

شركة ياقوت وزمرد
Yaqoot & Zumurod Co.



Confidence in Crisis

Navigating Risk
and Resilience in
Saudi Arabia's
Transformative
Economy





Confidence in Crisis

A Strategic Look at Crisis Preparedness
in Saudi Arabia's Dynamic Economy

The Vision 2030 Engine:

A Landscape of Growth & Risk

Saudi Arabia's Vision 2030 is fueling historic economic diversification and attracting global investment. This rapid growth, however, creates a complex new risk environment that organizations must navigate.

Non-Oil
GDP Growth
4.4%

Q1 2025
FDI Inflow
22.2B SAR
(+44% YoY)

Cyber
Disruption Risk
72%
of firms expect disruption

Credits



Mansour Al Jabarty

Communications & Media Consultant
Strategic Communications | Public Relations (PR)
Media Relations | Reputation Management
Crisis Communications | Certified Trainer
Media Training | Public Speaking Coaching



Tasneem Edwan

Digital Communication Consultant
Business Development | Strategy
Planning and Implementation | Quality Control
Digital Transformation | Change Management
Continuous Improvement | Corporate Communication



Eng. Naif mashhor

Corporate Communication Consultant

Table of Content

Confidence in Crisis:	
Navigating Risk and Resilience in Saudi Arabia's Transformative Economy	3
Introduction:	7
Methodology:	9
Glossary	10
Executive Summary	12
The Dual Realities of the Saudi Business Landscape:	
Unprecedented Growth and Amplified Risk	13
The Engine of Transformation: Vision 2030 and Economic Diversification	13
The Inevitable Consequence: A New Generation of Interconnected Risks	14
Answering the Poll:	
A Multi-Faceted Analysis of Confidence in Crisis Communication	17
If the Dominant Answer is "Very Confident": The Preparedness Paradox	17
If the Dominant Answer is "Somewhat Confident": The Aspirational Gap	18
If the Dominant Answer is "Not Very Confident": The Overwhelmed Realists	19
If the Dominant Answer is "Unsure": The Ambiguity of a Transforming Market	20
Strategic Imperatives for Building Crisis Resilience in the Saudi Market	22
From Compliance to Competitive Advantage: Integrating Crisis Management with Strategy	22
Bridging the Cultural-Operational Divide: Creating a Bicultural Resilience Framework	22
Investing in Human and Technological Capital: The Twin Pillars of Modern Resilience	23
Proactive and Authentic Stakeholder Engagement: The Core of Crisis Communication	24
Conclusion:	27
References:	29

INTRODUCTION

Introduction

The business landscape of the Kingdom of Saudi Arabia (KSA) is undergoing a transformation of historic proportions, driven by the ambitious national strategy, Vision 2030. This period of hyper-growth has unlocked unprecedented opportunities, attracting significant foreign investment and fueling a dynamic non-oil economy.¹ However, this rapid evolution brings with it a new and complex array of risks, from the logistical challenges of delivering giga-projects to the ever-present threat of sophisticated cyberattacks.³ In this high-stakes environment, an organization's ability to prepare for, respond to, and recover from a crisis is no longer a secondary concern but a cornerstone of strategic success and long-term viability.

This report provides a strategic analysis of crisis communication preparedness within the Saudi market. It examines the paradox of a nation demonstrating high levels of macroeconomic resilience and investor confidence, while many individual organizations grapple with immature risk management frameworks and cultural barriers that hinder effective crisis response.⁵ The central argument is that the prevailing sentiment among businesses is one of "Somewhat Confident"—a state of awareness that a plan is necessary, but a lack of full confidence that the existing plan is adequate for the dynamic reality on the ground. By dissecting the drivers and vulnerabilities behind each possible level of confidence, this analysis offers a nuanced perspective on the Kingdom's collective resilience and outlines the strategic imperatives for leaders aiming to navigate the intricate relationship between opportunity and risk in one of the world's most dynamic economies.

METHODOLOGY

Methodology

- 1** Analyze the current business and economic climate in Saudi Arabia, focusing on key initiatives like Vision 2030, major giga-projects, and the increasing role of foreign investment. Identify the common operational, reputational, and regulatory risks businesses face in this evolving market.
 
- 2** For the potential outcome "Very confident – we're fully prepared," investigate the characteristics of a best-in-class crisis communication plan tailored to the Saudi context. Research the strategic advantages this level of preparedness offers, such as investor confidence and brand resilience, and find examples of strong crisis management by companies in the region.
 
- 3** For the potential outcome "Somewhat confident – we have a plan, but it needs refining," explore the typical gaps in corporate crisis plans within the Saudi market. Analyze market trends, such as rapid digital transformation and a dynamic social media landscape, that would necessitate continuous refinement of these plans.
 
- 4** For the potential outcome "Not very confident – we need to develop/update our plan," identify the types of organizations that might lack preparedness and the underlying reasons, such as resource constraints or rapid growth. Detail the significant vulnerabilities these organizations face, from operational disruption to regulatory penalties.
 
- 5** For the potential outcome "Unsure – not directly involved in crisis planning," analyze what a high response rate would imply about corporate culture in Saudi Arabia. Explore themes like departmental silos, top-down communication structures, and the potential strategic risks of a workforce that is not engaged in crisis preparedness.
 
- 6** Compare the likely levels of crisis communication maturity across different key sectors in the Saudi economy, such as energy, finance, tourism, and technology. Identify sector-specific challenges and regulatory pressures that influence preparedness.
 
- 7** Synthesize the findings for each potential poll outcome. Formulate a deep analysis from the perspective of a market strategist, explaining what each dominant response would signify about the overall resilience, maturity, and risk landscape of the Saudi business environment.
 

Glossary

Term	Definition
BCM Business (Continuity Management)	A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities. ²¹
CERC (Crisis and Emergency Risk Communication)	A model that serves as a tool to guide authorities' communication strategies during different stages of a crisis, specifying a broad set of communication activities that vary throughout the life cycle of the crisis.
Cybersecurity	The practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. ⁸ In the Saudi context, it involves implementing robust protocols and data protection measures to counter rising threats. ⁸
DGA (Digital Government Authority)	A Saudi government body that plays a crucial part in enhancing the reliability and continuity of digital services in government entities. It has published guidelines on adopting resilience principles and hosts annual compliance scores to strengthen these efforts .
ERM (Enterprise Risk Management)	A comprehensive and integrated approach to managing an organization's risks, which involves identifying, analyzing, and responding to potential risks that could impact its objectives. It considers a wider range of risks beyond traditional safety and compliance. ⁴⁴
FDI (Foreign Direct Investment)	A long-term investment by an entity residing in one economy into an enterprise in another economy, where the investor holds 10% or more of the voting power, implying a significant degree of influence over the enterprise.
Giga-Projects	Extremely large-scale and ambitious investment projects designed to stimulate economic growth and diversification. In Saudi Arabia, these include projects like NEOM, the Red Sea Project, and Qiddiya, which are central to Vision 2030. ¹³
GSR (Governance, Sustainability, and Resilience)	A performance framework used to evaluate sovereign wealth funds and other large investors. It assesses an organization's commitment and performance in the areas of governance, sustainability, and resilience .

Glossary (continued)

Term	Definition
IMF (International Monetary Fund)	A global organization of 190 countries working to foster global monetary cooperation, secure financial stability, facilitate international trade, promote high employment and sustainable economic growth, and reduce poverty around the world.
KSA	An acronym for the Kingdom of Saudi Arabia.
NCA (National Cybersecurity Authority)	The Saudi government authority responsible for developing and issuing national cybersecurity policies, frameworks, standards, and guidelines to ensure national cyber resilience.
NEOM	A futuristic giga-project in northwest Saudi Arabia, envisioned as a smart city and a hub for innovation, technology, and sustainable living. ¹³
PIF (Public Investment Fund)	The sovereign wealth fund of Saudi Arabia, which plays a central role in driving the economic transformation of the Kingdom by making strategic, long-term investments both domestically and internationally.
PMI (Purchasing Managers' Index)	An economic indicator derived from monthly surveys of private sector companies. A reading above 50 indicates an expansion of the manufacturing sector compared to the previous month; below 50 represents a contraction.
Resilience	The ability of an organization to adapt and respond to disruption in a way that protects its stakeholder value, reputation, and brand. It involves an integrated approach to managing risks and opportunities.
SAMA (Saudi Central Bank)	The central bank of Saudi Arabia, responsible for issuing the national currency, supervising commercial banks, and managing foreign exchange reserves. It also sets regulatory frameworks for the financial sector, including for business continuity and cybersecurity.
Saudization (Nitaqat)	A national policy of the Kingdom of Saudi Arabia that requires companies to hire Saudi nationals on a quota basis, aiming to reduce unemployment among Saudi citizens and localize the workforce. ¹
SMEs (Small and Medium Enterprises)	Businesses whose personnel numbers fall below certain limits. In the context of Saudi Arabia, they are a key focus of Vision 2030 for economic diversification and are often more vulnerable to market fluctuations and crises. ¹⁶
Vision 2030	A comprehensive national strategic framework to reduce Saudi Arabia's dependence on oil, diversify its economy, and develop public service sectors such as health, education, infrastructure, recreation, and tourism. ⁹

Executive Summary

The Kingdom of Saudi Arabia's business landscape presents a compelling paradox. On one hand, the national transformation under Vision 2030 has unleashed unprecedented economic dynamism, marked by robust non-oil sector growth, a surge in foreign direct investment, and soaring investor confidence.¹ On the other hand, this hyper-growth has amplified a new generation of complex, interconnected risks, from giga-project delivery challenges to pervasive cyber threats.³ This report analyzes organizational confidence in crisis communication plans within this dual reality, arguing that the most prevalent sentiment is likely to be "Somewhat Confident." This response reflects a widespread "knowing-doing gap," where strategic awareness of risk has outpaced the development of mature, integrated, and culturally-attuned crisis response capabilities.

While national-level resilience frameworks and high investor confidence suggest a mature market, a granular analysis reveals significant vulnerabilities at the corporate level. These include immature risk management practices that struggle to keep pace with the speed of change, cultural barriers such as departmental silos and hierarchical communication styles that impede transparency, a critical shortage of skilled resilience professionals, and a systemic underestimation of novel cyber and supply chain threats.⁵ Ultimately, achieving genuine crisis resilience in the Saudi market requires a strategic evolution beyond mere compliance. It demands an integrated approach that prioritizes human capital development, sophisticated technological integration, and a commitment to authentic, transparent stakeholder engagement.

The Dual Realities of the Saudi Business Landscape: Unprecedented Growth and Amplified Risk

To understand crisis preparedness in Saudi Arabia is to first grasp the twin forces shaping its modern economy: a period of historic opportunity driven by a visionary national agenda, and the emergence of a risk environment as ambitious and complex as the vision itself. For any strategist, recognizing that these two realities are inextricably linked is paramount. In the Kingdom today, effective crisis management is not a peripheral function but a core strategic imperative for both survival and success.

The Engine of Transformation: Vision 2030 and Economic Diversification

The primary catalyst for all economic activity and reform in the Kingdom is Vision 2030, a comprehensive national blueprint built on three foundational pillars: creating a Vibrant Society, fostering a Thriving Economy, and building an Ambitious Nation.⁹ This strategy has successfully ignited the non-oil economy, which is forecast to grow by 4.4% in 2025, significantly outpacing the overall GDP growth projections of around 3.3%.¹ This momentum is vividly illustrated by the Kingdom's Purchasing Managers' Index (PMI), which in January reached 60.5, its highest level in a decade and a strong signal of expansion.¹

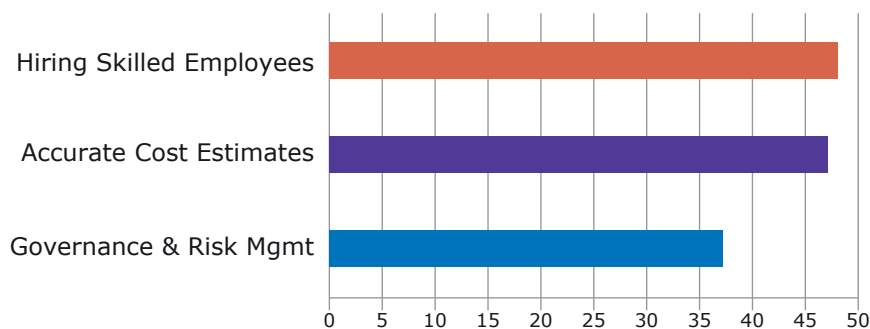
This robust domestic activity has captured global attention, leading to a surge in Foreign Direct Investment (FDI). In the first quarter of 2025 alone, net FDI inflows reached SAR 22.2 billion, a 44% year-on-year increase, demonstrating powerful international investor confidence in the Kingdom's trajectory.² This confidence is further solidified by the formidable brand strength of the Public Investment Fund (PIF), now ranked as the world's most valuable sovereign wealth fund brand, and positive macroeconomic assessments from the International Monetary Fund (IMF), which has praised the Kingdom's economic resilience and containment of inflation.¹¹ This influx of capital is actively encouraged by continuous reforms to improve the ease of doing business, including allowing 100% foreign ownership in numerous sectors.⁹

The Inevitable Consequence: A New Generation of Interconnected Risks

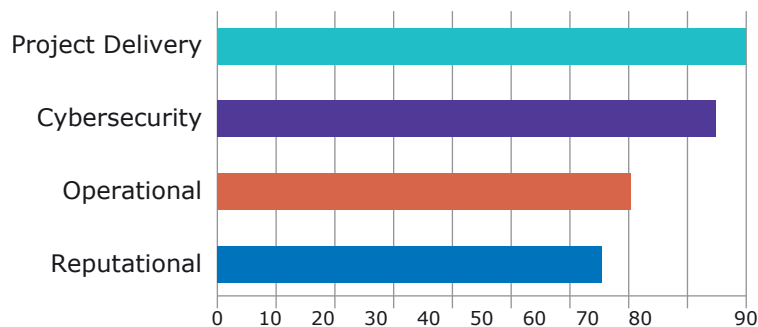
Anatomy of Risk

The consequences of the Kingdom's rapid transformation manifest in specific, high-stakes business risks that demand strategic attention.

Top 3 Giga-Project Delivery Challenges



Top-Tier Business Risks



The sheer velocity and scale of this transformation inevitably generate a new and more challenging risk landscape. The ambition of Vision 2030 is matched only by the complexity of the risks it produces.

- **Giga-Project Complexity:** The development of giga-projects like NEOM and the Red Sea Project involves unprecedented scale, concentrating materials, skills, and technology in ways that magnify risk.¹³ A 2022 PwC survey identified the top three challenges in delivering these projects as hiring and retaining high-skilled employees (cited by 48% of respondents), developing accurate cost estimates (47%), and creating suitable governance and risk management processes (37%).³ The historically adversarial nature of the Saudi construction market, characterized by issues like delayed payments and design-centric failures, creates what one analysis calls a “toxic incubator” for major delays, cost overruns, and disputes.¹⁴
- **Digital Transformation and Cyber Vulnerability:** The national mandate for digital transformation and the development of smart cities has dramatically expanded the potential attack surface for cyber threats.¹⁵ This is not a theoretical risk; recent research indicates that 72% of organizations in Saudi Arabia expect business disruptions from cyber incidents within the next two years.⁴ The most acute threats include sophisticated ransomware campaigns, attacks targeting vulnerabilities in the software supply chain, and security gaps in cloud infrastructure, which is being rapidly adopted across the Kingdom.¹⁶
- **Operational Strain of Rapid Growth:** The intense pace of change places immense strain on internal corporate systems. This manifests as operational risks arising from human error, the failure of legacy systems, and inadequate internal procedures.¹⁹ Many companies find their traditional risk management frameworks are insufficient for this new environment and are struggling to implement more holistic Enterprise Risk Management (ERM) systems that can keep pace with the business.¹⁷
- **Human Capital and Regulatory Hurdles:** Despite significant reforms, navigating the Saudi business environment remains complex. Foreign and local companies alike face challenges related to bureaucracy, evolving Saudization policies that mandate workforce localization, and the need to adapt to local laws and cultural customs.¹²

This dynamic creates a “Preparedness Paradox.” The powerful macro-level narrative of stability, driven by strong government initiatives and high FDI, can foster a sense of security among executives and investors. This confidence, however, may not be reflective of the significant, unmanaged operational risks at the firm level. A strategist must look beyond headline growth figures to question the underlying resilience of the organizations driving that growth.

The risks are not random events but are the direct byproducts of Vision 2030's ambition. Every major opportunity has a corresponding, equally large risk. Therefore, crisis preparedness is not about preventing unforeseen events, but about managing the predictable consequences of the strategic path the entire country is on.

Table 1: The Saudi Business Environment at a Glance (2025)

Macroeconomic Indicators	Foreign Direct Investment (FDI)	Vision 2030 Strategic Goals	Top-Tier Business Risks
Non-Oil GDP Growth: 4.4% ¹	Q1 2025 Net Inflow: SAR 22.2B (+44% YoY) ²	Private Sector GDP Share Target: 65% ⁹	Project Delivery: Skills shortage, cost overruns, supply chain limitations ³
Overall GDP Growth: ~3.3% ¹	Vision 2030 Target: 5.7% of GDP ⁹	Women in Workforce Target: 30% ⁹	Cybersecurity: Ransomware, supply chain attacks, cloud gaps ⁴
Purchasing Managers' Index (PMI): 60.5 (10-year high) ¹		Unemployment Target: 7% ⁹	Operational & Regulatory: Bureaucracy, Saudization compliance, cultural adaptation ¹²
Inflation: Contained at ~2% ⁷			Reputational: Social media missteps, public relations crises ²³

Answering the Poll:

A Multi-Faceted Analysis of Confidence in Crisis Communication

The level of confidence an organization in Saudi Arabia has in its crisis communication plan is a direct reflection of its maturity, regulatory environment, and cultural realities. No single answer will be universal, but by analyzing the specific drivers behind each potential response, a clear picture of the market's overall state of preparedness emerges. The most likely dominant answer is "Somewhat Confident," indicating a market that is aspiring to resilience but has not yet fully bridged the gap between intent and capability.

If the Dominant Answer is "Very Confident": The Preparedness Paradox

A "Very Confident" response would likely be concentrated among large, well-resourced corporations in highly regulated sectors such as finance, energy, and insurance, as well as government-related entities.²⁵ Their confidence is not misplaced but is built on a specific set of foundations.

Drivers of Confidence:

Their high confidence stems primarily from regulatory compulsion. Bodies like the Saudi Central Bank (SAMA), the National Cybersecurity Authority (NCA), and the Digital Government Authority (DGA) have issued comprehensive and mandatory frameworks for Business Continuity Management (BCM) and cybersecurity.¹⁵ These organizations have invested in plans, policies, and technology because they are legally required to do so. This confidence is further bolstered by a "halo effect" of national resilience; a strong belief in the government's proven ability to manage macro-crises, as seen during the COVID-19 pandemic, and the immense financial strength of state actors like the PIF creates a perception of a secure operating environment.¹¹ Finally, these entities have often made significant capital investments in modern crisis management tools, including cloud-based emergency communication systems and real-time monitoring dashboards.²⁹

Hidden Vulnerabilities & Blind Spots:

This confidence, however, may mask critical vulnerabilities. The most significant is the gap between compliance and true capability. Having a plan on paper is not the same as having a battle-tested, proven ability to execute it under stress. A telling study of Jeddah hospitals revealed that while all 13 facilities had a formal disaster plan, none had conducted an unannounced drill in the previous year.³⁰ Their confidence was based on the existence of the plan, not its verified efficacy.

Furthermore, Saudi Arabia's hierarchical business culture can create a dangerous disconnect.³¹ Senior leadership may see a completed plan and assume preparedness, while operational teams are aware of flaws that are not communicated upwards due to a cultural reluctance to deliver bad news or challenge authority.³³ Lastly, their plans, while robust for traditional risks like fires or floods, may be inadequate for novel threats. The speed of digital transformation means that many plans have not been tested against complex scenarios like a sophisticated AI-powered cyberattack or a catastrophic mega-project supply chain failure.³

If the Dominant Answer is “Somewhat Confident”:

The Aspirational Gap

This is the most probable dominant response, representing the broad middle of the Saudi market. This group includes a mix of large private sector companies, multinational corporations adapting to local norms, and ambitious, fast-growing Saudi firms across sectors like logistics, manufacturing, and retail.

Drivers of Sentiment:

Their sentiment is defined by an awareness of risk without a mastery of the response. These organizations have moved beyond inaction; they have a basic plan, a designated crisis team, and some established protocols.⁸ This foundational work prevents them from feeling “Not Very Confident.” However, their lack of full confidence stems from the “knowing-doing gap”—a clear-eyed recognition that their aspirations for resilience are ahead of their current operational reality. A PwC survey highlights this gap: while 33% of Middle East firms report a “fully integrated” resilience program (ahead of the 21% global average), this still means two-thirds of organizations have not achieved this level of maturity.²⁶ They are acutely aware of the persistent challenges in hiring skilled resilience professionals and dedicating sufficient budget and time to large-scale training and simulation exercises.³

Hidden Vulnerabilities & Blind Spots:

The primary vulnerability for this group is the “silo effect.” Crisis plans are often developed independently by different departments—IT, HR, Operations, Communications—and are not holistically integrated.⁶ In a real crisis, this can lead to the operational response being disconnected from the communication strategy, resulting in conflicting actions and messages. This is exacerbated by cultural inertia; the Saudi business culture, which emphasizes relationships and indirect communication, can inhibit the direct, cross-functional collaboration required to break down these silos.³³ Finally, their plans are often static documents, created at a single point in time. In the hyper-dynamic Saudi environment, these plans quickly become outdated, failing to account for new risks emerging from the company’s own rapid growth and digital transformation.¹⁷

If the Dominant Answer is “Not Very Confident”:

The Overwhelmed Realists

This sentiment would be most common among Small and Medium Enterprises (SMEs) and companies operating in highly volatile and less-regulated sectors, such as construction and parts of the logistics and supply chain ecosystem.

Drivers of Sentiment:

Their lack of confidence is a pragmatic assessment of their situation. SMEs are traditionally considered higher-risk ventures and possess limited resources—capital, time, and specialized expertise—to dedicate to non-core functions like comprehensive crisis planning.³⁹ They are also on the front lines of the Kingdom’s most acute risks. They are prime targets for cyberattacks but often lack adequate defenses; they are directly exposed to supply chain disruptions and cash flow volatility from delayed payments; and they must navigate the often-adversarial dynamics of industries like construction.¹⁴ Their lack of confidence is an honest acknowledgment that their posture is, by necessity, reactive rather than proactive, lacking the foresight and planning capabilities of larger firms.⁴³

Hidden Vulnerabilities & Blind Spots:

The greatest vulnerability for this group is dependency. An SME’s survival can hinge on a single large client or government contract. A crisis for that client—or even just a significant payment delay, a known issue in the market—can trigger an existential crisis for the SME.¹⁴ They also lack the regulatory leverage and in-house legal expertise of larger firms, leaving them vulnerable to complex legal disputes and sudden shifts in regulations that they are ill-equipped to handle.²¹

If the Dominant Answer is “Unsure”: The Ambiguity of a Transforming Market

An “Unsure” response is a clear symptom of organizational dysfunction and can be found across companies of all sizes, but it is particularly indicative of those with weak internal communication, deep departmental silos, or those undergoing major restructuring.

Drivers of Sentiment:

This response signals a fundamental lack of transparency and a fragmented corporate culture. Employees and even mid-level managers genuinely do not know if a comprehensive, integrated plan exists or who is responsible for it.⁶ In a strictly hierarchical culture, crisis planning can be an exclusively C-suite activity that is never effectively communicated or cascaded down to the teams who would be responsible for execution.³¹ This disconnect is compounded by low employee engagement. A significant portion of the workforce in the region remains disengaged, and these employees are unlikely to be aware of or involved in strategic initiatives like crisis planning.⁴⁴ Studies on HR adaptations during the COVID-19 pandemic found that “enhanced communication” was a key strategy to boost engagement, implying it was a pre-existing weakness.⁴⁶

Hidden Vulnerabilities & Blind Spots:

An “Unsure” response is the clearest indicator of an absent enterprise-wide risk culture. There is no shared understanding of threats and no collective ownership of the response. This creates a critical “single point of failure” risk. If knowledge of the crisis plan resides only with a handful of senior leaders, the organization is profoundly vulnerable should those individuals be unavailable or incapacitated during an emergency.

Table 2: Comparative Analysis of Crisis Preparedness Confidence Levels

Confidence Level	Likely Organizational Profile	Key Drivers of Sentiment	Underlying Assumption	Hidden Vulnerabilities / Blind Spots
Very Confident	Large, regulated entities (Finance, Energy); Government-related bodies	Regulatory compulsion; Belief in national resilience; High-tech investments	"Our compliance with mandates equals true capability."	Untested plans; Hierarchical disconnect; Underestimation of novel threats
Somewhat Confident	Growing private sector; Multinational corporations	Awareness of risks; Partial planning and resource allocation	"Our current plan is good enough for now and we will improve it later."	Departmental silos; Static plans in a dynamic environment; Cultural inertia
Not Very Confident	Small & Medium Enterprises (SMEs); Construction; Supply chain firms	Severe resource constraints; Overwhelming and direct threat exposure	"We are too small, busy, or resource-poor to plan effectively."	Reactive posture; High dependency on single clients; Lack of regulatory leverage
Unsure	Organizations with poor internal communication; Deep silos; Low employee engagement	Organizational opacity; Lack of information flow; Employee disengagement	"Someone else is probably handling it."	Absence of a unified risk culture; Critical knowledge held by only a few leaders

Strategic Imperatives for Building Crisis Resilience in the Saudi Market

For strategists operating in Saudi Arabia, moving an organization up the confidence spectrum—from “Unsure” or “Not Very Confident” to a robust and realistic state of preparedness—requires more than just drafting a document. It demands a deliberate, integrated, and culturally intelligent approach. The following imperatives provide a roadmap for transforming crisis management from a reactive necessity into a source of enduring competitive advantage.

From Compliance to Competitive Advantage: Integrating Crisis Management with Strategy

The most mature organizations view crisis readiness not as a cost center or a compliance burden, but as a strategic enabler that protects brand value, strengthens investor confidence, and creates a distinct competitive advantage.²⁶ In a market where global investors are actively seeking resilient partners, a demonstrable ability to navigate disruption is a powerful differentiator.⁴⁸

The necessary action is to embed the crisis management program within the organization’s core strategy. Investments in resilience should be framed not as expenses, but as measures to protect the massive growth opportunities presented by Vision 2030. When seeking FDI or bidding on major projects, a company’s robust and tested resilience posture can be a key selling point, signaling reliability and long-term viability to partners and stakeholders.⁵⁰

Bridging the Cultural-Operational Divide: Creating a Bicultural Resilience Framework

A crisis plan designed in a Western corporate headquarters and implemented without adaptation in Riyadh is likely to fail. Global best practices are essential, but they must be translated to fit the Saudi cultural context to be effective.⁵¹ A successful framework must navigate the realities of hierarchy, indirect communication, and relationship-based business practices to foster the necessary transparency and collaboration.³¹

Actionable steps include designing communication protocols that respect hierarchical structures but also create officially sanctioned channels for bottom-up risk reporting, empowering employees to raise concerns without fear of reprisal. Implementing intensive, cross-functional crisis simulation exercises is one of the most effective ways to physically break down departmental silos and build the “one team” mentality needed for a coordinated response.⁶ Critically, senior leadership must visibly champion and model a “no-blame” approach to risk identification, actively countering the “saving face” culture that often conceals vulnerabilities until it is too late.²⁷

Investing in Human and Technological Capital:

The Twin Pillars of Modern Resilience

The Saudi market faces the dual challenges of a significant skills shortage in specialized fields like risk management and a rapidly evolving technological threat landscape.³ Addressing this requires a parallel investment in both people and systems.

On the human capital front, organizations must focus on developing in-house talent. This can be achieved through dedicated training programs, leveraging excellent available resources like the Business Continuity Institute’s (BCI) Good Practice Guidelines, which are now available in Arabic.⁸ The goal is to build a multi-disciplinary team with the right skills to manage an integrated program, not just a siloed one.²⁶ HR departments have a crucial role to play, not only in recruitment but in fostering a resilient culture through employee engagement and clear communication.⁴⁶

On the technological front, investment in modern crisis management platforms is essential. These are typically cloud-based systems that offer multi-channel mass notifications (SMS, email, app alerts), real-time incident dashboards, and automated response workflows.²³ For organizations in the Kingdom, it is critical to ensure these systems comply with Saudi data sovereignty regulations, which often require local data hosting.²³

Proactive and Authentic Stakeholder Engagement:

The Core of Crisis Communication

In any crisis, trust is the ultimate currency.⁴⁷ An effective communication plan is built on a foundation of transparency, timeliness, and empathy, using the right channels to reach the right audiences. This requires significant preparatory work.

Organizations should develop a suite of pre-approved, culturally sensitive communication templates for various potential scenarios.⁵¹ Mastering the use of social media is non-negotiable, both for disseminating real-time updates and for actively countering the misinformation and rumors that can rapidly poison the information environment during a crisis—a key challenge identified in the region.²⁴ Research from the COVID-19 pandemic in Saudi Arabia shows that messages focusing on warnings, uncertainty reduction, and reassurance generate the highest levels of public engagement.⁵⁴ Communication plans must also be multi-lingual (primarily Arabic and English) to effectively address the diverse mix of employees, customers, partners, and regulators in the Kingdom.³⁸

Table 3: Strategic Roadmap for Enhancing Crisis Resilience

01 Integrate with Strategy

Action: Link resilience to Vision 2030 goals and use it as a competitive differentiator.

Tech: ERM software, BI dashboards.

02 Bridge Cultural Divide

Action: Run cross-functional simulations and create safe channels for risk reporting.

Tech: Cloud-based collaboration platforms, anonymous reporting tools.

03 Invest in Capital

Action: Develop in-house talent and implement modern crisis communication platforms.

Tech: E-learning, Employee engagement platforms, mass notification systems

04 Engage Stakeholders

Action: Develop multi-lingual templates and master social media monitoring.

Tech: Social listening tools, multi-channel notification platforms with two-way communication.

Strategic Imperative	Key Actions	Technological Enablers	KSA-Specific Cultural Considerations
1. Integrate with Strategy	Link resilience program directly to Vision 2030 goals; Develop ROI-based investment cases for preparedness initiatives; Use resilience as a competitive differentiator.	Enterprise Risk Management (ERM) software; Business intelligence dashboards.	Frame value to hierarchical leaders in terms of national contribution and protecting high-profile projects.
2. Bridge Cultural-Operational Divide	Conduct intensive, cross-functional crisis simulations; Establish sanctioned "safe" channels for bottom-up risk reporting; Mandate senior leadership involvement.	Cloud-based collaboration platforms; Anonymous reporting tools.	Leadership must visibly champion a "no-blame" culture to overcome the reluctance to share bad news ("saving face").
3. Invest in Human & Tech Capital	Develop in-house talent via training (e.g., BCI's Arabic GPGs); Implement a modern, multi-channel crisis communication platform; Empower HR to drive engagement.	E-learning modules; Mass notification systems; Employee engagement platforms.	Frame training as prestigious professional development to appeal to a culture where status and certification are valued.
4. Proactive Stakeholder Engagement	Develop pre-approved, multi-lingual communication templates; Implement social media monitoring and response protocols; Engage employees as crisis ambassadors.	Social listening tools; Multi-channel notification platforms with two-way communication.	Utilize religious and collectivist framing in reassurance messaging, a proven strategy from the COVID-19 response. ²⁷

CONCLUSION

Conclusion

In the high-growth, high-risk environment of modern Saudi Arabia, an organization's confidence in its crisis communication plan serves as a direct proxy for its strategic maturity and long-term viability. The landscape is not uniform; confidence levels vary predictably based on an organization's size, sector, and proximity to regulatory oversight. While highly regulated entities may feel "Very Confident" based on their compliance-driven plans, the bulk of the market likely resides in a state of being "Somewhat Confident." This reflects a market in a critical state of transition, aware of the escalating risks but still working to close the gap between planning and practice.

For strategists, the path to true resilience is clear. It requires moving beyond the siloed, static plans of the past toward a future defined by an integrated, dynamic, and culturally-aware approach. The ultimate goal is to transform crisis management from a reactive, compliance-focused necessity into a proactive source of strategic strength—one that not only protects the organization in times of turmoil but also enhances its reputation and secures its position as a trusted and resilient partner in the unfolding story of Vision 2030.

REFERENCES

References:

1. Saudi Arabia's economic diversification to drive robust growth in ..., accessed July 29, 2025, <https://www.arabnews.com/node/2591308/business-economy>
2. Foreign Investment in Saudi Arabia Surges in 2025 | Peninsula, accessed July 29, 2025, <https://www.peninsulacs.com/post/foreign-investment-saudi-arabia-q1-2025>
3. Confidence in Saudi giga-projects is rising and so are its challenges, accessed July 29, 2025, <https://www.pwc.com/m1/en/media-centre/articles/confidence-in-saudi-giga-projects-is-rising.html>
4. Future Master News Analysis Cybersecurity Preparedness Remains Low in Saudi Arabia, accessed July 29, 2025, <https://futuremaster.net/cybersecurity-preparedness-remains-low-in-saudi-arabia-2/>
5. Exploring the uptake of business continuity in Saudi Arabia | BCI, accessed July 29, 2025, <https://www.thebci.org/news/exploring-the-up-take-of-business-continuity-in-saudi-arabia.html>
6. How to Break Down Silos in Your Organization | Together Mentoring Software, accessed July 29, 2025, <https://www.togetherplatform.com/blog/how-to-break-down-silos-in-your-organization>
7. Saudi economy proves resilient to global shocks: IMF, accessed July 29, 2025, <https://www.argaam.com/en/article/articledetail/id/1823853>
8. Challenges and opportunities in resilience: The case of Saudi ..., accessed July 29, 2025, <https://www.thebci.org/news/challenges-and-opportunities-in-resilience-the-case-of-saudi-arabia.html>
9. Saudi Arabia's Vision 2030: Five years left, how much progress has ..., accessed July 29, 2025, <https://timesofindia.indiatimes.com/world/middle-east/saudi-arabias-vision-2030-five-years-left-how-much-progress-has-been-made-and-will-it-succeed/articleshow/122861726.cms>
10. Saudi Arabia's FDI reaches SAR 22.2B in Q1 2025, accessed July 29, 2025, <https://www.argaam.com/en/article/articledetail/id/1824200>
11. Saudi Arabia's PIF named most valuable and fastest-growing ..., accessed July 29, 2025, <https://timesofindia.indiatimes.com/world/middle-east/saudi-arabias-pif-named-most-valuable-and-fastest-growing-sovereign-wealth-fund-brand-in-2025/articleshow/122956176.cms>
12. Doing Business in Saudi Arabia: 2025 Guide - J K Management Consultancies, accessed July 29, 2025, <https://jkmanagement.ae/doing-business-in-saudi-arabia-2025-guide/>

- 13.** How Saudi Arabia's Giga Projects Are Attracting US Partnerships, accessed July 29, 2025, <https://www.us-saudi-business.org/how-saudi-arabia-giga-projects-are-attracting-us-partnerships/>
- 14.** Can the Kingdom's Vision 2030 Giga Projects afford not to take a collaborative approach?, accessed July 29, 2025, <https://www.hka.com/article/kingdoms-vision-2030-giga-projects-collaborative-approach-hka/>
- 15.** Saudi Arabia's Path to Resilience: The Role of Vision 2030, accessed July 29, 2025, <https://www.thebci.org/news/saudi-arabia-s-path-to-resilience-the-role-of-vision-2030.html>
- 16.** Top Cybersecurity Threats 2025 - Cybersecurity Saudi Arabia, accessed July 29, 2025, <https://itbutler.sa/blog/top-10-cybersecurity-threats-for-saudi-businesses-in-2025/>
- 17.** KSA Tech Transformation & The Need For ERM | Grant Thornton, accessed July 29, 2025, https://www.grantthornton.sa/en/insights/articles-and-publications/KSA_Tech_Transformation_The_Need_For_ERM/
- 18.** Saudi's industrial sector increasingly vulnerable to cyber attacks - Consultancy-me.com, accessed July 29, 2025, <https://www.consultancy-me.com/news/4394/saudis-industrial-sector-increasingly-vulnerable-to-cyber-attacks>
- 19.** Risk Management in Saudi Arabia: Effective Strategies and Tools - Eyad Reda Law Firm, accessed July 29, 2025, <https://erlf.com/publications/risk-management/>
- 20.** [Withdrawn] Overseas business risk: Saudi Arabia - GOV.UK, accessed July 29, 2025, <https://www.gov.uk/government/publications/overseas-business-risk-saudi-arabia/overseas-business-risk-saudi-arabia>
- 21.** Legal Risks to Business Owners in Saudi Arabia - AHYSP Law Firm, accessed July 29, 2025, <https://ahysp.com/legal-risks-to-business-owners-in-saudi-arabia/>
- 22.** Saudi Arabia: Country File, Economic Risk Analysis | Coface, accessed July 29, 2025, <https://www.coface.com/news-economy-and-insights/business-risk-dashboard/country-risk-files/saudi-arabia>
- 23.** Crisis Management Saudi Arabia: Leverage Mass Notification - Crises Control, accessed July 29, 2025, <https://www.crisis-control.com/blogs/crisis-management-saudi-arabia/>
- 24.** The use of social media for crisis communication during the COVID-19 pandemic: The case of Lebanon - Cairn, accessed July 29, 2025, <https://shs.cairn.info/revue-projectique-2023-1-page-11?lang=fr>

- 25.** Cyber Security Framework Saudi Arabian Monetary Authority, accessed July 29, 2025, <https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Cyber%20Security%20Framework.pdf>
- 26.** PwC Middle East Crisis and Resilience Survey 2023, accessed July 29, 2025, <https://www.pwc.com/m1/en/publications/middle-east-crisis-and-resilience-survey-2023.html>
- 27.** Narratives of Crisis: Female Saudi Students and the Covid-19 Pandemic - PMC, accessed July 29, 2025, <https://pmc.ncbi.nlm.nih.gov/articles/PMC9638505/>
- 28.** The impact of crisis and disasters risk management in COVID-19 ..., accessed July 29, 2025, <https://pmc.ncbi.nlm.nih.gov/articles/PMC9765402/>
- 29.** Emergency Communication System for Saudi Arabia - Crises Control, accessed July 29, 2025, <https://www.crisis-control.com/blogs/emergency-communication-system-saudi/>
- 30.** Evaluation of disaster preparedness for mass casualty incidents in private hospitals in Central Saudi Arabia - PMC - PubMed Central, accessed July 29, 2025, <https://pmc.ncbi.nlm.nih.gov/articles/PMC5387908/>
- 31.** A Guide to Business Etiquette in Saudi Arabia - CIBT Visas, accessed July 29, 2025, <https://cibtvisas.com/blog/business-etiquette-saudi-arabia>
- 32.** Saudi Arabia - Culture, Etiquette and Business Practices, accessed July 29, 2025, <https://www.commisceo-global.com/resources/country-guides/saudi-arabia-guide>
- 33.** Saudi Arabian Communication Styles | World Business Culture, accessed July 29, 2025, <https://www.worldbusinessculture.com/country-profiles/saudi-arabia/business-communication-style/>
- 34.** 5 Most Common Gaps in Crisis Management That Could Cripple ..., accessed July 29, 2025, <https://www.earlyalert.com/5-most-common-gaps-in-crisis-management/>
- 35.** Giga-projects in the Middle East: How to manage risk effectively - HKA, accessed July 29, 2025, <https://www.hka.com/article/giga-projects-in-the-middle-east-how-to-manage-risk-hka/>
- 36.** Breaking Silos with AI: How Multi-Agent Systems Are Powering UAE's Digital Economy, accessed July 29, 2025, <https://medium.com/@wdcsuae/breaking-silos-with-ai-how-multi-agent-systems-are-powering-uaes-digital-economy-3c998578ca64>

- 37.** What Are Data Silos? Why Are They Problematic? | Oracle Middle East Regional, accessed July 29, 2025, <https://www.oracle.com/middle-east/database/data-silos/>
- 38.** Business culture in Saudi Arabia - myNZTE, accessed July 29, 2025, <https://my.nzte.govt.nz/article/business-culture-in-saudi-arabia>
- 39.** Consequences of COVID-19 Shocks and Government Initiatives on Business Performance of Micro, Small and Medium Enterprises in Saudi Arabia, accessed July 29, 2025, <https://jsbs.scholasticahq.com/article/87568-consequences-of-covid-19-shocks-and-government-initiatives-on-business-performance-of-micro-small-and-medium-enterprises-in-saudi-arabia>
- 40.** De-Risking SME Investment in Saudi Arabia: A Strategic Shift Towards Economic Maturity, accessed July 29, 2025, <https://www.sbjbc.org/de-risking-sme-investment-in-saudi-arabia-a-strategic-shift-towards-economic-maturity/>
- 41.** Doing Business in Saudi Arabia: Challenges, Risks, & Culture - Horizons, accessed July 29, 2025, <https://joinhorizons.com/doing-business-in-saudi-arabia/>
- 42.** 7 SMB Cybersecurity Statistics for 2025 - NinjaOne, accessed July 29, 2025, <https://www.ninjaone.com/blog/smb-cybersecurity-statistics/>
- 43.** The effectiveness of crisis management in encouraging technical innovation among medium and small companies in the Kingdom of Saudi Arabia, accessed July 29, 2025, https://www.eimj.org/uplode/images/photo/The_effectiveness_of_crisis_management_in_encouraging_technical_innovation..pdf
- 44.** Rising Employee Engagement In Saudi Arabia: Decreasing ..., accessed July 29, 2025, <https://www.prnewswire.com/ae/news-releases/rising-employee-engagement-in-saudi-arabia-decreasing-work-place-stress-and-growing-job-market-optimism-302165596.html>
- 45.** Why Middle East companies must tackle the employee engagement crisis in 2025, accessed July 29, 2025, <https://fastcompany.me.com/work-life/why-middle-east-companies-must-tackle-the-employee-engagement-crisis-in-2025/>
- 46.** Adapting human resources management to global health crises ..., accessed July 29, 2025, <https://www.emerald.com/insight/content/doi/10.1108/agjsr-10-2023-0488/full/html>
- 47.** Campaign Middle East-Saudi Arabia Report 2025 by Motivate Media Group - Issuu, accessed July 29, 2025, https://issuu.com/motivatepublishing/docs/campaign_middle_east-saudi_arabia_report_2025

- 48.** Saudi Arabia's transformation boosts investor confidence - Arab News, accessed July 29, 2025, <https://www.arabnews.com/node/2605686/corporate-and-sponsored-content>
- 49.** Saudi Arabia's transformation boosts investor confidence - Arab News PK, accessed July 29, 2025, <https://www.arabnews.pk/node/2605686/corporate-and-sponsored-content>
- 50.** Capital with Intention: Charting UNDP's Path Toward Impact Investment in Saudi Arabia, accessed July 29, 2025, <https://www.undp.org/saudi-arabia/press-releases/capital-intention-charting-undps-path-toward-impact-investment-saudi-arabia>
- 51.** Crisis Management Strategies for the Modern Middle East, accessed July 29, 2025, <https://www.crisis-control.com/blogs/crisis-management-strategies-2/>
- 52.** Crisis Preparedness and Response: The Vital Role of Risk Advisors in Saudi Businesses, accessed July 29, 2025, <https://insightss.co/blogs/the-vital-role-of-risk-advisors-in-saudi-businesses/>
- 53.** (PDF) Transforming Saudi Arabia's workforce: HR management strategies in action, accessed July 29, 2025, https://www.researchgate.net/publication/389696292_Transforming_Saudi_Arabia's_workforce_HR_management_strategies_in_action
- 54.** The Saudi Ministry of Health's Twitter Communication Strategies and Public Engagement During the COVID-19 Pandemic: Content Analysis Study - PMC, accessed July 29, 2025, <https://pmc.ncbi.nlm.nih.gov/articles/PMC8276783/>
- 55.** Crises information dissemination through social media in the UK ..., accessed July 29, 2025, <https://pmc.ncbi.nlm.nih.gov/articles/PMC10162563/>
- 56.** Public relations via X: A critical study of crisis communication by Saudi government organisations during the Covid-19 pandemic - University of Strathclyde, accessed July 29, 2025, <https://pureportal.strath.ac.uk/en/publications/public-relations-via-x-a-critical-study-of-crisis-communication-b>