/14/2026).

[50] Deborah J. Mitchell, J. Edward Russo, and Nancy Pennington. "Back to the Future: Temporal Perspective in the Explanation of Events". In: *Journal of Behavioral Decision Making* 2.1 (1989), pp. 25–38.
[51] Monetary Authority of Singapore. *Guidelines on Outsourcing (Banks)*. Monetary Authority of Singapore. Singapore, Dec. 2023.
[52] Office of Inspector General, Board of Governors of the Federal Reserve System. *Material Loss Review of Silicon Valley Bank*. Tech. rep. Evaluation Report 2023-SR-B-013. Washington, DC: Board of Governors of the Federal Reserve System, Sept. 2023. URL: https://oig.federalreserve.gov/reports/board-material-loss-review-silicon-valley-bank-sep2023.pdf.
[53] Ponemon Institute. *The True Cost of Compliance with Data Protection Regulations*. Tech. rep. Ponemon Institute, 2017.
[54] Karl R. Popper. *Conjectures and Refutations: The Growth of Scientific Knowledge*. London: Routledge and Kegan Paul, 1963.
[55] Karl R. Popper. *The Open Society and Its Enemies*. Reprint ed. 2011. London: Routledge, 1945.
[56] Michael Power. *Organized Uncertainty: Designing a World of Risk Management*. Oxford, UK: Oxford University Press, 2007.
[57] Michael Power. *The Audit Society: Rituals of Verification*. Oxford, UK: Oxford University Press, 1997.
[58] PricewaterhouseCoopers. *Continuous Monitoring and Compliance Cost Reduction*. Tech. rep. London, UK: PricewaterhouseCoopers, 2023.
[59] PricewaterhouseCoopers. *Global Risk Survey*. Tech. rep. London, UK: PricewaterhouseCoopers, 2024.
[60] Peter Schwartz. *The Art of the Long View: Planning for the Future in an Uncertain World*. New York, NY: Doubleday, 1991.
[61] Shearman & Sterling LLP. *Independent Directors of the Board of Wells Fargo & Company Sales Practices Investigation Report*. Tech. rep. Prepared by Shearman & Sterling LLP on behalf of the independent directors of the Board of Directors of Wells Fargo & Company. New York, NY: Wells Fargo & Company (Independent Directors), Apr. 2017. URL: https://www08.wellsfargomedia.com/assets/pdf/about/investor-relations/presentations/2017/board-report.pdf.
[62] Herbert A. Simon. *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations*. New York, NY: Macmillan, 1947.
[63] James Surowiecki. *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*. New York, NY: Doubleday, 2004.
[64] Swiss Financial Market Supervisory Authority (FINMA). *FINMA Report: Lessons Learned from the CS Crisis*. Tech. rep. Bern, Switzerland: Swiss Financial Market Supervisory Authority (FINMA), Dec. 2023. URL: https://www.finma.ch/en/news/2023/12/20231219-mm-lehren-aus-der-cs-krise/.
[65] Nassim Nicholas Taleb. *The Black Swan: The Impact of the Highly Improbable*. New York, NY: Random House, 2007.
[66] Philip E. Tetlock and Dan Gardner. *Superforecasting: The Art and Science of Prediction*. New York, NY: Crown Publishers, 2015.
[67] Thomson Reuters Regulatory Intelligence. *Cost of Compliance Report 2023*. Tech. rep. Published under the Thomson Reuters Regulatory Intelligence imprint; subsequently rebranded as LSEG Regulatory Intelligence in 2023. Thomson Reuters Regulatory Intelligence, 2023.

[68] U.S. Department of Justice. *Deferred Prosecution Agreement: United States of America v. The Boeing Company*. No. 21-cr-005-O (N.D. Tex. filed Jan. 7, 2021). Jan. 2021.
[69] U.S. House Committee on Transportation and Infrastructure. *Final Committee Report: The Boeing 737 MAX: A Failure of Management, Engineering Culture, and the FAA's Aircraft Certification Process*. Tech. rep. Washington, DC: U.S. House of Representatives, 2020.
[70] United Kingdom Parliament. *Post Office (Horizon System) Offences Act 2024*. 2024 c. 14. Received Royal Assent 24 May 2024. 2024.
[71] United States Congress. *Dodd-Frank Wall Street Reform and Consumer Protection Act*. Pub. L. No. 111-203, 124 Stat. 1376. Signed into law 21 July 2010. 2010.
[72] University of Foreign Military and Cultural Studies. *Red Team Handbook*. Tech. rep. Multiple editions; 2012 edition cited. Fort Leavenworth, KS: U.S. Army University of Foreign Military and Cultural Studies, Fort Leavenworth, 2012.
[73] Elizabeth Warren. *Letter to Chair Jerome Powell Regarding Federal Reserve Accountability for Silicon Valley Bank Failures*. U.S. Senate Committee on Banking, Housing, and Urban Affairs. Ranking Member letter. Sources management conduct claims to *FDIC v. Becker et al.*, Case No. 5:25-cv-569. Washington, DC, Mar. 2025.
[74] Sir Wyn Williams. *Post Office Horizon IT Inquiry: Final Report*. Tech. rep. HC 1119. London, UK: Post Office Horizon IT Inquiry, July 2025. URL: https://www.postofficehorizoninquiry.org.uk/.
[75] World Economic Forum. *The Global Risks Report 2026*. Tech. rep. In collaboration with Marsh McLennan and Zurich Insurance Group. Geneva, Switzerland: World Economic Forum, Jan. 2026.
[76] WTW. *Insurance Marketplace Realities 2025*. Tech. rep. London, UK: WTW (Willis Towers Watson), 2025.
[77] Micah Zenko. *Red Team: How to Succeed by Thinking Like the Enemy*. New York, NY: Basic Books, 2015.



Marentis Labs Ltd
Registered in England and Wales
Company Number: 16600357
Registered Address: 167–169 Great Portland Street,
5th Floor, London, UK, W1W 5PF