Global Business Challenge (BMMB7006)

Advisory Report: The Impact of Artificial Intelligence on Risk Management at Samsung

Tekle Atobrhan (2210427)

27 April 2026

Executive Summary

Samsung's extensive use of AI across devices, services, and manufacturing creates significant strategic opportunity but also complex, interdependent risks. Operating in a volatile macroeconomic and geopolitical environment, Samsung must manage operational failures, strategic lock-in, reputational exposure, and tightening legal and regulatory obligations, especially under the EU AI Act and diverging UK/EU data regimes. The report argues that data and ethical capabilities can be strategic assets or major liabilities, depending on the quality of governance. Using ERM, RBV, and stakeholder theory, it recommends that Samsung implement a global AI governance framework, advanced data governance, embedded ethical AI practices, and proactive regulatory engagement, supported by a phased 36-month implementation roadmap to protect customer trust and sustain long-term competitive advantage.

Table of Contents

Executive Summary *1*

1. Introduction *0*

2. Main Body *1*

2.1. International Economic and Political Environment **1**

2.1.1. **Macroeconomic Pressures and AI Investment** 1

2.1.2. **Geopolitical Fragmentation and AI** 2

2.2. AI Risk Typology **3**

2.2.1. **Operational Risk** 3

2.2.2. **Strategic and Reputational Risk** 4

2.2.3. **Legal and Regulatory Risk** 5

2.3. Data Governance **5**

2.3.1. **Data as a Strategic Asset** 6

2.3.2. **Key Data Governance Challenges** 6

2.3.3. **UK vs EU Data Governance** 7

2.3.4. **Strategic Implications** 8

2.4. Ethical AI Use **8**

2.4.1. **The Ethics–Profit Tension** 8

2.4.2. **Algorithmic Bias and Fairness** 9

2.4.3. **Explainability and Accountability** 10

2.4.4. **Critical Insight** 10

2.5. Regulatory Compliance **11**

2.5.1. **The UK's Pro-Innovation Model** 11

2.5.2. **The EU's Risk-Based Model** 11

2.5.3. **Regulatory Fragmentation** 12

2.6. Maintaining Customer Trust **13**

2.6.1. **Trust as Competitive Advantage** 13

2.6.2. **Trust Risks in AI** 13

2.6.3. **Trust-Building Strategies** 14

2.7. Strategic Recommendations **15**

3. Conclusion *16*

4. References *1*

5. Appendix *14*

5.1. Implementation Plan **14**

1. Introduction

Artificial intelligence (AI) is reshaping how multinational enterprises operate, compete, and manage risk. Modern AI differs from earlier waves of digitalisation and automation because it can learn and adapt using large datasets, often runs with limited human intervention, and now influences decisions from high-level strategy to day-to-day operations. These features shift firms away from linear, predictable risks towards adaptive, emergent, and systemic risks that can spread quickly across functions and geographies (Finextra, 2025; Gibson, 2026).

At Samsung Electronics, AI is now deeply embedded across business units and value chains. In Consumer Electronics, it powers smartphones, Bixby, recommendation engines, and smart TVs. In Smart Home and IoT, it supports connected appliances and platforms that process real-time user data. In Semiconductor Manufacturing, it enables process optimisation, predictive maintenance, yield management, and quality control. Samsung also relies on AI for data analytics and cloud services to analyse consumer behaviour and market trends and integrate these insights into its wider digital platforms. This broad and connected use of AI amplifies AI-related risks across diverse legal, regulatory, and political regimes (Samsung Newsroom U.K., 2026a; Chopvitayakun et al., 2026; Samsung Newsroom, 2024).

Analytically, this report draws on three main frameworks. Enterprise Risk Management (ERM) explains how AI challenges traditional assumptions about risk and control. The Resource-Based View (RBV) treats data and AI as strategic assets that can also become liabilities if governance is weak. Stakeholder theory highlights ethical tensions and trust issues, and the need for Samsung to balance the interests of customers, regulators, employees, shareholders, and wider society. Together, these perspectives provide a theoretically grounded but practical basis for AI-specific risk governance.

This reflects an evolution in risk thinking: from traditional, siloed risk management, to integrated ERM, and now towards an AI-aware risk ecosystem in which AI itself is a central part of the risk environment. This new phase requires more dynamic governance, continuous monitoring, and stronger ethical oversight. As a result, Samsung must develop AI-specific risk capabilities that bring together technological, legal, ethical, and strategic dimensions into a coherent and adaptive governance approach.

2. Main Body

2.1. International Economic and Political Environment

Building on these conceptual foundations, this section examines the international economic and political context in which Samsung uses AI. It shows how macroeconomic pressures and geopolitical fragmentation shape Samsung's risk exposure and strategic choices.

2.1.1. Macroeconomic Pressures and AI Investment

The current macroeconomic environment is characterised by tight financial conditions and rapid technological change, both of which strongly influence AI investment and use. High interest rates raise the cost of large AI projects and may slow some expansion. At the same time, inflationary pressures on energy, logistics, and labour encourage firms to adopt AI to cut costs and improve efficiency. Slower global growth can weaken demand, pushing companies to focus more on productivity, optimisation, and targeted marketing—areas where AI offers a clear competitive edge (European Banking Authority, 2024; IMF, 2026a; IMF, 2026b).

From a Keynesian perspective, governments have responded to uncertainty and strategic competition by intervening more actively through industrial and innovation policy. Many states now subsidise AI research and development through grants, tax incentives, and public–private partnerships; invest in digital and computing infrastructure, including 5G networks, data centres, and cloud platforms; and promote technological sovereignty to reduce dependence on foreign suppliers for semiconductors and AI platforms (Ghisellini et al., 2021; Tao et al., 2025).

For Samsung, these trends intensify competition from state-backed firms, increase pressure to localise chip production and data handling, and require closer alignment between AI strategy and national industrial priorities to access public support. In a COSO-style ERM view, they are key drivers of strategic, operational, and compliance risk across the business. This forces Samsung to balance cost control and innovation against the additional risks that come with large-scale AI deployment (Dees, 2025; Criddle, 2021; Soner and Karadag, 2026).

While macroeconomic conditions and industrial policies shape the overall level and direction of AI investment, Samsung's risk environment is also heavily influenced by geopolitical rivalry and regulatory divergence (Ozan, 2025).

2.1.2. Geopolitical Fragmentation and AI

Beyond macroeconomic constraints, the global AI landscape is increasingly shaped by geopolitical rivalry and techno-nationalism among three major actors. The United States seeks to maintain technological leadership and protect national security. China aims for technological self-reliance and greater global influence in AI and semiconductors. The European Union positions itself as a leader in rights-based, human-centric AI regulation (World Economic Forum, 2025).

This rivalry has produced a range of policy instruments and constraints that directly affect Samsung. These include export controls on advanced semiconductor technologies, restrictions on cross-border data flows framed under data protection, cybersecurity, or national security legislation, and divergent regulatory standards governing AI safety, privacy, transparency, and accountability (Samsung SDS, 2026; Han, 2024).

For Samsung, this environment generates multi-layered risk exposure in at least three areas:

• **Supply chain risk:** Export controls can limit access to advanced fabrication equipment, design tools, or critical materials, while sanctions or logistical disruptions can destabilise global supply networks. AI systems used to optimise supply chains may also become less reliable if data from restricted regions is removed or limited (Berkovitch, 2026).

• **Market access risk:** Some countries may restrict foreign AI technologies, favour domestic providers, or block specific applications. Tensions between major powers can lead to sudden policy shifts that affect Samsung's presence and operations in key markets (Korea Pro, 2025).

• **Regulatory risk:** Conflicting regulations across the EU, US, China, and the UK create complex compliance obligations. AI systems may need to be modified, restricted, or redesigned to meet local standards, raising development and maintenance costs (Esposito and Sergi, 2026).

These dynamics reflect a reconfiguration of globalisation, where decades of deep integration are slowing or reversing. Regional blocs and alliances are gaining importance, pushing firms like Samsung to adopt modular, region-specific, and politically aware AI and risk strategies. ERM therefore requires tailoring risk appetite and responses by region rather than assuming a single global profile. Stakeholder theory also stresses that Samsung must reconcile divergent expectations such as the EU's focus on fundamental rights, US national security concerns, and many Asian governments' emphasis on industrial competitiveness within a single corporate strategy (Colantone, 2025; Samsung, 2025; Kumar, 2025).

Together, macroeconomic pressures and geopolitical fragmentation define the external context in which Samsung must govern AI and structure its AI-related risk management.

2.2. AI Risk Typology

This section assesses Samsung's AI risk landscape across operational, strategic, reputational, and legal and regulatory areas. COSO ERM helps evaluate impacts on operations, long-term positioning, and compliance. RBV shows that AI-based advantages can also create vulnerabilities if they are poorly governed. Stakeholder theory highlights how different groups experience and judge these risks differently. Overall, AI risks are organisational, strategic, and social, not just technical.

2.2.1. Operational Risk

The first category, operational risk, focuses on how AI can disrupt or undermine day-to-day processes and production systems, particularly in semiconductor fabrication and manufacturing (teammate, 2026).

Operational risk traditionally arises from failures in processes, systems, people, or external events. When AI is integrated into Samsung's operations, especially in semiconductor fabrication, a set of specific concerns becomes visible. One is incorrect optimisation due to flawed or biased training data: AI systems may prioritise suboptimal configurations, for instance, by over-emphasising throughput at the expense of quality. Another is edge-case failures, in which AI performs well in common scenarios but fails when confronted with conditions not represented in the training data, such as rare machine faults or unusual environmental anomalies (teammate, 2026; Coleman, 2011; Chanda and Banerjee, 2022).

For example, an AI-driven system responsible for interpreting sensor data in a semiconductor plant might misclassify subtle anomalies as normal variation, allowing defective wafers to pass quality checks. The downstream consequences could include product failures, recalls, and substantial financial and reputational losses (Chanda and Banerjee, 2022).

Within the COSO ERM framework, these operational risks must be systematically identified, assessed, and controlled across the value chain, with clear risk ownership and tolerance levels. Yet because AI models are often opaque, emergent, and dynamic, Samsung cannot rely on traditional control checklists alone. It needs continuous monitoring, stress testing, and incident-reporting processes tailored to AI systems. Stakeholder theory further highlights that operational AI failures erode trust among customers, supply chain partners, and regulators, and

that this loss of trust must factor into Samsung's risk–return trade–offs (Soner and Karadag, 2026; Kumar, 2025; John et al., 2025).

Overall, these operational vulnerabilities show how AI can cause immediate, tangible losses if not properly controlled. At the same time, AI is reshaping Samsung's longer-term positioning and public image, which gives rise to a distinct but related set of strategic and reputational risks (Digital Watch, 2026).

2.2.2. Strategic and Reputational Risk

Beyond the factory floor, AI directly influences Samsung's long-term strategic direction and brand perception. This subsection examines how technological lock-in, rapid obsolescence, and ethical controversies surrounding AI contribute to strategic and reputational risks (Han, 2024).

Strategic risk involves threats to an organisation's long-term direction and competitive position, with AI now a key driver. Rapid technological change means AI tools and infrastructures can quickly become obsolete, turning major investments into short-lived assets. There is also lock-in risk: committing to specific cloud providers, frameworks, or chipsets can create long-term dependencies and limit Samsung's ability to pivot or negotiate. Path dependency theory shows how early AI choices can lock Samsung into suboptimal trajectories, reducing its capacity to adjust to new regulations, technologies, or market expectations (Allan and Beer, 2017; Samsung Newsroom, 2025; Baggiony-Taylor, 2026).

Reputational risk is particularly acute in AI, especially for consumer-facing products. Issues such as bias and discrimination in facial recognition, voice assistants, or recommendation systems can trigger intense public criticism and regulatory scrutiny. Concerns about surveillance and opaque data use in smart devices further undermine trust. In a highly connected media environment, such crises can rapidly escalate and spread, amplifying their impact (Holweg et al., 2022; ICO, 2025; Treharne, 2026).

From a stakeholder theory perspective, different groups of consumers, civil society, regulators, and investors will interpret the same AI incident in divergent ways, and Samsung must manage these expectations rather than focus only on short-term sales. For a brand built on trust, innovation, and quality, AI-related reputational failures can significantly affect market share and brand equity. From an ERM perspective, these strategic and reputational risks should be explicitly reflected in Samsung's risk appetite and culture so that AI innovation is assessed not

just on financial returns but also on its impact on key stakeholder relationships (Gutterman, 2023; Samsung U.S. Newsroom, 2026).

In practice, strategic missteps and reputational damage in AI-enabled products are closely intertwined with the regulatory environment, where non-compliance can trigger severe financial, operational, and market consequences (Wei et al., 2025).

2.2.3. Legal and Regulatory Risk

Complementing the operational and strategic dimensions, legal and regulatory risk captures the potential impact of non-compliance with evolving AI and data protection laws, such as the EU AI Act and the General Data Protection Regulation (GDPR) (European Parliament, 2020).

Legal and regulatory risk arises when organisations fail to comply with these emerging AI and data laws. For Samsung, non-compliance with the EU AI Act and related legislation could result in substantial financial penalties of up to 6% of annual global turnover for serious violations, as well as product restrictions or outright bans in the EU market. Such measures could prevent Samsung from selling certain AI-enabled products or services within the EU. Given Samsung's global footprint, these sanctions would not only have immediate financial implications but also weaken its strategic positioning and undermine trust with regulators in other jurisdictions (European Parliament, 2020; Gerken and McMahon, 2022).

In COSO ERM terms, regulatory shifts are both compliance and strategic risks, requiring proactive identification, assessment, and response. Stakeholder theory positions regulators as key stakeholders whose expectations shape Samsung's licence to operate. Accordingly, constructive regulatory engagement and alignment of internal governance with external norms are central to Samsung's AI risk management, with many risks ultimately rooted in how data is collected, managed, and protected, linking AI risk closely to data governance (Deloitte, 2017; Bräuer-Provasnek, 2017).

2.3. Data Governance

Having outlined Samsung's AI risk typology, this section examines data governance as a foundational factor that both enables and constrains AI deployment. It applies the Resource-Based View (RBV), COSO ERM, and stakeholder theory to assess whether Samsung's data resources function as strategic assets or significant liabilities.

2.3.1. Data as a Strategic Asset

Under the Resource-Based View (RBV), firms achieve competitive advantage by developing and leveraging resources that are valuable, rare, inimitable, and non-substitutable (VRIN). High-quality data, managed through strong governance capabilities, can meet these criteria. For Samsung, rich datasets on consumer behaviour, product usage, and manufacturing performance can power more accurate and effective AI models. In addition, proprietary data generated by its own devices and platforms can offer insights that competitors cannot easily replicate. In RBV terms, Samsung's ability to collect, curate, and exploit such data at scale has the potential to be a core source of sustained competitive advantage (Holz, 2024; Samsung Newsroom, 2024b).

This potential depends on strong data governance. Without clear ownership, robust controls, and sufficient protections, Samsung's data assets can become liabilities, leading to breaches, sanctions, and reputational harm. COSO ERM highlights that data risks are enterprise-wide, while stakeholder theory stresses rising expectations for responsible data use. Thus, the value of Samsung's data is shaped by both its internal capabilities and its external legitimacy (De-Yolande et al., 2023; Shah et al., 2024; De Waard, 2024). Durable competitive advantage from data ultimately hinges on how effectively it is governed in practice (De Waard, 2024).

2.3.2. Key Data Governance Challenges

Samsung faces several interrelated data governance challenges that directly affect AI performance and risk. Three particularly important issues are data quality, data security, and data sovereignty (Baggiony-Taylor, 2026).

• **Data quality:** Incomplete, outdated, or biased datasets can lead to flawed AI outputs. If different business units or regions use inconsistent data standards, it becomes harder to integrate models and maintain accuracy across the organisation (Government Data Quality Hub, 2021; Samsung Newsroom, 2025).

• **Data security:** AI systems, especially those connected to the internet and cloud services, expand the potential attack surface for cybercriminals. Adversaries may target training data, models, or interfaces to manipulate outputs through data poisoning or adversarial attacks (National Cyber Security Centre, 2021; Jackson, 2023).

• **Data sovereignty:** Growing government requirements for certain categories of data to be stored and processed within national borders complicate global data architectures. These rules

may require regional data centres, segmented data flows, and differentiated AI models for different jurisdictions (Flinders and Smalley, 2026).

From a COSO ERM standpoint, these challenges cut across operational, compliance, and strategic risk categories and therefore call for integrated controls and board-level oversight (Pierce and Goldstein, 2016). Stakeholder theory also suggests that perceived mishandling of data can erode trust among core stakeholder groups, even if the company is technically compliant with formal regulations. In this sense, the risks are as much about legitimacy as about legal exposure (Ayaz et al., 2024). These governance challenges are further complicated by divergent regulatory expectations across jurisdictions, particularly between the UK and the EU.

2.3.3. UK vs EU Data Governance

The UK's data governance regime, based on the UK GDPR and related policy documents, is relatively flexible and principles-based. It places significant responsibility on organisations to interpret and apply high-level rules, with an explicit emphasis on supporting innovation, including in AI and emerging technologies. From an RBV perspective, this flexibility can be attractive, as it may allow Samsung to experiment more freely with data-driven innovation and to extract value from its data assets with fewer ex ante constraints (GOV.UK, 2023; Dessaints, 2026).

However, this model also has drawbacks. The lack of prescriptive, detailed guidance can create uncertainty, as firms may be unsure what counts as full compliance in borderline cases. Heavy reliance on organisational discretion can lead to inconsistent practices across sectors and firms. From an ERM and stakeholder-theoretic viewpoint, such uncertainty can translate into reputational and regulatory risks, especially if future scandals trigger stricter enforcement or legal reform (Travieso-Morales and Smirnova, 2025; Forbes, 2025).

By contrast, the EU, through the General Data Protection Regulation (GDPR) and the EU AI Act, adopts a more rules-based and stringent approach. This framework combines strong enforcement mechanisms, such as high fines and proactive supervisory authorities, with detailed compliance requirements for high-risk AI systems. These requirements include documentation, risk assessments, transparency obligations, and provisions for human oversight. The EU model raises compliance costs and may limit certain forms of data exploitation, potentially constraining RBV-style competitive advantages. Yet it can also provide clearer expectations and stronger consumer trust, aligning with stakeholder theory's

focus on protecting fundamental rights and broader societal interests (Dessaints, 2026; Thomson Reuters Legal, 2026; Brewis et al., 2023; Thambir, 2025).

Overall, this comparison highlights a fundamental trade-off between regulatory flexibility and legal certainty. For Samsung, the challenge is to navigate these differences without fragmenting its internal practices.

2.3.4. Strategic Implications

From a global perspective, these divergent regimes suggest that Samsung should adopt a "highest-standard compliance" strategy, designing AI and data governance to meet the EU's stringent requirements and applying them globally where feasible (Samsung New Zealand, 2025). This promotes operational consistency, reduces the complexity of managing multiple frameworks, simplifies the ERM risk landscape by aligning with demanding stakeholders, and signals a strong commitment to privacy and rights that can build trust among consumers and regulators.

There are, however, clear trade-offs. A highest-standard strategy may impose higher short-term costs and reduce Samsung's ability to exploit more permissive regimes for rapid experimentation and innovation. The strategic task is to balance these risk-reduction and legitimacy benefits against potential opportunity costs. In doing so, Samsung needs to treat data governance not as a purely legal function but as a central component of its long-term value-creation strategy (Samsung Knox, 2018; Travieso-Morales and Smirnova, 2025; Lamba, 2024; Beharry and Pahwa, 2025).

In summary, strong data governance provides the structural backbone for responsible AI, but it does not resolve deeper ethical questions about fairness, autonomy, and surveillance. These issues are explored in the next section on ethical AI use.

2.4. Ethical AI Use

Having established the technical and regulatory foundations of AI risk, this section turns to the ethical tensions inherent in Samsung's AI deployment. It focuses on three key areas: the ethics–profit trade–off, algorithmic bias and fairness, and the challenges of explainability and accountability.

2.4.1. The Ethics–Profit Tension

AI intensifies long-standing tensions between profit maximisation and responsible conduct. On the one hand, there are strong commercial incentives to maximise data utilisation to personalise

services, optimise operations, and increase revenue. On the other hand, protecting user privacy, fairness, and autonomy may require limiting data collection and processing. This tension speaks directly to stakeholder theory, which argues that firms should balance the interests of multiple stakeholders, including customers, employees, regulators, and society, rather than focusing exclusively on shareholders (Alawamleh et al., 2024; Ibidunmoye et al., 2026).

For Samsung, short-term gains from aggressive data use must be weighed against long-term trust, legitimacy, and its broader social licence to operate. COSO ERM is relevant here because it integrates ethical and reputational risks into risk appetite and performance metrics, rather than treating them as purely qualitative. Fully aligning stakeholder interests is unlikely, so Samsung must make explicit trade-offs and be transparent about its choices. This ethics–profit tension is especially visible when AI systems reproduce or amplify social inequalities (Pimentel, 2025; Telecom, 2024).

2.4.2. Algorithmic Bias and Fairness

Algorithmic bias arises when training data reflects existing societal inequalities, such as the under-representation or misrepresentation of certain demographic groups, and models carry these inequalities into their predictions or decisions. In Samsung's case, this could manifest as facial recognition systems that perform less accurately across ethnicities, or as recommendation algorithms that systematically favour certain types of content or products in ways that appear discriminatory or opaque (Jonker and Rogers, 2026).

The impact of such bias can be significant. It may create legal liability under anti-discrimination or consumer protection laws, attract negative media attention and regulatory scrutiny, and undermine consumer trust, thereby reducing the willingness to adopt AI-enabled products and services. Stakeholder theory highlights that marginalised groups, advocacy organisations, and regulators are becoming increasingly vocal stakeholders whose perceptions can shape Samsung's legitimacy and market access. From an ERM perspective, bias-related incidents should therefore be treated as material risks with defined controls, rather than as isolated anomalies (PwC, 2022; Karami et al., 2024).

Addressing these risks requires sustained investment in bias detection methods, inclusive dataset design, and fairness-aware modelling techniques (Chinta et al., 2025). Technical measures alone, however, are insufficient. They need to be supported by multidisciplinary oversight that incorporates legal, ethical, and social perspectives. Even where bias is mitigated,

opaque decision-making can still undermine accountability and stakeholder trust (Hanna et al., 2024).

2.4.3. Explainability and Accountability

Many advanced AI systems function as “black boxes” in the sense that their internal reasoning is difficult for developers, managers, or regulators to interpret. As a result, it may be unclear why a particular decision or prediction was made. This lack of explainability raises both regulatory and ethical concerns. Regulators are increasingly demanding transparency and human-understandable justification for high-risk AI decisions in domains such as finance, healthcare, and employment. Without adequate explainability, it becomes difficult to assign responsibility when AI systems cause harm or make errors (Kosinski, 2026; Paloalto, 2026).

For Samsung, improving explainability means building Explainable AI (XAI) into system design rather than adding it later, and establishing clear accountability for AI-enabled decisions. In COSO ERM terms, this strengthens control activities and information, communication, and monitoring processes. Stakeholder theory highlights that explainability is both a technical need and a means of demonstrating accountability to customers, regulators, and society (IBM, 2026).

2.4.4. Critical Insight

Taken together, these considerations suggest that ethical AI should not be treated merely as a compliance exercise or a marketing slogan. Instead, it should be understood as a strategic necessity that underpins long-term sustainability. By embedding ethical considerations into AI design, deployment, and governance processes, Samsung can reduce legal and regulatory risks, strengthen brand trust and differentiation, and support internal cultures of responsibility and innovation (Bohnsack, 2025).

RBV offers an important additional insight here: ethical governance capabilities can themselves become distinctive organisational resources that are difficult for rivals to imitate, thereby contributing to long-term competitive advantage (Holz, 2024). Ethical AI practices can also help Samsung anticipate and align with future regulatory expectations, although formal compliance requirements will remain a separate and expanding source of risk (Radanliev, 2025).

2.5. Regulatory Compliance

Building on the ethical considerations discussed above, this section examines how different regulatory models shape Samsung's compliance obligations and risk management strategies. It focuses on the contrast between the UK's "pro-innovation" approach and the EU's more prescriptive, risk-based model, before considering the broader challenge of regulatory fragmentation (Donelan, 2023; European Commission, 2026; European Council, 2024).

2.5.1. The UK's Pro-Innovation Model

The UK has articulated a pro-innovation approach to AI regulation that emphasises sector-specific rules and experimentation rather than a single, overarching AI law. Regulators in sectors such as finance, healthcare, and transport are encouraged to tailor AI guidance to their own domains. In parallel, mechanisms like regulatory sandboxes allow firms to test AI solutions under supervision and with some regulatory flexibility. This approach offers several advantages. It provides firms with flexibility to innovate and adapt quickly, and can reduce initial compliance burdens when adopting AI. For Samsung, this may make the UK an attractive environment for piloting new AI applications and data-driven services (Donelan, 2023; Rough, 2026).

However, the model also carries clear risks. Regulatory fragmentation within the UK may emerge as sectoral regulators adopt divergent standards, while long-term uncertainty remains if today's permissive principles are tightened after high-profile AI incidents (Adebisi, 2023). From a COSO ERM perspective, this instability complicates risk assessment and response planning (Sheth and Sinfield, 2024). Stakeholder theory further suggests that serious AI failures could quickly shift public expectations towards a more restrictive regime, directly affecting Samsung's operations (Seddon, 2023).

Overall, while the UK's pro-innovation approach creates room for experimentation, Samsung must manage the associated uncertainty and avoid over-reliance on a regime that may tighten in the future. At the same time, it must navigate the EU's far more detailed and rights-based AI framework.

2.5.2. The EU's Risk-Based Model

The EU AI Act introduces a comprehensive, risk-based framework for artificial intelligence. It categorises AI applications according to their potential impact on fundamental rights and safety. Systems deemed to pose an unacceptable level of risk, such as certain forms of social

scoring, are prohibited outright. High-risk AI systems, including those used in critical infrastructure, employment, and law enforcement, are subject to stringent obligations. These include detailed documentation and technical files, robust risk and quality management processes, and requirements related to transparency, human oversight, robustness, and cybersecurity (European Commission, 2026; European Council, 2024).

For Samsung, any high-risk AI applications in the EU will require significant compliance work, including meeting technical standards, maintaining continuous monitoring, and proving compliance to regulators upon request. COSO ERM offers a structure for integrating these duties into internal controls and governance, ensuring that AI-related risks are captured in risk registers, control activities, and monitoring (EU Artificial Intelligence Act, 2024).

From a stakeholder theory perspective, strong EU expectations around rights-based protections shape what counts as legitimate AI and limit acceptable trade-offs between innovation and fundamental rights (Knowledge Leader, 2022; Gstrein et al., 2024). Consequently, Samsung must treat EU regulators and citizens as central stakeholders whose concerns directly affect its licence to operate in this key market. The contrast between the UK and EU approaches reflects a broader trend towards regulatory divergence in AI.

2.5.3. Regulatory Fragmentation

Beyond the UK and EU, multiple jurisdictions around the world are developing their own AI rules and guidance. The result is a complex and evolving patchwork of requirements that can overlap, diverge, or even conflict. For a global firm such as Samsung, this regulatory fragmentation creates overlapping and sometimes inconsistent compliance demands and can drive up operational costs (Hodge, 2024).

Fragmentation also generates strategic challenges. Product design and AI functionalities may need to be customised by region, which complicates product management and increases the risk of inconsistent user experiences or fragmented data architectures (Lancieri et al., 2025). In addition, regulatory changes can be rapid and politically driven, making it difficult to plan long-term AI investments with confidence.

To respond effectively, Samsung needs strong regulatory intelligence and foresight capabilities. From an ERM standpoint, this means enhancing processes for risk identification and monitoring, with a particular focus on tracking external regulatory developments and feeding them into strategic decision-making (Sermhattakit and Sae Lim, 2025). From a stakeholder perspective, Samsung can also benefit from engaging in multi-stakeholder

initiatives and standard-setting bodies, which can allow it to help shape, rather than simply react to, evolving norms (Blind and Heß, 2023).

In sum, navigating fragmented regulations is not only a legal compliance exercise but also a core element in maintaining stakeholder trust, especially among consumers who may be sensitive to how AI is governed across regions.

2.6. Maintaining Customer Trust

Trust is a crucial outcome of Samsung's technical, ethical, and regulatory choices around AI. This section examines how AI affects customer trust, the risks associated with trust erosion, and practical strategies to build and sustain trust over time (Samsung Newsroom U.K., 2026b).

2.6.1. Trust as Competitive Advantage

In AI-enabled markets, trust is a central determinant of competitive advantage. It influences purchase decisions, since consumers are more likely to buy devices and services from brands they believe will handle their data responsibly. Trust also underpins brand loyalty, enabling firms to retain customers longer and increase customer lifetime value. A visible commitment to privacy, security, and ethical AI can serve as a powerful form of market differentiation, potentially positioning Samsung ahead of less-trusted competitors (Dolen and Islam, 2025; Asaftei et al., 2026).

From an RBV perspective, trust and reputation can be viewed as strategic, hard-to-imitate intangible assets, built over time through consistent behaviour and credible signalling. They are not easily replicated, which makes them particularly valuable in competitive markets. Stakeholder theory reinforces this view by emphasising that these assets depend on Samsung's ability to meet or exceed the expectations of multiple stakeholder groups simultaneously, including consumers, regulators, and civil society organisations (Deloitte, 2024; Aversano, 2025; Afroogh et al., 2024). Recognising trust as a key driver of competitive advantage raises the question of how AI can, in practice, undermine it.

2.6.2. Trust Risks in AI

AI introduces several trust-related risks, notably around data breaches, lack of transparency, and ethical controversies. Hacking incidents or accidental leaks involving AI systems or their training data can significantly undermine confidence and lead to regulatory penalties. Even without breaches, users may become suspicious if they do not understand how AI features work, what data is collected, or how that data is used. Allegations of bias, manipulation, or

intrusive surveillance can quickly damage public perception and erode trust in both AI technologies and the brand that deploys them (Asaftei et al., 2026; Afroogh et al., 2024).

Within the COSO ERM framework, these issues should be classified as key reputational and compliance risks, with clear controls, monitoring mechanisms, and escalation paths. Stakeholder theory suggests that trust erosion in one stakeholder group (for example, privacy activists or digital rights) can spill over to others, including regulators and mainstream consumers, thereby amplifying the impact of individual incidents. In this environment, purely reactive crisis management is unlikely to be sufficient; Samsung needs a proactive and sustained approach to trust-building (Polemi et al., 2024).

2.6.3. Trust-Building Strategies

To maintain and strengthen customer trust, Samsung should embed privacy and security principles into AI-enabled products from the outset, rather than treating them as add-ons. This implies adopting privacy-by-design and security-by-design practices, supported by robust testing and verification procedures (Hiscock, 2023).

In addition, Samsung should provide clear and accessible AI disclosures. These should explain, in straightforward language, how AI features function, what data they rely on, and what choices users have regarding data collection and use. Transparency is more effective when it is specific and concrete, rather than buried in lengthy legal documents (Nabirye et al., 2025).

Meaningful user control is another key element. Samsung can strengthen trust by giving users options to opt out of certain AI features, limit the types of data processing, and manage data retention periods. Providing visible, easy-to-use controls can demonstrate respect for user autonomy and reduce perceptions of surveillance (Deloitte, 2026; Richter, 2025).

Over time, consistent, transparent, and respectful data practices can transform trust into a more durable strategic asset. RBV suggests that organisational capabilities in privacy, security, and ethical communication, when deeply embedded and well executed, can function as sources of enduring competitive advantage. The preceding analysis of risks, governance, ethics, regulation, and trust provides the foundation for the concrete strategic recommendations that follow (Richter, 2025).

2.7. Strategic Recommendations

Based on the findings, Samsung should implement an integrated AI risk management strategy across four key domains: global AI governance, advanced data governance, ethical AI, and regulatory engagement.

Global AI Governance Framework:	Develop a centralised, corporate-level AI governance framework aligned with enterprise risk management (ERM). This framework should establish global principles and risk thresholds while allowing for regional customisation. Invest in Explainable AI (XAI) for high-risk use cases so that regulators, customers, and internal stakeholders can access auditable explanations. Robust governance and XAI capabilities enhance accountability and function as strategic resources (Yu, 2025; Grennan et al., 2022; Damen et al., 2025).
Advanced Data Governance Systems:	Introduce strong data governance mechanisms to support this framework. Use real-time data monitoring to track quality, detect anomalies, and maintain data lineage; reinforce cybersecurity for AI systems; and standardise data classification and retention practices. These steps embed ERM principles into data control and oversight, protect data as a strategic asset, and demonstrate strong data stewardship to stakeholders (Vadher, 2024; Pate, 2024).
Ethical AI Integration:	Integrate ethics throughout AI development and deployment. Mandate ethics training for staff involved in AI and create or strengthen independent ethics or oversight committees for high-risk initiatives. This approach embeds fairness, privacy, and autonomy into decision-making, extends ERM to cover ethical risks, and cultivates distinctive ethical AI capabilities as valuable intangible assets (Lparsons, 2025).
Regulatory Engagement:	Proactively engage with regulators, policymakers, and standard-setting organisations to anticipate legal developments and shape the evolution of AI standards. This enhances ERM by improving the identification of regulatory risks and the ability to respond to them, while also recognising regulators and civil society as critical stakeholders (Metric Stream, 2019).

NB: These recommendations require phased implementation, continuous refinement, and will be further elaborated in the appendix.

3. Conclusion

This conclusion synthesises the report's core arguments and shows how an integrated, theory-informed approach to AI risk management can support Samsung's long-term competitive advantage. Artificial intelligence is reshaping the global business environment, creating major opportunities while introducing complex, interdependent risks for Samsung Electronics. The report has argued that AI risk management must move beyond traditional frameworks by incorporating model and data risk, ethical considerations, and dynamic oversight, extending COSO-style enterprise risk management (ERM) to address AI's emergent properties.

It further contends that regulatory compliance requires a proactive, globally coordinated approach that anticipates regulatory trends and harmonises standards across regions, recognising regulators and policymakers as key stakeholders. At the same time, the ethical and trust-related dimensions of AI are central to sustainable success, influencing customer loyalty, brand equity, and long-term legitimacy.

Drawing on stakeholder theory and the resource-based view (RBV), the report concludes that ethical AI capabilities and robust data governance can serve as durable sources of competitive advantage. By adopting a forward-looking, integrated AI risk management approach grounded in ERM, RBV, and stakeholder theory, Samsung can better mitigate emerging risks, maintain stakeholder trust in its AI-enabled products and services, and secure its long-term competitive position in an increasingly AI-driven global economy.

4. References

1. Adebisi, F. (2023) *What are the main shortcomings of the 'Pro-Innovation Approach to AI Regulation' white paper published by the UK Government in March 2023? – University of Bristol Law School blog*. Available at: https://legalresearch.blogs.bris.ac.uk/2023/07/what-are-the-main-shortcomings-of-the-pro-innovation-approach-to-ai-regulation-white-paper-published-by-the-uk-government-in-march-2023/ (Accessed: 22 April 2026).

2. Afroogh, S., Akbari, A., Malone, E., Kargar, M. and Alambeigi, H. (2024) "Trust in AI: progress, challenges, and future directions." *Humanities and Social Sciences Communications* 11(1). Available at: doi:10.1057/s41599-024-04044-8.

3. Alawamleh, M., Shammas, N., Alawamleh, K. and Ismail, L.B. (2024) "Examining the limitations of AI in business and the need for human insights using Interpretive Structural Modelling." *Journal of Open Innovation Technology Market and Complexity* 10(3), p. 100338. Available at: doi:10.1016/j.joitmc.2024.100338.

4. Allan, N. and Beer, L. (2017) "Strategic Risk: It's all in your head." *ResearchGate*. Available at: https://www.researchgate.net/publication/251746563_Strategic_Risk_It's_all_in_your_head.

5. Asaftei, G.M., Roberts, R., Sticha, A. and Prinsen, C. (2026) *State of AI Trust in 2026: Shifting to the Agentic Era*. Available at: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/state-of-ai-trust-in-2026-shifting-to-the-agentic-era (Accessed: 23 April 2026).

6. Aversano, B. (2025) *Trust is the new currency: How transparency became the ultimate competitive advantage*. Available at: https://www.forbes.com/councils/forbesbusinesscouncil/2025/10/24/trust-is-the-new-currency-how-transparency-became-the-ultimate-competitive-advantage/ (Accessed: 23 April 2026).

7. Ayaz, O., Tabaghdehi, S.A.H., Rosli, A. and Tambay, P. (2024) "Ethical implications of employee and customer digital footprint: SMEs perspective." *Journal of Business Research* 188, p. 115088. Available at: doi:10.1016/j.jbusres.2024.115088.

8. Baggiony-Taylor, M. (2026) "Samsung's AI Strategy and Data Centres: What Links Them?" *Data Centre Magazine* 10 January. Available at: https://datacentremagazine.com/news/samsungs-ai-strategy-and-data-centres-what-links-them.

9. Beharry, R. and Pahwa, S. (2025) "Data and AI governance: a complementary duo for enterprise success." *IBM* 18 November. Available at: https://www.ibm.com/think/insights/data-ai-governance-complementary-duo-enterprise-success#:~:text=While%20data%20and%20AI%20governance,trustworthy%2C%20transparent%20and%20responsible%20AI.

10. Berkovitch, D. (2026) *The 2026 Supply Chain Challenge: Global Trade Disruption*. Available at: https://tax.thomsonreuters.com/blog/2026s-supply-chain-challenge-confronting-complexity-and-disruption-in-global-trade-tri/ (Accessed: 21 April 2026).

11. Blind, K. and Heß, P. (2023) "Stakeholder perceptions of the role of standards for addressing the sustainable development goals." *Sustainable Production and Consumption* 37, pp. 180–190. Available at: doi:10.1016/j.spc.2023.02.016.

12. Bohnsack, R. (2025) *Ethical AI as Competitive Advantage: Why doing the right thing pays off*. Available at: https://www.linkedin.com/pulse/ethical-ai-competitive-advantage-why-doing-right-thing-ren%C3%A9-bohnsack-fdjgf (Accessed: 22 April 2026).

13. Bräuer-Provasnek, A.K. (2017) "Stakeholder engagement to secure legitimacy – the social license to operate." *ResearchGate*. Available at: https://www.researchgate.net/publication/310604621_Stakeholder_Engagement_to_Secure_Legitimacy_-_The_Social_License_to_Operate.

14. Brewis, C., Dibb, S. and Meadows, M. (2023) "Leveraging big data for strategic marketing: A dynamic capabilities model for incumbent firms." *Technological Forecasting and Social Change* 190, p. 122402. Available at: doi:10.1016/j.techfore.2023.122402.

15. Chanda, S.S. and Banerjee, D.N. (2022) "Omission and commission errors underlying AI failures." *AI & Society* 39(3), pp. 937–960. Available at: doi:10.1007/s00146-022-01585-x.

16. Chinta, S.V. et al. (2025) "AI-driven healthcare: A review on ensuring fairness and mitigating bias." *PLOS Digital Health* 4(5), p. e0000864. Available at: doi:10.1371/journal.pdig.0000864.

17. Chopvitayakun, S., Rattanasiriwongwut, M. and Kadmateekarun, P. (2026) "IoT-Based Smart Home Integration: innovative system architecture for intelligent monitoring and control." in *Lecture notes in networks and systems*., pp. 299–310. Available at: doi:10.1007/978-3-032-13153-9_23.

18. Colantone, I. (2025) *De-Globalization and fragmentation*. Available at: https://iep.unibocconi.eu/sites/default/files/media/attach/WP_Colantone.pdf (Accessed: 21 April 2026).

19. Coleman, R. (2011) "Operational Risk." *Wiley Encyclopedia of Operations Research and Management Science*. Available at: doi:10.1002/9780470400531.eorms0591.

20. Criddle, C. (2021) *Chip shortage: Samsung warns of "serious imbalance."* Available at: https://www.bbc.co.uk/news/technology-56433082 (Accessed: 20 April 2026).

21. Damen, V., Wiersma, M., Aydin, G. and Van Haasteren, R. (2025) "Explainable AI for EU AI Act compliance audits." *Maandblad Voor Accountancy En Bedrijfseconomie* 99(4), pp. 231–242. Available at: doi:10.5117/mab.99.150303.

22. De Waard, F. (2024) *Samsung proves real-time data is a catalyst for better customer experiences*. Available at: https://business.adobe.com/blog/the-latest/samsung-proves-real-time-data-is-a-catalyst-for-better-customer-experiences (Accessed: 21 April 2026).

23. Dees, M. (2025) *U.S. grants Samsung and SK Hynix temporary leeway in China*. Available at: https://www.techzine.eu/news/privacy-compliance/137585/us-grants-samsung-and-sk-hynix-temporary-leeway-in-china/ (Accessed: 20 April 2026).

24. Deloitte (2017) *COSO ERM Framework Update | Deloitte Ireland | Risk Advisory*. Available at: https://www.deloitte.com/ie/en/services/consulting-risk/perspectives/coso-erm-update.html (Accessed: 21 April 2026).

25. Deloitte (2024) *Building trust in digital strategy: a key to competitive advantage and Long-Term success*. Available at: https://www.deloitte.com/in/en/issues/trust/building-trust-in-digital-strategy-a-key-to-competitive-advantage-and-long-term-success.html (Accessed: 23 April 2026).

26. Deloitte (2026) *How trust in your organisation can drive performance*. Available at: https://www.deloitte.com/uk/en/issues/trust.html (Accessed: 23 April 2026).

27. Dessaints, A. (2026) "UK GDPR vs. EU GDPR (2026) | DPO Consulting." *Learn GDPR* 14 April. Available at: https://www.dpo-consulting.com/blog/uk-gdpr-vs-eu-gdpr#:~:text=The%20UK%20has%20expressed%20a%20desire%20to,leading%20to%20more%20complex%20data%20transfer%20requirements. (Accessed: 20 April 2026).

28. De-Yolande, M.H., Doh-Djanhoundji, T. and Constant, G.Y. (2023) "Breach Notification in the General Data Protection Regulation." *Voice of the Publisher* 09(04), pp. 334–347. Available at: doi:10.4236/vp.2023.94026.

29. Digital Watch (2026) "Samsung advances toward AI autonomous factories by 2030 | Digital Watch Observatory." *Digital Watch Observatory* 2 March. Available at: https://dig.watch/updates/samsung-advances-toward-ai-autonomous-factories-by-2030.

30. Dolen, D. and Islam, K. (2025) *Competing on trust in the age of AI*. Available at: https://www.pwc.com/gx/en/issues/trust/competing-trust-age-of-ai.html (Accessed: 27 April 2026).

31. Donelan, M. (2023) *A pro-innovation approach to AI regulation*. Available at: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper (Accessed: 22 April 2026).

32. Esposito, M. and Sergi, B.S. (2026) *Technology restrictions have become a central instrument of economic statecraft*. Available at: https://www.techpolicy.press/technology-restrictions-have-become-a-central-instrument-of-economic-statecraft/ (Accessed: 21 April 2026).

33. EU Artificial Intelligence Act (2024) *High-level summary of the AI Act*. Available at: https://artificialintelligenceact.eu/high-level-summary/ (Accessed: 24 April 2026).

34. European Banking Authority (2024) *Macroeconomic Environment and Market Sentiment | European Banking Authority*. Available at: https://www.eba.europa.eu/publications-and-media/publications/macroeconomic-environment-and-market-sentiment-0 (Accessed: 20 April 2026).

35. European Commission (2026) *AI Act*. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (Accessed: 22 April 2026).

36. European Council (2024) *ARTIFICIAL Intelligence (AI) Act: Council gives final green light to the first worldwide rules on AI*. Available at: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/ (Accessed: 22 April 2026).

37. European Parliament (2020) *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*., p. PE 641.530. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (Accessed: 21 April 2026).

38. Finextra (2025) *How AI Will Reshape Banking Risk Management: By Stanley Epstein*. Available at: https://www.finextra.com/blogposting/30251/how-ai-will-reshape-banking-risk-management (Accessed: 20 April 2026).

39. Flinders, M. and Smalley, I. (2026) "Data sovereignty." *Think* 10 March. Available at: https://www.ibm.com/think/topics/data-sovereignty (Accessed: 21 April 2026).

40. Forbes (2025) *Strengthening AI strategies with proactive compliance: expert tips*. Available at: https://www.forbes.com/councils/forbestechcouncil/2025/12/02/strengthening-ai-strategies-with-proactive-compliance-expert-tips/ (Accessed: 22 April 2026).

41. Gerken, T. and McMahon, L. (2022) *Big tech must deal with disinformation or face fines, says EU*. Available at: https://www.bbc.co.uk/news/technology-61817647 (Accessed: 21 April 2026).

42. Ghisellini, P., Passaro, R. and Ulgiati, S. (2021) "Revisiting Keynes in the Light of the Transition to Circular Economy." *Circular Economy and Sustainability* 1(1), pp. 143–171. Available at: doi:10.1007/s43615-021-00016-1.

43. Gibson, K. (2026) *The role of artificial intelligence in digital transformation*. Available at: https://online.hbs.edu/blog/post/ai-digital-transformation (Accessed: 20 April 2026).

44. Government Data Quality Hub (2021) "What is data quality?" *GOV.UK* 6 May. Available at: https://www.gov.uk/government/news/what-is-data-quality.

45. GOV.UK (2023) "British Businesses to Save Billions Under New UK Version of GDPR." *GOV.UK* 8 March. Available at: https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr.

46. Grennan, L., Kremer, A., Singla, A. and Zipparo, P. (2022) *Why businesses need explainable AI—and how to deliver it*. Available at: https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-businesses-need-explainable-ai-and-how-to-deliver-it (Accessed: 23 April 2026).

47. Gstrein, O.J., Haleem, N. and Zwitter, A. (2024) "General-purpose AI regulation and the European Union AI Act." *Internet Policy Review* 13(3). Available at: doi:10.14763/2024.3.1790.

48. Gutterman, A.S. (2023) "Stakeholder Theory." *ResearchGate*. Available at: https://www.researchgate.net/publication/369194606_Stakeholder_Theory.

49. Han, M. (2024) *Global Trends and Implications in AI Risk Management*. Available at: https://www.samsungsds.com/eu/insights/ai-risks-and-responses.html (Accessed: 21 April 2026).

50. Hanna, M.G. et al. (2024) "Ethical and bias considerations in Artificial Intelligence/Machine Learning." *Modern Pathology* 38(3), p. 100686. Available at: doi:10.1016/j.modpat.2024.100686.

51. Hiscock, R. (2023) "A Guide to Privacy by Design | Blog | OneTrust." *OneTrust* 30 August. Available at: https://www.onetrust.com/blog/privacy-by-design/ (Accessed: 27 April 2026).

52. Hodge, N. (2024) *AI and regulatory overlap*. Available at: https://www.ibanet.org/ai-and-regulatory-overlap (Accessed: 22 April 2026).

53. Holweg, M., Younger, R. and Wen, Y. (2022) "The reputational risks of AI." *California Management Review* 24 January. Available at: https://cmr.berkeley.edu/2022/01/the-reputational-risks-of-ai/ (Accessed: 21 April 2026).

54. Holz, H.F. (2024a) "The Resource-Based View of the Firm." in *Elsevier eBooks*, pp. 316–323. Available at: doi:10.1016/b978-0-443-13701-3.00383-2.

55. Ians (2024) "Samsung vows to prioritise retaining its technological supremacy." *ET Telecom.com* 2 January. Available at: https://telecom.economictimes.indiatimes.com/news/devices/samsung-vows-to-prioritise-retaining-its-technological-supremacy/106475398.

56. Ibidunmoye, A.F., Eneano, G.A., Ikeakaonwu, O.M., Kolawole, L.O., Omigbodun, F.T., Olawale, R.A. and Chuwa, C.C. (2026) "The Structural Tension Between AI Optimisation and Ethical Governance: Empirical Evidence from Organisational Decision-Making." *Research Square*. Available at: doi:10.21203/rs.3.rs-8605675/v1.

57. IBM (2026) "Explainable AI." *IBM* 9 March. Available at: https://www.ibm.com/think/topics/explainable-ai#:~:text=Explainable%20AI%20is%20used%20to,responsible%20approach%20to%20AI%20development. (Accessed: 22 April 2026).

58. ICO (2025) *New guidance to help smart product manufacturers get data protection right*. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/06/new-guidance-to-help-smart-product-manufacturers-get-data-protection-right/ (Accessed: 21 April 2026).

59. IMF (2026a) *Global economy in the shadow of war*. Available at: https://www.imf.org/en/publications/weo/issues/2026/04/14/world-economic-outlook-april-2026 (Accessed: 20 April 2026).

60. IMF (2026b) *WORLD ECONOMIC OUTLOOK UPDATE*. Available at: https://www.imf.org/-/media/files/publications/weo/2026/january/english/text.pdf (Accessed: 20 April 2026).

61. Jackson, A. (2023) "Major Samsung data breach exposes customer data." *Cyber Magazine* 20 November. Available at: https://cybermagazine.com/operational-security/major-samsung-data-breach-exposes-customer-data.

62. John, A.O., Adejumo, E. and Larbi, S.Y. (2025) "AI-Driven Supply Chain Risk Management in the Manufacturing Sector: Tackling Data Bias, Ensuring..." *ResearchGate*. Available at: https://www.researchgate.net/publication/392496390_AI-Driven_Supply_Chain_Risk_Management_in_the_Manufacturing_Sector_Tackling_Data_Bias_Ensuring_Algorithmic_Transparency_and_Enhancing_Human-AI_Collaboration.

63. Jonker, A. and Rogers, J. (2026) "Algorithmic bias." *IBM* 26 February. Available at: https://www.ibm.com/think/topics/algorithmic-bias (Accessed: 22 April 2026).

64. Karami, A., Shemshaki, M. and Ghazanfar, M.A. (2024) "Exploring the Ethical Implications of AI-Powered Personalisation in Digital Marketing." *Data Intelligence* 7(4), pp. 1035–1084. Available at: doi:10.3724/2096-7004.di.2024.0055.

65. Knowledge Leader (2022) *COSO: Step up your ERM, integrated and internal controls | Knowledge Leader*. Available at: https://www.knowledgeleader.com/blog/coso-step-your-erm-integrated-and-internal-controls (Accessed: 22 April 2026).

66. Korea Pro (2025) "Samsung's record quarter belies rising risks from weaponised US trade policy." *Korea Pro* 1 May. Available at: https://koreapro.org/2025/04/samsungs-record-quarter-belies-rising-risks-from-weaponized-us-trade-policy/.

67. Kosinski, M. (2026) "Black Box AI." *IBM* 19 March. Available at: https://www.ibm.com/think/topics/black-box-ai (Accessed: 22 April 2026).

68. Kumar, S. (2025) "The Strategic Imperative of Enterprise Risk Management (ERM)." *ResearchGate*. Available at: doi:10.13140/rg.2.2.17884.86400.

69. Lamba, S. (2024) *Why should you audit your business's UK GDPR compliance?* Available at: https://legalvision.co.uk/data-privacy-it/audit-business-uk-gdpr-compliance/ (Accessed: 22 April 2026).

70. Lancieri, F., Lancieri, L. and Bechtold, S. (2025) "AI Regulation: The Politics of Fragmentation and Regulatory Capture." *Oxford Law Blogs* 19 June. Available at: https://blogs.law.ox.ac.uk/oblb/blog-post/2025/06/ai-regulation-politics-fragmentation-and-regulatory-capture (Accessed: 22 April 2026).

71. Lparsons (2025) *Ethics in AI: Why it Matters - Professional & Executive Development | Harvard DCE*. Available at: https://professional.dce.harvard.edu/blog/ethics-in-ai-why-it-matters/#Meet-Our-Expert (Accessed: 23 April 2026).

72. Metric Stream (2019) *Regulatory Engagement Roundtable: Key takeaways*. Available at:

https://www.garp.org/hubfs/Whitepapers/a2r1W0000015RsbQAE_regulatoryengagement.whitepaper.Oct19.pdf?utm_source=chatgpt.com (Accessed: 23 April 2026).

73. Nabirye, A., Okwir and Special, K. (2025) "The role of transparency in legal communication." *ResearchGate*. Available at: https://www.researchgate.net/publication/388919154_The_Role_of_Transparency_in_Legal_Communication.

74. National Cyber Security Centre (2021) *Data security*. Available at: https://www.ncsc.gov.uk/collection/10-steps/data-security (Accessed: 21 April 2026).

75. Ozan, S. (2025) "The ripple effects of US export controls on Samsung and the semiconductor industry." *Report Linker* 13 May. Available at: https://www.reportlinker.com/article/11492.

76. PaloAlto (2026) *What is explainability?* Available at: https://www.paloaltonetworks.com/cyberpedia/ai-explainability (Accessed: 22 April 2026).

77. Pate, W. (2024) *What is advanced data governance from Microsoft?* Available at: https://www.innovativecomp.com/what-is-advanced-data-governance-from-microsoft/ (Accessed: 23 April 2026).

78. Pierce, E.M. and Goldstein, J. (2016) "Moving from enterprise risk management to strategic risk management: Examining the revised COSO ERM framework." *ResearchGate*. Available at: https://www.researchgate.net/publication/308890946_Moving_From_Enterprise_Risk_Management_to_Strategic_Risk_Management_Examining_the_Revised_COSO_ERM_Framework.

79. Pimentel, B. (2024) *Enterprise Risk Management (ERM): An Overview*. Available at: https://legal.thomsonreuters.com/blog/what-is-enterprise-risk-management/ (Accessed: 22 April 2026).

80. Polemi, N., Praça, I., Kioskli, K. and Bécue, A. (2024) "Challenges and efforts in managing AI trustworthiness risks: a state of knowledge." *Frontiers in Big Data* 7, p. 1381163. Available at: doi:10.3389/fdata.2024.1381163.

81. PwC (2022) *Understanding algorithmic bias and how to build trust in AI: PwC*. Available at: https://www.pwc.com/us/en/tech-effect/ai-analytics/algorithmic-bias-and-trust-in-ai.html (Accessed: 22 April 2026).

82. Radanliev, P. (2025) "Privacy, ethics, transparency, and accountability in AI systems for wearable devices." *Frontiers in Digital Health* 7, p. 1431246. Available at: doi:10.3389/fdgth.2025.1431246.

83. Richter, A. (2025) *How to build trustworthy AI from the ground up with privacy by design?* Available at: https://techgdpr.com/blog/how-to-build-trustworthy-ai-from-the-ground-up-with-privacy-by-design/ (Accessed: 23 April 2026).

84. Rough, E. (2026) *AI regulation in the UK*. Available at: https://researchbriefings.files.parliament.uk/documents/CBP-10003/CBP-10003.pdf (Accessed: 27 April 2026).

85. Samsung (2025) *Human rights due diligence*. Available at: https://www.samsung.com/global/sustainability/popup/popup_doc/AYUqpazKDLYAIx_C/ (Accessed: 21 April 2026).

86. Samsung Knox (2018) *General Data Protection Regulation (GDPR) | Samsung Knox*. Available at: https://www.samsungknox.com/en/gdpr (Accessed: 22 April 2026).

87. Samsung New Zealand (2025) *Turn regulatory pressure into operational advantages with Galaxy Devices! | Samsung Business New Zealand*. Available at: https://www.samsung.com/nz/business/insights/turn-regulatory-pressure-into-operational-advantages-with-galaxy-devices/?srsltid=AfmBOooVN89H7U254VmTyZkvoKKRTf8uAtmd2MWvz786fWnjAjQHthGk (Accessed: 22 April 2026).

88. Samsung Newsroom (2024) "[AI Leadership] 3 Samsung's AI strategy centred on customer experiences." *Samsung Global Newsroom* 9 December. Available at: https://news.samsung.com/global/ai-leadership-%E2%91%A2-samsungs-ai-strategy-centered-on-customer-experiences.

89. Samsung Newsroom (2025a) "Samsung and Google Cloud Join Forces to Bring Generative AI to Samsung Galaxy S24 Series." *Samsung Global Newsroom* 17 October. Available at: https://news.samsung.com/global/samsung-and-google-cloud-join-forces-to-bring-generative-ai-to-samsung-galaxy-s24-series.

90. Samsung Newsroom (2025b) "The Learning Curve, Part 3: Taking AI Data from Good to Great." *Samsung Global Newsroom* 17 October. Available at: https://news.samsung.com/global/the-learning-curve-part-3-taking-ai-data-from-good-to-great.

91. Samsung Newsroom U.K. (2026a) *Samsung Electronics announces strategy to transition global manufacturing into 'AI-Driven Factories' by 2030*. Available at: https://news.samsung.com/uk/samsung-electronics-announces-strategy-to-transition-global-manufacturing-into-ai-driven-factories-by-2030 (Accessed: 20 April 2026).

92. Samsung Newsroom U.K. (2026b) *Samsung explores how trust, security and privacy shape the future of AI at CES 2026*. Available at: https://news.samsung.com/uk/samsung-explores-how-trust-security-and-privacy-shape-the-future-of-ai-at-ces-2026 (Accessed: 23 April 2026).

93. Samsung SDS (2026) *Samsung SDS unveils Top 5 cybersecurity threats for 2026*. Available at: https://www.samsungsds.com/en/news/enterpriseai-260128.html (Accessed: 21 April 2026).

94. Samsung U.S. Newsroom (2026) "Samsung explores how trust, security and privacy shape the future of AI at CES 2026." *Emerging Technology* 6 January. Available at: https://news.samsung.com/us/samsung-trust-security-privacy-future-ai-ces-2026.

95. Seddon, P. (2023) "UK government must be more open on use of AI, say campaigners." *BBC News* 13 June. Available at: https://www.bbc.co.uk/news/uk-politics-65842385.

96. Sermhattakit, A. and Sae-Lim, P. (2025) "Key Risks and Mitigation Strategies in Enterprise Risk Management for Private Hospitals: A Mixed-Method Study." *INQUIRY the Journal of Health Care Organisation Provision and Financing* 62, p. 469580251347132. Available at: doi:10.1177/00469580251347132.

97. Shah, S.Q.A., Woon, L.F., Shad, M.K. and Hamad, S. (2024) "Integrating enterprise risk Management on the nexus of sustainability reporting and firm Performance: A Conceptual study." in *The Emerald Handbook of Ethical Finance and Corporate Social Responsibility:* pp. 565–579. Available at: doi:10.1108/978-1-80455-406-720241025.

98. Sheth, A. and Sinfield, J.V. (2024) "Advancing the complex adaptive systems approach to enterprise risk management with quantified risk networks (QRNs)." *Scientific Reports* 14(1), p. 22312. Available at: doi:10.1038/s41598-024-71764-x.

99. Soner, M. and Karadag, M. (2026) "A COSO-Based Enterprise Risk Management Maturity in the Service Industry: Perspectives from Turkish Hotels and Hospitals." *Sustainability* 18(4), p. 1929. Available at: doi:10.3390/su18041929.

100. Tao, C., Li, X. and Xu, Y. (2025) "Government digital subsidies and corporate digital technology innovation: Evidence from Chinese listed companies." *Journal of Innovation & Knowledge* 10(5), p. 100797. Available at: doi:10.1016/j.jik.2025.100797.

101. TeamMate (2026) *Two perspectives on AI in Operational Risk management*. Available at: https://www.wolterskluwer.com/en/expert-insights/two-perspectives-ai-operational-risk-management (Accessed: 21 April 2026).

102. Thambir (2025) "UK GDPR vs EU GDPR: What Businesses Need to Know in 2024." *Creative Networks* 17 March. Available at: https://www.creative-n.com/blog/uk-gdpr-vs-eu-gdpr-what-businesses-need-to-know-in-2024/ (Accessed: 22 April 2026).

103. Thomson Reuters Legal (2026) *Top five concerns with GDPR compliance*. Available at: https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance (Accessed: 22 April 2026).

104. Travieso-Morales, V. and Smirnova, Y. (2025) "Why is GDPR compliance still so difficult? - LSE Business Review." *LSE Business Review - Connecting business research with policy, practice and public debate* 1 August. Available at: https://blogs.lse.ac.uk/businessreview/2025/08/01/why-is-gdpr-compliance-still-so-difficult/ (Accessed: 22 April 2026).

105. Treharne, T. (2026) *How social media can damage a company's reputation – and how to address it*. Available at: https://www.strategic-risk-global.com/reputational-risk/how-social-media-can-damage-a-companys-reputation-and-how-to-address-it/1430701.article (Accessed: 21 April 2026).

106. Vadher, K. (2024) *Data governance – why it matters to AI success and more*. Available at: https://www.useready.com/blog/data-governance-why-it-matters-to-ai-success-and-more (Accessed: 23 April 2026).

107. Wei, T., Wu, H., Dowling, M. and Ardekani, A.M. (2025) "Financial perceptions and AI infringement risks." *International Review of Economics & Finance* 101, p. 104204. Available at: doi:10.1016/j.iref.2025.104204.

108. World Economic Forum (2025) *AI geopolitics and data in the era of technological rivalry*. Available at: https://www.weforum.org/stories/2025/07/ai-geopolitics-data-centres-technological-rivalry/ (Accessed: 21 April 2026).

109. Yu, J. (2025) *How the world can build a global AI governance Framework*. Available at: https://www.weforum.org/stories/2025/11/trust-ai-global-governance/ (Accessed: 23 April 2026).

5. Appendix

5.1. Implementation Plan

A three-phase, 36-month roadmap translates these strategies into action: Foundation (0–12 months), Integration (12–24 months), and Optimisation (24–36 months).

1. **Foundation Phase (0–12 Months)**

Key activities: Samsung should first conduct an enterprise-wide AI risk audit that maps AI systems, use cases, data flows, and risk exposures using COSO ERM categories, integrating AI model and data risks into existing risk registers and heat maps (Deloitte, 2017; Knowledge Leader, 2022; Pimentel, 2024; Kumar, 2025). An AI governance committee spanning technology, legal, compliance, security, ethics, and business units should be created and embedded within board-level risk structures to ensure clear ownership and oversight (Han, 2024; Shah et al., 2024). Internal AI policies and standards for model development, testing, documentation, and ethics should then be developed, aligning with stakeholder theory and treating AI risks as enterprise-wide rather than purely technical (Gutterman, 2023; Soner and Karadag, 2026).

KPIs: Success in this phase is evidenced by a comprehensive AI risk inventory and heat map integrated into the ERM framework, and by a formal AI governance structure with defined roles, responsibilities, and reporting lines (Sheth and Sinfield, 2024; Sermhattakit and Sae-Lim, 2025).

2. **Integration Phase (12–24 Months)**

Key activities: In the second phase, Samsung should deploy Explainable AI (XAI) for critical, high-risk applications and phase out opaque "black box" models where they undermine accountability, auditability, or regulatory compliance (Grennan et al., 2022; Damen et al., 2025; IBM, 2026; Kosinski, 2026; PaloAlto, 2026). In parallel, it should implement compliance frameworks aligned with the EU AI Act, EU/UK GDPR, and the UK's pro-innovation model, explicitly linking these obligations to ERM risk registers, controls, and monitoring (European Parliament, 2020; European Council, 2024; European Commission, 2026; Dessaints, 2026; Donelan, 2023; Travieso-Morales and Smirnova, 2025).

AI risk, ethics, and compliance training should be delivered to technical and non-technical staff, covering issues such as algorithmic bias, fairness, and the ethics–profit tension (PwC, 2022; Lparsons, 2025; Hanna et al., 2024; Jonker and Rogers, 2026; Alawamleh et al., 2024; Ibidunmoye et al., 2026). This embeds ethical AI considerations into day-to-day decision-making and strengthens Samsung's organisational capabilities in responsible AI.

KPIs: Key indicators include a reduction in AI-related compliance gaps and audit findings, and a higher proportion of high-risk AI systems equipped with documented explanations, human oversight, and clear accountability lines (EU Artificial Intelligence Act, 2024; Hodge, 2024).

3. **Optimisation Phase (24–36 Months)**

Key activities: The final phase focuses on continuous improvement. Samsung should introduce real-time monitoring of AI performance, bias, drift, and security, integrated with ERM reporting and existing cyber-risk processes (TeamMate, 2026; Polemi et al., 2024; National Cyber Security Centre, 2021; Samsung SDS, 2026). Data governance must be strengthened through real-time data quality management, anomaly detection, and robust lineage tracking, protecting data as a strategic and trustworthy asset (Government Data Quality Hub, 2021; Beharry and Pahwa, 2025; Vadher, 2024; Pate, 2024; De Waard, 2024).

Samsung should also enhance regulatory intelligence and scenario planning to anticipate and respond quickly to new AI and data rules in fragmented global regimes (Lancieri et al., 2025; Hodge, 2024; Han, 2024). Strategic refinement should explicitly apply the Resource-Based View and stakeholder theory, treating ethical AI capabilities, data governance, and trust as VRIN-type resources that underpin long-term competitive advantage (Holz, 2024a; Bohnsack, 2025; Gutterman, 2023).

KPIs: Optimisation success is reflected in improved customer trust metrics such as brand indices, NPS, and targeted trust surveys alongside a reduction in AI-related incidents, including operational failures, data breaches, and regulatory issues (Deloitte, 2024; Deloitte, 2026; Dolen and Islam, 2025; Asaftei et al., 2026; Afroogh et al., 2024; Aversano, 2025). Over time, these outcomes demonstrate that robust, ethical AI risk management has become a source of durable strategic advantage for Samsung.

At the end, to stay resilient amid rapid change, Samsung should actively implement scenario planning, feed its insights into ERM, embed agile AI governance in day-to-day decisions, and build routine ethical review into new AI initiatives. These implementation-focused steps create a future-ready AI risk management ecosystem that captures AI's benefits while managing long-term risks in practice.