RAIS Journal for Social Sciences | VOL. 9, No. 2, 2025
ISSN 2574-0245 (Print) | ISSN 2574-1179 (Online) | DOI: 10.5281/zenodo.17468923

# Dynamic Modulation of Imperceptible Risks: Theoretical Foundations and a Rheostat Analogy

**Laura A. JONES**

*Capitol Technology University, Laurel, Maryland, USA*
*ORCID: https://orcid.org/0000-0002-0299-370X*

**Abstract:** This concept paper advances theoretical understanding of imperceptible risk dynamics by conceptualizing risk modulation through a rheostat-inspired lens, addressing the complex interplay between latent risk vectors and organizational vulnerability. Despite increasing sophistication in risk governance, conventional frameworks often fail to adequately capture gradual or low-velocity risks that silently accumulate and evade early detection, ultimately undermining strategic resilience. By synthesizing principles from adaptive systems theory and risk velocity research, the study introduces a novel analogy wherein risk exposure and aligned responses are continuously modulated in response to evolving internal and external stimuli, akin to the subtle, regulator-like function of a rheostat. The theoretical foundations laid herein interrogate prevailing risk taxonomies, articulate the shortcomings of static assessment approaches, and propose actionable insights for both researchers and risk practitioners. Designed for an interdisciplinary audience at the nexus of risk management, organizational science, and cybersecurity, this work invites critical reflection on dynamic measurement, anticipatory governance, and the future of imperceptible risk intervention.

**Keywords:** Continuum Of Calibration, Dynamic Modulation, Imperceptible Risk, Risk Management, Risk Rheostat, Theoretical Foundations

## Introduction

Across the hyper-transmogrified landscape of organizational risk, the capacity to anticipate, interpret, and modulate emergent threats has become indispensable for ensuring sustained resilience and strategic advantage. Conventional risk management frameworks, often rooted in static models and backward-looking assessments, are increasingly outpaced by the sheer velocity and complexity of modern risk environments (Kaplan & Mikes, 2023). Recent empirical research has revealed that latent and imperceptible risks, by their very nature, are challenging to quantify or forecast and now account for a significant proportion of operational disruptions and strategic failures (Frigo & Anderson, 2023). Within the past five years, industry reports indicate that over 60% of organizations have experienced notable losses arising from previously unrecognized risks, with annual financial impact estimates exceeding $200 billion globally (COSO, 2024).

A combination of factors drives this surge in unforeseen risk exposure: accelerating technological change, the proliferation of interconnected systems, increasingly dynamic threat actors, and the volatile interplay of global market forces (Lam, 2023). As organizational ecosystems become more complex and interconnected, the traditional reliance on static controls and episodic risk reviews falls short of providing the adaptive protection required for today's turbulent environment (Burton, 2025; Power, 2022). The consequences are far-reaching, not only in terms of financial harm but also in innovation stagnation, erosion of stakeholder confidence, and diminished organizational agility

(Hubbard, 2024; Jones, 2020; Lam, 2023). These realities underscore an urgent need for effective frameworks that enable the continuous and real-time modulation of risk exposure.

Despite mounting evidence of these challenges, scholarly analyses consistently highlight a critical gap: the absence of actionable, empirically validated tools for dynamic risk calibration (Frigo & Anderson, 2023; Power, 2022). Existing models, although effective in static or slowly evolving contexts, often fail to provide leaders with sufficient foresight or operational flexibility to respond to ambiguous, low-visibility threats (Kaplan & Mikes, 2023). This gap is particularly acute in sectors such as finance, healthcare, and critical infrastructure, where the cost of failing to detect and manage latent risks can escalate rapidly with cascading effects (COSO, 2024).

This study addresses this pressing need by critically examining adaptive risk frameworks, with a specific focus on the rheostat analogy as a conceptual and analytical tool for continuous risk modulation. Drawing on an interdisciplinary synthesis of peer-reviewed research from the past five years, the paper situates itself at the nexus of risk management, organizational behavior, and systems theory. The aim is to generate new insights into the mechanisms, benefits, and practical applications of dynamic risk calibration, thereby contributing not only to academic scholarship but also to the evolving toolkit available for organizational leaders charged with safeguarding value in an environment where change is the only constant.

## Methodology and Research Design

This study employs a rigorous literature review methodology, purposefully designed to synthesize and critically evaluate the current body of knowledge (Snyder, 2024) concerning the dynamic modulation of imperceptible and emergent risks within organizational settings. The research process begins with the systematic identification of peer-reviewed journal articles, authoritative books, and current industry reports (Paul & Barari, 2022) published over the past seven years, leveraging digital databases such as Scopus, Web of Science, and Google Scholar. Targeted search terms, including "dynamic risk management," "rheostat," "imperceptible risk," and "organizational resilience," guide the selection process, ensuring comprehensive coverage of both foundational theories and recent advancements in the field. After the initial collection, sources were screened according to defined inclusion criteria, including scholarly rigor, contemporary relevance, empirical or conceptual contributions to adaptive risk management, and clear articulation of frameworks or mechanisms related to risk calibration. Each document underwent review for consistency to determine relevance (Lyndgaard & Kanfer, 2024).

The analytic phase deployed thematic coding and comparative synthesis, examining key elements such as conceptual definitions, methodological diversity, mechanisms of risk modulation, evidence of practical implementation, and real-world outcomes. Attention is paid to both the convergences and divergences across disciplines, allowing for critical interrogation of how adaptive frameworks, particularly those drawing on the rheostat analogy, address the complexity and velocity of modern risk environments. The review is structured to highlight gaps, limitations, and frontier debates, while maintaining its primary focus on extracting actionable design principles and evaluative criteria for organizational leaders. Throughout, the research design adheres to established standards for qualitative synthesis, striving for transparency, reproducibility, and analytic depth. The ultimate aim is to generate a meticulously documented, high-impact contribution that not only consolidates current scholarship but also advances the strategic and operational discourse on risk calibration in volatile contexts. The implications for managing rheostat risks include the potential to modulate imperceptible risk, reducing organizational risk, and increasing resilience.

## Problem Statement

The persistent challenge in organizational risk management is highlighted by empirical studies, which show that significant operational disruptions often arise from imperceptible and emergent risks that conventional frameworks fail to address. For instance, research by Power (2022) reveals that traditional risk assessment models inadequately capture low-visibility risk vectors, contributing to a gap in continuous risk recalibration necessary for adaptive governance. Similarly, Frigo and Anderson (2023) document an increasing frequency of latent risks materializing unexpectedly, underscoring limitations in static control systems and the need for dynamic risk management strategies. Furthermore, scholarly analyses suggest that approximately 68% of senior executives recognize deficiencies in methodological tools for real-time risk adjustment, which correlates with declines in organizational agility and increases in unplanned disruptions (Hubbard, 2024; Lam, 2023). Empirical data link these shortcomings with broader consequences, such as decreased innovation capacity and amplified exposure to cyber and operational threats (COSO, 2024; Kaplan & Mikes, 2023).

This research addresses these documented gaps by proposing the development and validation of the risk rheostat framework, intended as both a heuristic and analytic instrument for continuously modulating risk exposure in complex environments. Grounded firmly in the current academic discourse, this study aims to equip organizational leaders with evidence-based methodologies to anticipate, assess, and proactively manage imperceptible risks. Addressing this problem responds to a critical need for enhanced resilience. It supports the advancement of adaptive risk governance theories, which are essential for sustaining a competitive advantage and safeguarding organizational value in uncertain and volatile contexts.

## Purpose Statement

The purpose of this paper is to systematically investigate the dynamic modulation of imperceptible and emergent risks in contemporary organizational contexts through a comprehensive literature review methodology. By synthesizing current peer-reviewed research published within the past seven years, the study aims to elucidate how adaptive risk frameworks, specifically those employing rheostat analogies, can enable organizations to transcend static threat models in favor of continuous calibration and strategic foresight. The central objective is to clarify the mechanisms and practical value of risk modulation, drawing on interdisciplinary evidence from risk management, systems theory, and leadership studies. This inquiry is motivated by the urgent need for evidence-based approaches that can proactively identify, interpret, and respond to subtle or low-velocity risk vectors that traditional models often overlook. Anchored in contemporary scholarly discourse, this review aims not only to advance theoretical understanding but also to provide actionable insights for leaders and practitioners navigating environments characterized by volatility and uncertainty. The research evaluates the strengths and limitations of existing frameworks, details the implications of rheostat-inspired models for both governance and operational resilience, and proposes criteria by which organizations can measure the effectiveness of their risk calibration efforts. Ultimately, this paper aims to bridge the conceptual and practical divides in the discipline, guiding future inquiry and equipping decision-makers with the orientation and tools required to safeguard organizational value in an increasingly complex risk landscape.

## Significance and Rationale for Theory, Practice, and Policy

The rationale for this study rests on the recognition that imperceptible risks are defining features of modern organizational life. Static approaches fail in such contexts, but dynamic

modulation provides a viable alternative. The rheostat, a variable resistor that modulates electrical current by incorporating adjustable resistance into a circuit, serves as a primary metaphor (IEEE, 1996). Adjusting resistance parallels the managerial process of calibrating risk tolerance, whereby decision-makers can gradually increase or decrease their risk tolerance, directly affecting the scale of opportunities and threats within the organizational environment. This parallelism emphasizes the significance of deliberate, incremental risk management, enabling strategic responsiveness and flexibility in dynamic environments. The rheostat metaphor offers leaders a vivid and adaptable tool for guiding decisions. The significance of this research lies in its contributions to both theory and practice, as well as its implications for policies. The study of dynamic risk modulation holds significance across three domains: theoretical contribution, practical relevance, and policy implications.

### *Theoretical Contribution*

This theoretical contribution advances risk theory by positioning modulation, rather than prediction or elimination, as the primary mode of managing imperceptible risks. The rheostat analogy offers a conceptual scaffold that bridges disparate theories of resilience, sensemaking, and dynamic capabilities.

### *Practical Relevance*

For leaders in highly regulated industries such as healthcare, finance, technology, aviation, aerospace, and government, the metaphor offers a pragmatic lens to guide decisions. Instead of static policies, it suggests a flexible calibration of monitoring and controls (Van Calster et al., 2016), as well as innovation tailored to real-time conditions.

### *Policy Implications*

Regulators and policymakers increasingly encounter the challenge of setting standards under uncertainty (e.g., cybersecurity mandates, pandemic protocols, and climate disclosures). A rheostat framework could inform adaptive regulation, recognizing that *risk tolerance*, the specific maximum risk that an organization is willing to take in pursuit of its objectives (International Organization for Standardization, 2018; Darroch & Finnie, 2021), must be variable and context-sensitive rather than fixed.

## Nature of the Study

The nature of this study is qualitative, structured as a comprehensive literature review to elucidate the dynamic modulation of imperceptible and emergent risks within contemporary organizations. This approach is grounded in interpretivist philosophical underpinnings, leveraging the principles of thematic synthesis and narrative integration to explore how adaptive, rheostat-inspired risk frameworks are conceptualized, operationalized, and critiqued across scholarly domains. This methodology is well-suited to the research problem, as it enables a nuanced exploration of evolving theoretical models and practical tools derived from a diverse range of interdisciplinary sources, including risk management, systems theory, and organizational leadership. The review systematically identifies, selects, and analyzes peer-reviewed literature published within the past seven years, employing defined search terms such as “dynamic risk management,” “imperceptible risk,” and “rheostat model” across academic databases like Scopus, Web of Science, and Google Scholar. Inclusion criteria mandate scholarly rigor, contemporary relevance, and explicit contribution to the understanding of risk calibration, while exclusion criteria eliminate sources lacking peer review or empirical grounding. The process incorporates iterative screening, citation tracking, and thematic coding to ensure both breadth and analytic depth. The scope of the examination is delineated by its focus on publications that address the

mechanisms, applications, and critiques of adaptive risk modulation strategies relevant to volatile organizational environments.

To maximize transparency and reproducibility, the methodology explicitly documents search strategies, temporal boundaries (covering the past five years), and analytic frameworks that guide evidence synthesis. The review's analytical lens is shaped by ongoing debates in resilience engineering and organizational sensemaking, offering a robust foundation for drawing integrative, evidence-based conclusions. Acknowledging inherent limitations, such as potential publication bias and linguistic boundaries, the study aspires to generate transferable insights, support scholarly advancement, and inform practice in risk governance and adaptive systems leadership.

## Literature Review

### *Early Actuarial and Probabilistic Models*

The earliest systematic approaches to risk management emerged in the seventeenth and eighteenth centuries, coinciding with the development of probability theory and actuarial science. Thinkers such as Blaise Pascal and Pierre de Fermat began to frame risk as measurable uncertainty (Mathieu & Miermont, 2023), while Jacob Bernoulli introduced the law of large numbers (Kitagawa, 2022). These foundations allowed insurers and financiers to use mathematical models to predict the likelihood of adverse events. Actuarial tables, first applied in the context of life insurance, enabled institutions to calculate expected losses and distribute risk across broad populations (Kitagawa, 2022; Leung, 2021). A practical example of this early model can be seen in the operations of Lloyd's of London in the eighteenth century (Leonard, 2022). Merchants and shipowners pooled premiums to protect against losses from maritime risks such as shipwrecks, piracy, or storms. The ability to quantify probabilities made the pooling of resources feasible and efficient, providing stability for long-distance trade. The limitations of these models are significant when viewed through a contemporary lens. These methods were essentially static, focusing on the frequency and severity of known risks and offered little in the way of foresight for systemic or emergent risks. As a result, they left organizations vulnerable to disruptive events that fell outside predictable patterns, such as sudden political upheavals or new forms of technological disruption. The actuarial approach created a foundation for modern risk management, but it was too narrow to accommodate the complexities of dynamic organizational environments.

### *Risk as Uncertainty*

In 1921, economist Frank Knight introduced a critical conceptual breakthrough by distinguishing between measurable risks and true uncertainties. According to Knight, risks are situations in which probabilities can be assigned to outcomes, while uncertainties are those in which outcomes cannot be quantified. This framework emphasized that many business decisions involve uncertainty rather than calculable risk, thereby underscoring the limitations of actuarial and probabilistic methods. An entrepreneur who invests in a new technology provides a useful illustration of this distinction. The probability of success or failure in such a venture cannot be reliably measured, unlike the risk of fire or illness, where probabilities are established through historical data. Knight's framework highlighted that managerial decision-making often takes place under conditions of uncertainty, where decision-makers rely on judgment, experience, and creativity rather than statistical calculation. The flaw in traditional risk management practices revealed by Knight's theory is their overemphasis on measurable risks. By focusing only on quantifiable variables, organizations often ignored or underestimated the impact of true uncertainties. This created blind spots in strategic planning and made firms vulnerable to disruptive shocks that

historical probability distributions could not capture. The Knightian distinction reframed the way scholars and practitioners began to think about the limits of risk measurement and the need for broader approaches to managing uncertainty.

### *The Risk Management Process Model*

By the mid-twentieth century, corporate risk management began to coalesce into a standardized process model. This model consisted of four steps: risk identification, risk assessment, risk control, and risk financing. The framework represented an effort to systematize risk management practices across industries and became particularly central in the fields of insurance and corporate governance. A manufacturing company provides a clear example of this process in action. The firm might begin by identifying the risk of fire within its facilities, then assessing the likelihood and potential severity of such an event. It would proceed to implement preventive controls such as fire sprinklers and finally purchase insurance to transfer the residual financial risk. This systematic process allowed organizations to address risk in a structured and repeatable manner. Despite its usefulness, the process model suffered from important limitations. It tended to be siloed, treating risks as independent events rather than interconnected phenomena. The model did not sufficiently account for systemic risks, such as the cascading effects of supply chain disruptions or financial contagion. In practice, this narrow approach often resulted in firms addressing surface-level vulnerabilities without recognizing how risks could amplify one another in complex organizational systems.

### *Modern Portfolio Theory*

In 1952, Harry Markowitz introduced Modern Portfolio Theory (MPT), which reshaped the understanding of financial risk by conceptualizing it as variance in asset returns. The central insight of this theory was that diversification reduces risk, since holding a portfolio of assets with uncorrelated movements smooths out volatility and lowers overall exposure. This mathematical approach to balancing risk and return became a cornerstone of modern financial management. An investment fund illustrates how MPT works in practice. By combining equities, bonds, and commodities, the fund manager reduces the impact of any single asset's decline on the overall portfolio. For example, when stock markets fall, government bonds often increase in value, providing a stabilizing counterbalance. In this way, MPT operationalized the principle that investors can manage risk more effectively through diversification than through individual asset selection. The limitations of MPT became glaring during the global financial crisis of 2008. The theory assumes normal distributions of returns and rational actors, which underestimates the possibility of extreme, systemic events. In times of crisis, correlations between asset classes increase dramatically, undermining the very foundation of diversification. This flaw demonstrated that while MPT provides powerful tools for everyday risk management, it fails to protect against rare but catastrophic events that emerge during systemic breakdowns.

### *High Reliability Organization Theory*

By the 1980s and 1990s, scholars studying industries such as nuclear power, aviation, and firefighting developed the concept of High Reliability Organizations (HROs). This theory sought to explain how organizations operating in high-risk environments achieved consistently low error rates. HROs were characterized by redundancy, deference to expertise, constant vigilance, and an organizational culture that emphasized mindfulness about potential failures. Air traffic control offers a striking example of an HRO in practice. Controllers are trained to constantly cross-check data, defer to frontline staff with specialized knowledge when anomalies arise, and build redundancy into systems to prevent

accidents. These practices enable air traffic systems to maintain extremely low accident rates despite the inherent dangers of managing thousands of flights simultaneously.

The challenges of adopting HRO practices lie in their cost and scalability. Building redundancy and cultivating a culture of mindfulness require significant resources, training, and organizational commitment. While highly effective in industries where failure is catastrophic, such as aviation or nuclear energy, many commercial sectors resist such rigor because of the perceived costs and competitive pressures. For example, the aviation and aerospace sectors face significant cybersecurity threats that can substantially impact personal safety and national security (Burton, 2025). These hazards are highlighted by recent events, such as the 2023 Boeing data breach (Baran, 2025; Burton, 2025; Petkauskas, 2023) and the 2024 ransomware assault at Seattle-Tacoma Airport (Burton, 2025; Lambert, 2024). Thus, while HRO theory advanced understanding of organizational reliability, it remains unevenly applied outside safety-critical industries.

### *Enterprise Risk Management*

In the 1990s and 2000s, Enterprise Risk Management (ERM) emerged as a comprehensive framework that integrated risk management across the entire organization. Unlike earlier models that addressed risks in isolation, ERM sought to align risk management with strategic objectives and account for interdependencies between financial, operational, and reputational risks (Jones, 2020). Frameworks such as COSO ERM and ISO 31000:2018 (International Organization for Standardization, 2018) provided formal structures for this holistic approach. Despite its promise, ERM has often fallen short of its potential. In many organizations, ERM has devolved into a compliance exercise, resulting in extensive risk registers that fail to influence actual decision-making. As a result, companies frequently underestimate or ignore rare, catastrophic risks. The challenge of translating ERM principles into actionable strategic guidance remains one of its most significant limitations.

### *Behavioral Risk Theories*

The emergence of behavioral economics in the late twentieth century provided another essential perspective on risk management. Daniel Kahneman and Amos Tversky's Prospect Theory, introduced in 1979, demonstrated that individuals systematically deviate from rational decision-making (Barberis et al., 2021). People tend to outweigh losses relative to gains and misjudge probabilities, leading to flawed assessments of risk. An instructive example is the dot-com bubble of the late 1990s. Investors, driven by herd behavior and cognitive biases, underestimated downside risks and poured capital into unproven companies. This behavior created inflated asset valuations that eventually collapsed, illustrating the real-world consequences of decision-making distortions described by *Prospect Theory* (Barberis et al., 2021; Kahneman & Tversky, 2013). Although behavioral theories revealed the cognitive flaws underlying risk assessment, they offered limited prescriptive guidance for organizations. Correcting biases on an organizational scale remains challenging, and firms often lack the tools to counteract irrational behavior systematically. The need persists for human-factor strategies, ethical accountability, and legal compliance, summoning organizations to employ a holistic defense strategy that addresses both technical and human behavioral risks (Burrell, 2024; Burton, 2025).

### *Complex Systems and Resilience Thinking*

In the early twenty-first century, risk scholars increasingly emphasized resilience and complexity theory. Organizations can be viewed as complex adaptive systems, in which risks can cascade in nonlinear ways. The focus shifted from attempting to predict and control every possible risk to building adaptive capacity and resilience in the face of uncertainty. The COVID-19 pandemic provides a compelling example of resilience

thinking in practice (Burrell, 2024). Organizations with flexible supply chains, capable of switching suppliers or digitizing operations, were able to adapt and survive in ways that rigid, just-in-time models could not. The COVID-19 pandemic has underscored that although medical equipment, medications, and supplies can preserve life, their efficacy depends on their rapid and efficient distribution to individuals in urgent need (Burrell, 2024; Kennedy-Sims, 2021). This highlighted the importance of agility and adaptability in managing organizational risk in a complex global environment. The challenge of resilience frameworks is that they often lack quantifiable metrics, making them difficult to institutionalize. Without clear operational guidance, resilience risks become more of a broad aspiration than a concrete management strategy. Nonetheless, resilience thinking represents a critical evolution in the history of risk management, particularly in its recognition of systemic complexity.

### *Critical Reflections on Older Practices*

Taken together, these theories and models reveal both progress and persistent challenges in the history of risk management research. Early actuarial and probabilistic models provided the foundation for measuring and distributing risk but ignored uncertainty and systemic complexity. The process model and portfolio theory standardized practices and introduced mathematical rigor, yet they underestimated interconnections and tail risks. Behavioral theories revealed the human biases that distort decision-making, while ERM and resilience frameworks offered holistic approaches to managing risks across organizations. The flaws of older practices lie primarily in their assumptions of predictability, linearity, and rationality. Real-world crises such as financial collapses and global pandemics have consistently demonstrated that risks interact in unpredictable and cascading ways. Modern approaches have sought to address these flaws, but they too face limitations in terms of cost, measurement, and implementation. The history of risk management demonstrates an ongoing struggle to balance the measurable and the uncertain, the rational and the behavioral, and the predictive and the adaptive (Jones, 2020).

Recent scholarship highlights a profound evolution in risk management thought, as organizations grapple with multifaceted and imperceptible threats that evade static categorization and traditional mitigation strategies. Rather than anchoring risk governance in fixed taxonomies, contemporary models emphasize a fluid continuum of vulnerability and opportunity, one where the very notion of risk now implies dynamic calibration and continuous oversight. The rheostat analogy, emerging as a conceptual milestone, illuminates this paradigm shift by positing risk as an adjustable spectrum, refracted through the lenses of leadership judgment, organizational controls, feedback systems, and strategic ambition, all in real-time. Within this framework, organizations become not only observers but also active choreographers of their risk exposure, attuned to shifting signals in the business environment that often remain beneath the threshold of conventional detection.

A closer inspection of interdisciplinary literature reveals that theories such as adaptive systems, *Normal Accident Theory* (Bianchi et al., 2023), and dynamic capabilities inform the foundation of the rheostat model. Scholars draw on resilience engineering to emphasize that systems must be able to absorb subtle disturbances, not just withstand visible shocks. High Reliability Organization research further demonstrates the vital importance of redundancy and situational awareness, a posture mirrored in the incremental adjustments of the risk rheostat. Cognitive perspectives, ranging from Prospect Theory to the sensemaking literature, reinforce that risk responses are filtered through subjective frames, losses and gains are calibrated not only by data alone, but also by how leaders perceive the ambiguous contours of threat. The Cynefin framework extends this insight, revealing how imperceptible risks often lurk within complex and emergent domains, where experimental modulation must replace linear protocols.

Practical frameworks, such as ISO 31000:2018, emphasize the importance of iterative, context-dependent risk management. The modern risk management framework mandates more than identification and categorization; it advocates continuous measurement, periodic reassessment, and adaptive mitigation aligned with systemic feedback loops. In this expanded landscape, the risk rheostat metaphor proves instructive, enabling leaders to oscillate between high resistance (preservation and compliance) and low resistance (experimentation and opportunity), always guided by the latest intelligence from key risk indicators, scenario analyses, and governance reports. Rather than relying on the binary assignment of risk, organizations deploy nuanced controls, recalibrating their tolerance and appetite to seize value while guarding against the silent erosion of resilience. The literature affirms that risk orchestration, anchored in deliberate, evidence-driven modulation, now stands as the strategic imperative for organizations navigating the volatility and ambiguity of contemporary enterprise contexts.

### *Gap in the Literature and Unresolved Issues*

Despite the breadth of theories on risk and resilience, a gap remains in the scholarship. Existing approaches often treat risk appetite as fixed statements, compliance thresholds, or binary decisions, when in reality, leaders constantly "turn the dial" of exposure depending on feedback, signals, and evolving contexts. Much of the existing literature focuses on either macro-level analyses of systemic risk (e.g., Beck's risk society) or micro-level practices in high-reliability settings. While risk management literature is extensive, gaps persist. First, existing frameworks essentially treat risk appetite as static or codified in statements and compliance thresholds (Power, 2007). Few studies examine how leaders dynamically modulate exposure in real time, especially when risks remain invisible. Second, while concepts like resilience and sensemaking emphasize adaptation, they often lack a clear operational image of how adjustment occurs. Finally, imperceptible risks, those that cannot be measured until manifested, remain understudied. These gaps justify a study that advances both conceptual clarity and practical utility. Missing is an integrative framework that captures how organizations in diverse domains actually modulate risk dynamically in real time. Another unresolved issue is the management of risks that remain imperceptible until they manifest. While predictive analytics and monitoring systems are advancing, many risks remain invisible to sensors or dashboards. How organizations respond to the imperceptible, and how they build a culture and strategy around constant recalibration, remains underexplored (Van Calster, 2016). Furthermore, a study by Wang (2023) suggests that modern neural networks, which possess high predictive capability, are insufficiently calibrated and generate unreliable estimations. This study addresses that blind spot by theorizing and empirically examining the metaphor of the risk rheostat.

This chapter introduces the context, theoretical foundations, and significance of studying the dynamic modulation of imperceptible risks through the risk rheostat analogy. It identified a gap in the literature, articulated the problem and its importance, and outlined the research aims, questions, and rationale. The next chapter will provide a detailed review of the relevant literature, situating the study within broader scholarly debates and highlighting the conceptual foundations that inform the rheostat framework.

### *Comparative Perspectives on Rheostat, Latent, and Watch-List Risks*

*Rheostat risks* represent -dynamic exposures whose intensity can be modulated rather than abruptly triggered, much like the gradual adjustment of a current regulator. They embody a continuum of threat expression, where the level of impact and urgency is not static but can increase or diminish depending on environmental, organizational, or systemic inputs. Unlike binary risks that are either present or absent, rheostat risks require constant

calibration and situational awareness, as their velocity and turbulence may shift unexpectedly and without evident boundary conditions.

In contrast to rheostat risks, *latent risks* exist beneath the operational surface, often remaining unseen until they become more apparent due to precipitating factors. Their defining feature is dormancy: they may be embedded in organizational processes, cultural blind spots, or technical infrastructures, persisting quietly until catalyzed by a disruptive event or compound vulnerability. They differ from rheostat risks in the sense that they are not necessarily adjustable or observable along a gradient. Instead, they represent concealed potentialities whose revelation is often abrupt, creating challenges for detection and early intervention.

*Watch-list risks* serve as a distinctive category, representing known areas of concern that have not yet crossed into active threat status but remain under deliberate scrutiny. They differ from latent risks in that they are recognized and cataloged, whereas latent risks are often unforeseen until they materialize. At the same time, they diverge from rheostat risks in that their intensification is not inherently gradual but contingent upon external signals or triggering conditions. The similarity across all three categories lies in their requirement for early monitoring and anticipatory governance: rheostat risks demand adaptive modulation, latent risks require uncovering hidden dynamics, and watch-list risks necessitate diligent surveillance to prevent escalation. The comparative examination of rheostat, latent, and watch-list risks underscores the spectrum of visibility, control, and predictability inherent in organizational threat landscapes. Latent risks conceal themselves in structural or cultural blind spots, surfacing only when catalyzed by unforeseen triggers, while watch-list risks are at least acknowledged and monitored in anticipation of possible escalation. Rheostat risks, however, represent a distinct paradigm: their significance lies not in sudden emergence or passive observation, but in their mutable intensity and capacity for gradual amplification. This malleable nature makes them central to effective risk governance, as they demand continuous calibration and nuanced response strategies, ensuring that early shifts in their trajectory are neither overlooked nor allowed to escalate unchecked (Van Calster et al., 2016).

## Theoretical Foundations: Why A Rheostat Analogy Matters

A *risk rheostat* is a conceptual tool or metaphor describing the ability of leaders, executives, or systems to adjust organizational exposure to risk dynamically, rather than treating risk as a binary "on/off" state. Instead of perceiving risk as a phenomenon to either accept or avoid, the "rheostat" suggests a continuum of calibration. The decision is made to dial in to increase tolerance (take on more risk to pursue opportunity, innovation, or growth) or decrease tolerance (tighten controls and safeguards in response to volatility, threats, or low appetite). The rheostat analogy draws intellectual power from multiple theoretical traditions. *Normal Accident theory* (Bianchi et al., 2023) emphasizes the inevitability of failures in tightly coupled systems, reminding us that imperceptibility is a structural, not accidental, phenomenon (Perrow, 1984). *High Reliability Organization theory* suggests that extraordinary vigilance and redundancy can maintain safety under high-risk conditions, provided they are continuously adapted (Weick & Sutcliffe, 2007*). ISO 31000: Risk Management Principles* is an iterative, principles-based, and context-dependent international standard for risk management.

*Resilience engineering* emphasizes anticipation and adaptation as systemic capacities rather than one-time solutions (Hollnagel et al., 2006; van der Kleij & Leukfeldt, 2020). A fundamental aspect of Resilience Engineering is the distinction between "work-as-done" and "work-as-imagined." This notion emphasizes the contrast between the design and planning of work (work-as-imagined) and its actual execution (work-as-done). In cybersecurity, firms frequently establish meticulously crafted security rules and procedures (work-as-imagined) yet may experience departures from these frameworks owing to human

factors, including employee conduct or unforeseen cyber threats (work-as-done). Comprehending this distinction enables companies to acknowledge that errors arise not only from individual shortcomings but may also be shaped by systemic limitations and environmental influences (Burrell, 2024; van der Kleij & Leukfeldt, 2020). *Sensemaking theory* relies on guidelines for how people explain things to one another; the purpose of the ML model is to enhance the artifact or explanation (Kaur et al., 2022; Weick, 1995). This theory further underscores that imperceptible risks require interpretation of weak signals before meaning crystallizes, demanding provisional decisions made under ambiguity.

Equally relevant are theories of decision-making and uncertainty. *Prospect theory* explains why leaders may adjust their risk posture (loosen or tighten) depending on whether they frame circumstances as losses or gains (Kahneman & Tversky, 1979). The *Cynefin framework* differentiates between ordered and chaotic contexts, suggesting that imperceptible risks often reside in the "complex" domain, requiring adaptive and experimental responses (Snowden & Boone, 2007). Finally, *Dynamic Capabilities theory* positions modulation itself as a source of strategic advantage, while concepts such as *antifragility, Black Swans, Dragon Kings,* and *risk society* remind us that invisible risks are not only unavoidable but may also serve as crucibles for growth. Against this rich theoretical backdrop, the *risk rheostat metaphor* contributes originality by offering a vivid, integrative image of how leaders, organizations, and societies can *operationalize* the dynamic calibration of imperceptible risks.

## Risk Rheostat as a Risk Conceptual Framework

The *rheostat*, an electromechanical variable resistor device that regulates electrical current by introducing variable resistance into a circuit (IEEE, 1996), serves as a central metaphor, illustrating the nuanced, continuous adjustment of flow rather than a binary on-off switch. This dynamic capability to finely tune resistance mirrors the managerial process of calibrating risk tolerance: decision-makers, like operators of a rheostat, can incrementally raise or lower their resistance to risk, directly influencing the magnitude of opportunities and threats traversing the organizational landscape. Through this analogy, the framework emphasizes intentional, graduated control over risk exposure, allowing for strategic responsiveness and adaptability in volatile environments.

### *Foundational Metaphor*

Organizations cannot eliminate risk, but they can mitigate its *intensity* by strengthening, increasing the frequency of, and refining the sophistication of controls, safeguards, and governance protocols in place to modulate risk exposure based on assessed conditions (Jarjoui & Murimi, 2021). The "risk rheostat" embodies the ability to calibrate exposure, neither treating risk as static nor binary, but as a continuum demanding constant adjustment. Within the risk rheostat conceptual framework, decision-makers actively adjust the organization's risk tolerance by metaphorically dialing up or down in response to shifting contextual factors and emerging intelligence. Increasing tolerance involves a deliberate loosening of restrictions, thereby enabling the pursuit of greater opportunity, innovation, or growth, such as authorizing exploratory investments, expanding into new markets, or accelerating the adoption of cutting-edge technologies (Lam, 2023). Conversely, in times of heightened volatility, acute threats, or diminished tolerance, the rheostat mechanism supports a dynamic and actionable contraction of tolerance. This translates to the rapid tightening of controls, fortification of safeguards, and implementation of stricter policies designed to shield the organization from exposure; for instance, temporarily elevating approval thresholds, restricting discretionary spending, or intensifying monitoring of critical assets. By continuously modulating risk tolerance in this manner, leaders foster an environment of resilience, one that responsively aligns operational posture with evolving

strategic imperatives and external uncertainties, ensuring that neither excessive restraint nor recklessness undermines long-term objectives.

### *Core Dimensions of the Framework*

*The Current (Opportunity Flow r*epresents the momentum of organizational ambition, growth, innovation, and expansion. Additionally, a stronger current may deliver rapid advancement, but it also heightens the risk of exposure.

*The Resistance (Governance and Controls)* symbolizes the structures, policies, risk controls, and oversight mechanisms that temper or redirect the current. Adjusting resistance does not block ambition but modulates its safe passage.

*The Dial (Decision-Maker Calibration)* serves as the locus of leadership judgment. Turning the dial reflects the willingness of executives or boards to adjust the balance between protection and pursuit, dynamically aligning, and risk tolerance with shifting contexts (Van Calster et al., 2016). The *risk appetite* refers to the baseline or pre-set willingness of an organization to assume risk, influenced by leadership ethos, culture, and regulatory context (Mandel & Parija, 2024). In this context, *risk tolerance* refers to the degree of risk an organization is willing and able to accept in pursuit of its objectives (International Organization for Standardization, 2018; Darroch & Finnie, 2021), which can be adjusted in response to strategic priorities and environmental changes.

### *Central Features of the Framework*

*Adjustable Exposure.* Similar to resistance in a rheostat, organizational risk levels can be fine-tuned in response to specific contexts.

*Situational Flexibility.* Different business units, projects, or geopolitical environments may require the dial to be set differently.

*Feedback-Driven.* The "current" risk can be monitored (via key performance indicators (KPIs), key risk indicators (KRIs), and early-warning indicators), and the dial adjusted accordingly based on stakeholder feedback, organizational controls, and other risk factors such as velocity, response time, and resource prioritization.

*Governance Alignment.* Tied to enterprise risk appetite statements, thresholds, and tolerances (Mandel & Parija, 2024).

### *Operational Modes of the Risk Rheostat*

*High Resistance Mode* prioritizes security, preservation, and strict compliance, typically used during times of heightened uncertainty, crisis, or when error tolerance must remain minimal. Emphasis is on conservation, security, and compliance. Used in environments of uncertainty, crisis, or when tolerance for error is minimal. This mode constitutes a deliberate operational stance characterized by maximizing organizational safeguards, enforcing strict compliance protocols, and rigorously preserving existing assets and capabilities. In this mode, leadership heightens the intensity of risk controls, elevates monitoring standards, and enacts comprehensive preventative measures to minimize vulnerabilities. Such a posture is most appropriate during periods of acute uncertainty, systemic threat, or strategic inflection points where even minor deviations can produce substantial negative impact. Rather than prioritizing growth or innovation, the focus shifts to maintaining stability, conserving resources, and ensuring unwavering adherence to regulatory and ethical standards. Decisions are rigorously scrutinized, discretionary actions are closely monitored, and incident response procedures are continually reviewed and reinforced. Through sustained vigilance and disciplined execution, High Resistance Mode fortifies resilience and preserves the organization's integrity against unpredictable disruptions.

*Low Resistance Mode* embodies a proactive strategic posture that deliberately relaxes restrictions to facilitate experimentation, accelerate innovation, and capitalize on emergent opportunities. Organizational leaders in this mode embrace uncertainty as a catalyst for advancement, allocating resources toward bold initiatives and rapid market entry when conditions are optimal. Safeguards are selectively diminished to encourage creative risk-taking, agile decision-making, and adaptive learning, all of which are essential when competitive advantage depends on speed and fluidity. This orientation promotes horizon scanning, disruptive thinking, and iterative prototyping, enabling the organization to pivot swiftly in response to favorable signals or shifting demand. By privileging dynamism and calculated risk exposure, Low Resistance Mode shapes an environment in which progress is enabled, and breakthrough performance is achievable without undue constraint.

*Adaptive Oscillation* emphasizes that risk postures are not static but evolve dynamically, continuously re-tuned in light of real-time feedback, shifting economic contexts, changing competitor actions, regulatory developments, and cultural dynamics. This oscillatory behavior reveals the framework's inherent agility: rather than locking into a single mode, organizations can modulate their risk settings with high fidelity, thus optimizing their response to uncertainty and complexity. Ultimately, adaptive oscillation enables persistent alignment of risk strategy with fluid external and internal conditions, preventing complacency and fostering sustainable resilience. The true strength of the metaphor: risk levels are not fixed but continuously re-tuned in response to feedback signals, economic conditions, competitor actions, regulatory shifts, or cultural factors (Ellström et al., 2022). However, a rheostat is blind without measurement. The framework emphasizes several factors:

*Feedback Loops and Sensors*

*Risk Indicators (KRIs)* as sensors.
*Scenario Analysis* as predictive feedback.
*Governance Reporting* is the stabilizer that prevents over-rotation.
Together, these ensure that adjustments are not arbitrary but evidence-driven.

*Strategic Implications*

*Leadership as the Operator:* Senior leaders must act not as passive risk recorders but as active regulators.
*Cultural Embedment*: Risk awareness must permeate the organization so that every layer can sense when the dial should shift.
*Resilience through Flexibility*: The capacity to "turn the dial" swiftly is itself a measure of resilience; rigidity is a sign of vulnerability.

*Applications Across Domains*

*Finance:* Adjusting exposure to volatile markets.
*Technology:* Balancing speed of deployment with cyber resilience.
*Operations:* Tuning supply chain efficiency against redundancy needs.
*Innovation:* Encouraging bold thinking while still maintaining safety nets.

*Integrative Value*

The Risk rheostat provides leaders and thinkers with:

*Proactive Risk Modulation:* A language of calibration rather than absolutes.
*Digestible Risk Comprehension:* A metaphor that conveys complexity in accessible imagery.
*Cultural Risk Instrumentation:* A strategic reminder that risk management is not suppression but orchestration.

## Case Studies

### Case Study 1: U.S. SEC—Mandating Cybersecurity Disclosure (2023 and onward)

*Situation:* Cybersecurity risk has become increasingly significant. Historically, many public companies have managed cybersecurity disclosure variably, with some providing minimal disclosure and others offering more robust disclosure, resulting in inconsistencies in risk transparency. This case study is a structural or ecosystem-level example of a rheostat, not a single enterprise dialing its posture, but a shift in the external environment that forces many institutions to adjust their risk calibration upward. It illustrates how regulatory actors can act as meta-operators of risk posture in a domain (Van Calster et al., 2016).

*Rheostat Dial in Motion:* In 2023, the U.S. Securities and Exchange Commission adopted new rules requiring the standardized, current disclosure of material cybersecurity incidents and the periodic reporting of processes, governance, and strategy related to cybersecurity (Securities and Exchange Commission, 2023). These rules effectively increase the resistance in companies: they must now maintain stronger internal controls, ensure timely incident reporting, and maintain clarity in risk governance.

*Why it Illustrates the Rheostat Metaphor:* This move by the SEC is a regulatory "dial twist" that forces all reporting companies to adopt a higher posture of accountability toward cyber risk. Companies that had been operating with lighter resistance (i.e., weaker disclosure and less formal risk governance) are now compelled to ramp up their guardrails (Securities and Exchange Commission, 2023).

### Case Study 2: Meta / Facebook—Governance and Rebranding (Post-2021 Scrutiny)

*Situation:* From 2021 onward, Meta (formerly Facebook) has come under increasing scrutiny over data privacy, misinformation, content moderation, regulatory risk, and governance oversight (Opgenhaffen, 2023). In late 2021, the company rebranded itself from "Facebook" to "Meta," framing itself as shifting toward metaverse ambitions while signaling a reorientation of identity amid crisis pressures (Meintjes & Botha, 2024).

*Rheostat Dial in Motion:* People may perceive the rebrand and public messaging as provoking resistance (Meintjes & Botha, 2024). Meta attempted to reset stakeholder expectations, reframe its trajectory, and preempt some regulatory backlash. Alongside rebranding, the company increased public disclosures, announced expanded commitments to oversight (e.g., content moderation reforms), and engaged in external reporting and communications strategies to manage reputational and regulatory risk (Jones, 2020; Meintjes & Botha, 2024). That said, critics have argued the shift was partly defensive and symbolic, with tension between maintaining growth ambitions (lower resistance) and bolstering controls (higher resistance) (Opgenhaffen, 2023).

*Why It Illustrates the Rheostat Metaphor:* Meta's stance is not absolute; it fluctuates over time. The company sought to balance between allowing innovation and platform growth (low resistance) and acknowledging the need for more governance, oversight, and public accountability (increased resistance). The rebrand itself is a signal of ambivalence in risk posture, reflecting both an outward change in identity and an inward rebalancing of risk tolerances (Meintjes & Botha, 2024). The modulation was responsive to external feedback (regulator pressure, reputational exposure, lawsuits) rather than following a static policy.

### Case Study 3: Peloton's Tread+ Recall (2021)

*Situation*: In April 2021, the U.S. Consumer Product Safety Commission (CPSC) issued an "urgent" warning about potential safety hazards with the Peloton Tread+ treadmill: reports had emerged of children or pets being drawn beneath the machine, including a tragic child fatality.

*Rheostat Dial in Motion:* Initially, Peloton responded defensively and slowly, indicating a low-resistance stance: they defended the product and delayed the recall action (Segal, 2021). Under mounting regulatory, media, and public pressure, the company shifted to higher resistance: it initiated a voluntary recall (May 5, 2021), offered refunds or repairs, enhanced safety controls, and later agreed to a $19 million civil penalty for delayed reporting and distribution of recalled units (U.S. Consumer Product Safety Commission, 2023). Having been cited for poor internal controls (Bajpai, 2022), Peloton also committed to implementing an enhanced compliance program, strengthening internal controls, and providing annual reporting for a period of five years (U.S. Consumer Product Safety Commission, 2023).

*How it Illustrates the Rheostat Metaphor:* The company shifted from a posture of risk tolerance (slow reaction) to risk aversion (aggressive recall and compliance) under stress. The decision was not binary; there was gradation: first warnings, then partial fixes, then full recall and remediation.

## Conclusions

Organizations that take imperceptible risks seriously recognize that management is less about absolute control than about calibration (Van Calster et al., 2016). Such leaders treat risk like current through a circuit: constantly flowing but varying in resistance depending on the conditions. To provide practical perspectives, several conclusions are drawn from this study. First, contemporary risk environments increasingly demand that organizations abandon rigid, binary models of risk classification in favor of frameworks that enable continuous calibration and adaptive response (Burrell, 2024; Jones, 2020). This conclusion is supported by the observation that imperceptible and low-velocity threats regularly bypass static monitoring systems, necessitating leadership to adopt dynamic, evidence-driven strategies that can anticipate shifting vulnerabilities and opportunities. Second, failure to recalibrate risk exposure is directly correlated with tangible organizational losses, including decreased productivity, increased turnover, and diminished stakeholder confidence. Data reveal that ineffective leadership can result in a 29% drop in productivity and a 23% increase in employee departure rates. Poor management decisions cost U.S. businesses up to $1.2 trillion annually, underscoring the costly consequences of inertia or miscalibration at the executive level. Next, empirical evidence demonstrates that nuanced risk modulation, exemplified by the rheostat framework, empowers leaders to balance defensive postures with innovation and growth, rather than defaulting to compliance or opportunism alone. Organizations that embrace feedback-driven and context-sensitive risk management consistently outperform peers who rely on one-size-fits-all controls, as their leaders are better positioned to synthesize weak signals, leverage scenario planning, and preempt silent erosions of resilience (Burrell, 2024). In addition, leadership development and effective communication remain crucial factors in determining the success or failure of risk management practices. Studies consistently show that up to 36–40% of new leaders fail within 18 months, primarily due to misalignment of expectations, poor adaptability, and insufficient engagement with evolving risk landscapes, rather than deficits in technical skill or industry knowledge (Heidrick & Struggles, 2021; PrimeGenesis, 2021). Strategic investment in continuous leadership training and change management can significantly mitigate these shortcomings. Lastly, the integrative value of adopting a risk rheostat approach extends beyond operational resilience; it also cultivates organizational cultures characterized by agility, trust, and sustained performance. As recent literature and global surveys confirm, enterprises that systematize adaptive recalibration and embed it within their leadership ethos are more likely to retain top talent, achieve strategic objectives, and maintain institutional viability in the face of volatility. This experience demonstrates that dynamic modulation is not only innovative but also essential for long-term success.

## Recommendations

For practical rheostat risk implementation, several recommendations are provided:

***Modulation Mechanism***

Practical modulation mechanisms involve concrete actions, such as revising approval workflows, adjusting risk escalation thresholds, or implementing regular scenario reviews, to respond to changing business realities. Risk monitoring can be achieved by establishing an early warning system that utilizes key risk indicators (Hartono et al., 2024; Herdianzah, 2020). For instance, risk committees might meet more frequently when market volatility increases, temporarily raise spending approval limits during periods of growth, or provide managers with real-time dashboards that flag when key indicators cross established boundaries. These operational levers empower organizations to make minor and timely tweaks, tightening or loosening restrictions as needed, which mirrors the rheostat's function of fine-tuning electrical current, ensuring that responses remain proportionate and adaptive to live conditions rather than delayed or static.

***Stakeholders and Governance for Dynamic Risk Modulation to Address Rheostatic Risk***

Effective governance for modulation should feature a structured risk oversight committee with clear mandates for real-time monitoring, escalation protocols, and periodic scenario testing. Leadership must set and communicate risk appetite, while risk owners and business unit leaders are empowered to make incremental operational adjustments within agreed-upon thresholds (Mandel & Parija, 2024). Strong governance requires the committee to meet regularly, review live risk indicator dashboards, and establish direct reporting lines to the board. Accountability frameworks, independent controls testing, and continuous engagement across all levels are essential to preserve transparency, agility, and resilience in risk adjustment efforts (Jones, 2020). A RACI (responsible, accountable, consulted, informed) matrix serves as an initial stage for organizations to implement risk management (Hartono et al., 2024; Pamungkas & Prasetyo, 2022). The RACI framework is utilized to delineate the roles and responsibilities of individuals within an organization, thereby enhancing operational efficiency by allocating tasks based on each member's competencies (Hartono et al., 2024; Pamungkas & Prasetyo, 2022). Table 1 presents the Dynamic Risk Modulation Stakeholder Roles Matrix, which assigns primary responsibility and accountability, ensuring clear ownership and facilitating cross-functional collaboration where strategic decisions, risk identification, and operational control are required. Consulted and informed roles ensure comprehensive input and transparent communication throughout the modulation process.

Table 1: Dynamic Risk Modulation Stakeholder Roles Matrix

| Dynamic Risk Modulation Stakeholder Roles Matrix | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Task/Responsibility | Board of Directors | Executive Leadership | Chief Risk Officer | Risk & Audit Committee | ERM/Risk Team | Compliance/ Legal | Operational Heads | IT/ Cybersecurity | External Stakeholder |
| Set risk appetite/tolerance | A | C | C | R | I | C | I | I | C |
| Establish strategic oversight/governance | A | R | C | R | I | I | I | I | C |
| Develop risk modulation framework | I | C | A | R | R | C | C | C | I |
| Publish risk-related policies | A | R | C | R | I | C | I | I | I |
| Escalate/respond to risks | I | A | R | R | R | C | R | R | I |
| Monitor risk indicators/dashboard | I | I | A | R | R | I | R | R | I |
| Perform scenario testing/controls review | I | C | A | R | R | R | R | R | C |
| Ensure regulatory compliance/reporting | I | I | C | C | C | A | I | I | R |
| Implement risk controls | I | C | C | I | R | R | A | R | I |
| Conduct staff training/reinforce culture | I | A | R | C | R | R | R | R | I |
| Develop risk modulation framework | I | C | A | R | R | C | C | C | I |

*Source: Developed by the author of this paper*

Managing such risks cannot be accomplished by static checklists or rigid compliance regimes (Jones, 2020; Klein Jr. & Reilley, 2024). Instead, organizations require conceptual models that allow for *dynamic modulation*: the continual adjustment of posture, tolerance, and safeguards in response to changing conditions and incomplete information. The metaphor of the rheostat offers a compelling way to understand and practice this form of risk management. Just as the rheostat dial may be turned to increase or decrease resistance without shutting the current off entirely, so too can organizations modulate their response to imperceptible risks, calibrating between ambition and caution in real time. In addition, Anderson (2022) provides nine risk process techniques to identify the unlikely, unusual, or undefined risk that can assist stakeholders in executing their responsibilities.

### *Practical Approaches: Turning the Dial in Real Time*

*Adaptive Risk Governance*
Establishing structures where risk appetite is revisited frequently, not just annually (Mandel & Parija, 2024). This involves dynamic committees, cross-functional crisis cells, and "living" risk registers that evolve in response to emerging signals.
*Scenario Experimentation*
Tabletop exercises or stress tests are regularly conducted to simulate "black box" events (Cao et al., 2024). These simulations expose imperceptible vulnerabilities and teach leaders to adjust the dial proactively.
*Signal Detection Network*
The development of distributed sensing mechanisms, frontline staff, customer feedback, supplier signals, and AI-driven monitoring serves as early-warning sensors to inform dial adjustments. Employing advanced technologies, such as artificial intelligence (Vanin et al., 2022), in conjunction with human behavior analysis, enables organizations to develop actionable strategies for combating digital attackers (Burton, 2025).

### *Proactive Actions: Beyond Compliance*

To be proactive, organizations should shift from a reactive shield to an anticipatory radar (Burrell, 2024). This involves:
*Embedding Weak-Signal Analysis*
Teams are trained to identify anomalies and "noise" that may indicate imperceptible risks. For instance, a slight uptick in error rates or unusual data traffic may be treated not as noise but as precursors to larger systemic problems (Hofbauer & Mayer, 2024; McCrie & Lee, 2021).
*Dynamic Buffering*
Maintaining flexible reserves, financial, operational, and human, that can be scaled up or down (Sivec & Volk, 2023). Instead of permanent redundancies (which are costly), buffers are modular and deployable.
*Decision Modulation Protocols*
Developing explicit "dial-turning" criteria: under what conditions leadership should tighten resistance (e.g., pause innovation projects, double compliance checks) or loosen it (e.g., fast-track pilots, reduce controls for agility) (Hillson, 2024).

### *Novel and Emerging Practices*

Beyond standard risk-management actions, leading-edge organizations are experimenting with novel practices that exemplify the rheostat in action:
*Digital Twins for Risk*
Advanced organizations are creating digital replicas of supply chains, hospital networks, or IT systems, which allow them to run "what if" scenarios (Pires et al., 2021)

on imperceptible risks and dial responses virtually before implementing them physically.

*Behavioral Analytics*

Utilize AI to monitor subtle shifts in human or system behavior (Cox et al., 2024; Samayamantri et al., 2024) as imperceptible risk signals, such as fatigue in clinicians, coding anomalies, or subtle supplier irregularities. Utilizing advanced technologies, such as artificial intelligence, to analyze human behavior enables cyber leaders to develop actionable strategies against digital attacks (Burton, 2025).

*Dynamic Regulation Interfaces*

Some firms in finance and healthcare are engaging regulators in real-time reporting environments, effectively creating a "shared rheostat" where compliance and innovation are calibrated collaboratively rather than competitively.

*Risk Culture Nudges*

Instead of static training, organizations are embedding behavioral nudges, small reminders, prompts, or dashboard indicators, that subtly encourage staff to adjust their risk posture in their day-to-day work (Galpin, 2022).

## Recommendations for Future Research

Future research should focus on advancing the concept of the risk rheostat from a theoretical metaphor to a practical and empirically validated framework for organizational decision-making. The problem that necessitates this work is the absence of effective tools for dynamically managing risks that are imperceptible, unquantifiable, or emergent. Conventional risk management practices tend to treat risks as either fully present or fully absent, thereby constraining innovation when controls are overly rigid or leaving organizations exposed when risks remain unacknowledged (Burrell, 2024; Jones, 2020; Settembre-Blundo et al., 2021). By conceptualizing risk tolerance as a continuum that can be dynamically adjusted, the risk rheostat addresses this limitation, yet its practical implementation remains underdeveloped. Three complementary research methods, Implementation Science, Action Research, and the Delphi Method, offer pathways for operationalizing and testing the rheostat framework. Each provides distinct advantages and can be engaged through systematic steps.

### *Implementation Science*

Implementation science offers the advantage of rigorously studying how new frameworks or tools become integrated into real-world organizational practice (Ramanadhan et al., 2021). The benefit of using this method for the risk methodology lies in its ability to evaluate the conditions, processes, and supports necessary to make calibration sustainable in everyday decision-making. Implementation science not only reveals the propensity for success or failure (Shi et al., 2023) but also whether the rheostat can be adopted in managing risk. This approach is particularly valuable in high-risk sectors, such as healthcare or aviation, where dynamic recalibration of risk is critical and must be embedded in the organizational culture rather than treated as a one-time intervention (Burton, 2025).

The steps to engage implementation science for the risk rheostat are as follows:

1. Identify the organizational setting and stakeholders where imperceptible risks pose challenges.
2. Define the intended use of the risk rheostat, specifying how it will inform decisions.
3. Conduct a baseline assessment of current risk management practices and limitations.
4. Introduce the rheostat framework to organizational processes through structured training and tools.

5. Measure outcomes over time, including changes in decision quality, adaptability, and resilience.
6. Evaluate barriers and facilitators to adoption, refining the framework accordingly.
7. Scale findings by comparing across different organizational contexts.

### *Action Research*

Action research is especially advantageous for developing the risk rheostat as a practical tool because it integrates inquiry with action, enabling iterative refinement through cycles of testing and reflection (Zuber-Skerritt, 2021). Its primary benefit lies in its collaborative nature, as it involves researchers and practitioners working together to experiment with the metaphor in real organizational contexts (Coughlan & Coughlan, 2023). This generates scholarly knowledge and produces immediate, practical improvements for the organizations involved (Coughlan & Coughlan, 2023). Action research thus allows the rheostat to evolve in tandem with the real-world challenges it seeks to address.

The steps to engage action research for the risk rheostat are as follows:

1. Form a partnership between researchers and organizational leaders.
2. Diagnose current challenges in managing imperceptible risks.
3. Co-design interventions that apply the rheostat metaphor to decision-making processes.
4. Implement the interventions in practice while monitoring outcomes.
5. Reflect jointly on the results, identifying successes, challenges, and unexpected effects.
6. Revise the intervention and repeat the cycle with refinements.
7. Document both the academic insights and practical outcomes to build cumulative knowledge.

### *Delphi Method*

The Delphi Method provides the distinct advantage of systematically gathering expert consensus on complex or ambiguous issues where empirical data may be limited (Cuhls, 2023). Its benefit for advancing the risk rheostat lies in leveraging diverse expertise to define principles, practices, and thresholds for calibration. Because imperceptible risks are inherently difficult to measure, expert judgment is essential for identifying weak signals, framing decision contexts, and clarifying when organizations should "dial up" or "dial down" their risk exposure. The Delphi Method generates not only a structured knowledge base but also legitimacy, since consensus reflects a collective judgment rather than an isolated opinion (Cuhls, 2023).

The steps to engage the Delphi Method for the risk rheostat are as follows:

1. Identify and recruit a diverse panel of experts in risk management, strategy, resilience, and decision-making.
2. Develop a set of initial questions exploring how the rheostat metaphor could be operationalized.
3. Conduct the first round of surveys, gathering individual responses anonymously.
4. Summarize and communicate results to the panel, highlighting areas of convergence and divergence.
5. Conduct successive rounds of questioning, asking participants to refine or reconsider their views.
6. Continue until consensus emerges or sufficient stability in responses is achieved.
7. Publish the findings as a framework of agreed-upon principles and practices for risk calibration.

## References


Anderson, D. (2021). Nine Techniques to Identify the Unlikely, Unusual, or Undefined Risk. AuditBoard. https://auditboard.com/blog/techniques-identify-unlikely-unusual-unidentified-risk

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Bajpai, K. (2022). *The Rise and Fall of Peloton: Financial Perspective* (Master's thesis, Universidade NOVA de Lisboa (Portugal)).

Baran, G. (2024, May 13). Boeing confirms LockBit hackers demanded $200 million ransom after 2023 data breach. *Cyber Security News: Ransomware*. https://cybersecuritynews.com/boeing-confirms-lockbit-demanded/

Barberis, N., Jin, L. J., & Wang, B. (2021). Prospect theory and stock market anomalies. *The Journal of Finance*, *76*(5), 2639-2687.

Beck, U. (1992). *Risk society: Towards a new modernity*. Sage.

Bianchi, F., Curry, A. C., & Hovy, D. (2023). Artificial intelligence accidents waiting to happen?. *Journal of Artificial Intelligence Research*, *76*, 193-199.

Bier, V. M. (2017). Challenges of risk management in a dynamic society. *Risk Analysis, 37*(11), 2100–2109. https://doi.org/10.1111/risa.12848

Burrell, D. N. (2024). Understanding healthcare cybersecurity risk management complexity. *Land Forces Academy Review*, *29*(1), 38-49.

Burton, S. L. (2025). Digital Saboteurs: Unmasking Insider Cybersecurity Threats in Aviation and Aerospace. *Law, Economics and Society*, *1*(2), p1-p1.

Cao, H., Hu, J. Q., & Lian, T. (2024). Blackbox simulation optimization. *Journal of the Operations Research Society of China*, 1-27.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2024). Enterprise Risk Management Framework Update.

Coughlan, P., & Coghlan, D. (2023). Action research. In *Research Methods for Operations and Supply Chain Management* (pp. 219-251). Routledge.

Cox, D. J., & Jennings, A. M. (2024). The promises and possibilities of artificial intelligence in the delivery of behavior analytic services. *Behavior Analysis in Practice*, *17*(1), 123-136.

Cuhls, K. (2023). The Delphi method: an introduction. In *Delphi methods in the social and health sciences: concepts, applications and case studies* (pp. 3-27). Wiesbaden: Springer Fachmedien Wiesbaden.

Darroch, J., & Finnie, D. "Risk Appetite and Tolerance in Competitive Strategy." *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives* (2021): 347.

Ellström, D., Holtström, J., Berg, E., & Josefsson, C. (2022). Dynamic capabilities for digital transformation. *Journal of Strategy and Management*, *15*(2), 272-286.

Frigo, M. L., & Anderson, R. J. (2023). The Risk Intelligent Enterprise: Risk Governance and Performance Management. *Journal of Business Ethics, 178*(1), 45-62.

Galpin, T. (2022). Nudging innovation across the firm–aligning culture with strategy. *Journal of Business Strategy*, *43*(1), 44-55.

Hartono, Y., Cahyo, W. N., & Immawan, T. (2024). The Assignment of Risk Mitigation Tasks Based on The RACI Matrix and Key Risk Indicator. *Jurnal Ilmiah Teknik Industri*, 235-244.

Heidrick & Struggles. (2021). Route to the Top 2021. https://www.heidrick.com/en/insights/chief-executive-officer/route-to-the-top-2021

Hillson, D. (2024). *Managing risk in projects*. Routledge.

Hofbauer, J., & Mayer, K. (2024). Blue Team Fundamentals: Roles and Tools in a Security Operations Center. In *SECURWARE 2024: The Eighteenth International Conference on Emerging Security Information, Systems and Technologies* (pp. 176-184). IARIA.

Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Ashgate.

Hubbard, D. (2024). *How to Measure Anything in Cybersecurity Risk*. Wiley Finance.

International Organization for Standardization (ISO). (2018). ISO 31000:2018, Risk management — Guidelines. International Organization for Standardization (ISO).

Jarjoui, S., & Murimi, R. (2021). A framework for enterprise cybersecurity risk management. In *Advances in cybersecurity management* (pp. 139-161). Cham: Springer International Publishing.

Jones, L. A. (2020). *Reputation risk and potential profitability: Best practices to predict and mitigate risk through amalgamated factors*. Capitol Technology University.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263–291. https://doi.org/10.2307/1914185

Kahneman, D., & Tversky, A. (2013). Prospect theory: An analysis of decision under risk. In *Handbook of the fundamentals of financial decision making: Part I* (pp. 99-127).

Kaplan, R. S., & Mikes, A. (2023). Managing Risks: A New Framework. *Harvard Business Review, 101*(4), 86-95.

Kaur, H., Adar, E., Gilbert, E., & Lampe, C. (2022, June). Sensible AI: Re-imagining interpretability and explainability using sensemaking theory. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 702-714).

Kennedy-Sims, C. (2021). *Supply chain management in level I trauma care facilities: Can it determine patient care delivery and funding*? (Order No. 28539929). Available from ProQuest Dissertations & Theses Global.

Kitagawa, T. L. (2022). The Origin of the Bernoulli Numbers: Mathematics in Basel and Edo in the Early Eighteenth Century. *The Mathematical Intelligencer*, *44*(1), 46-56.

Klein Jr, V. H., & Reilley, J. T. (2024). The temporal dynamics of enterprise risk management. *Critical Perspectives on Accounting*, *99*, 102363.

Lam, J. (2023). Enterprise Risk Management: From Incentives to Controls. Wiley.

Lambert, K. (2025, September 18). Hackers demand $6 million for files stolen from Seattle airport operator in cyberattack. AP: *The Seattle Times*. https://apnews.com/article/seattle-airport-cyberattack-ransomware-rhysida-95cd980a9f45112f0fdce488233eec9c

Leonard, A. (2022). *London Marine Insurance 1438-1824: Risk, Trade, and the Early Modern State*. Boydell & Brewe

Leung, A. (2021). *Actuarial Principles: Lifetables and Mortality Models*. Academic Press.

Lyndgaard, S. F., & Kanfer, R. (2024). Interpersonal, intrapersonal, and cognitive tactics: A thematic study of adults' 21st century learning management. *Journal of the Learning Sciences, 33*(1), 175-211. https://doi.org/10.1080/10508406.2024.2303777

Mathieu, P., & Miermont, G. (2023). Blaise Pascal et Pierre de Fermat, géomètres du hasard. *Courrier Blaise Pascal*, (45), 53-89.

McCrie, R., & Lee, S. (2021). *Security operations management*. Butterworth-Heinemann.

Meintjes, C., & Botha, Y. (2024). Rebranding as a crisis response strategy: a stakeholder perspective. *Corporate Reputation Review*, 1-17.

Opgenhaffen, M. (2023). Combatting disinformation with crisis communication: An analysis of Meta's newsroom stories. *Communications*, *48*(3), 352-369.

Pamungkas, C. H., & Prasetyo, A. H. (2022). Rancangan Manajemen Risiko pada Perusahaan Startup PT. Haruka Evolusi Digital Utama. *Journal of Emerging Business Management and Entrepreneurship Studies, 2*(1), 50–66. https://doi.org/10.34149/jebmes.v2i1.65

Paul, J., & Barari, M. (2022). Meta-analysis and traditional systematic literature reviews—What, why, when, where, and how?. *Psychology & Marketing*, *39*(6), 1099-1115.

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Basic Books.

Petkauskas, V. (2023, November 15). Boeing breach: LockBit leaks 50 GB of data. *Cybernews*. https://cybernews.com/news/boeing-data-leak-lockbit-ransomware/

Pires, F., Ahmad, B., Moreira, A. P., & Leitão, P. (2021, May). Digital twin based what-if simulation for energy management. In *2021 4th IEEE international conference on industrial cyber-physical systems (ICPS)* (pp. 309-314). IEEE

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press.

Power, M. (2022). Risk Culture and Risk Management: New Challenges for Theory and Practice. *Journal of Risk Research, 25*(3), 219-234.

PrimeGenesis. (2021). Heidrick and Struggles study of 20,000 searches highlights need for onboarding improvements. https://www.primegenesis.com

Ramanadhan, S., Revette, A. C., Lee, R. M., & Aveling, E. L. (2021). Pragmatic approaches to analyzing qualitative data for implementation science: an introduction. *Implementation Science Communications*, *2*(1), 70.

Samayamantri, L. S., Singhal, S., Krishnamurthy, O., & Regin, R. (2024). AI-driven multimodal approaches to human behavior analysis. In *Advancing Intelligent Networks Through Distributed Optimization* (pp. 485-506). IGI Global.

Securities and Exchange Commission. (2023). Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. SECURITIES AND EXCHANGE COMMISSION 17 CFR Parts 229, 232, 239, 240, and 249 [Release Nos. 33-11216; 34-97989; File No. S7-09-22] RIN 3235-AM89. https://www.sec.gov/files/rules/final/2023/33-11216.pdf

Segal, E. (2021). The 6 Crisis Management Lessons From Peloton's Delayed Recall Of Treadmills. *Forbes.* https://www.forbes.com/sites/edwardsegal/2021/05/05/the-6-crisis-management-lessons-from-pelotons-delayed-recall-of-treadmills

Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S., & García-Muiña, F. E. (2021). Flexibility and resilience in corporate decision making: a new sustainability-based risk management system in uncertain times. *Global Journal of Flexible Systems Management*, *22*(Suppl 2), 107-132.

Shi, J., Chen, X., Hu, H., & Ung, C. O. L. (2023). Application of implementation science framework to develop and adopt regulatory science in different national regulatory authorities. *Frontiers in Public Health*, *11*, 1172557.

Sivec, V., & Volk, M. (2023). Empirical evidence on the effectiveness of capital buffer release. *International Journal of Central Banking*, *19*(3), 139-173.

Snowden, D. J., & Boone, M. E. (2007). A leader's framework for decision making. *Harvard Business Review, 85*(11), 68–76.

Snyder, H. (2024). Designing the literature review for a strong contribution. *Journal of Decision Systems*, *33*(4), 551-558.

Taleb, N. N. (2010). *The Black Swan: The impact of the highly improbable* (2nd ed.). Random House.

The Institute of Electrical and Electronics Engineers (IEEE). (1996). IEEE Std 100, *The Authoritative Dictionary of IEEE Standards Terms*.

U.S. Consumer Product Safety Commission. (2023). Peloton Agrees to Pay $19 Million Civil Penalty for Failure to Immediately Report Tread+ Treadmill Entrapment Hazards and for Distributing Recalled Treadmills. https://www.cpsc.gov/Newsroom/News-Releases/2023/Peloton-Agrees-to-Pay-19-Million-Civil-Penalty-for-Failure-to-Immediately-Report-Tread-Treadmill-Entrapment-Hazards-and-for-Distributing-Recalled-Treadmills

University of Louisville. (2025, Jan 15). Critical thinking and academic research: Assumptions. *Author*. https://library.louisville.edu/ekstrom/criticalthinking/assumptions

Van Calster, B., Nieboer, D., Vergouwe, Y., De Cock, B., Pencina, M. J., & Steyerberg, E. W. (2016). A calibration hierarchy for risk models was defined: from utopia to empirical data. *Journal of clinical epidemiology, 74*, 167-176.

van der Kleij, R., & Leukfeldt, R. (2020). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity, July 24-28, 2019, Washington DC, USA 10*, 16-27. DOI:10.1007/978-3-030-20488-4_2.

Vanin, P., Newe, T., Dhirani, L. L., O'Connell, E., O'Shea, D., Lee, B., & Rao, M. (2022). A study of network intrusion detection systems using artificial intelligence/machine learning. *Applied Sciences*, *12*(22), 11752.

Wang, C. (2023). Calibration in deep learning: A survey of the state-of-the-art. *arXiv preprint arXiv:2308.01222*.

Weick, K. E. (1995). *Sensemaking in organizations*. Sage.

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty* (2nd ed.). Jossey-Bass.

Zuber-Skerritt, O. (Ed.). (2021). *Action research for change and development*. Routledge.