protiviti®
Global Business Consulting

ERM Reimagined in the Middle East 2026

From Readiness to Resilience

Protiviti ERM Survey 2026 — Middle East

Face the Future with Confidence®

CONTENTS

This report evaluates the maturity of Enterprise Risk Management (ERM) in the Middle East, five years after the Protiviti ERM Readiness Assessment Survey 2020 - Middle East. Using findings from the Protiviti ERM Survey 2026 - Middle East (the 2026 Survey), with more than 100 responses, and global risk-management research, it highlights areas of ERM progress, identifies less mature capabilities, and outlines key questions for boards and executives to address over the next 12 to 24 months, supported by a practical 90- to 180-day action agenda.

Executive Summary

Five years after our last Middle East ERM Readiness Assessment,* the regional picture has changed materially. Among the larger, governance-led organizations represented in this survey, ERM is now embedded in their governance and operating model. Among surveyed organizations the basic elements are largely present: 91% report a standardized risk-identification process, 88% have aligned ERM objectives with strategy, and 84% confirm that the Chief Risk Officer (CRO) has unrestricted access to the CEO and the Board.

The pivotal issue has shifted from whether ERM exists to how effectively it influences business outcomes. The data shows that while foundational ERM structures are largely established, more sophisticated capabilities continue to be underdeveloped. The pattern is clear on AI: only 29% of organizations have integrated AI into risk processes, 34% have an AI governance framework in place, and just 29% conduct formal AI-specific risk assessments. As a result, most organizations are not adequately managing emerging technological risks. Additionally, only 51% of organizations link executive compensation to risk performance, which suggests that risk accountability has not been fully institutionalized within performance management systems. These figures jointly demonstrate that, although the fundamental elements of ERM are present, many organizations have yet to embed ERM practices that produce measurable impact on strategic decisions and improve organizational resilience.

Structurally, ERM has arrived. In decisions, it has not. ERM is generally excluded from major business decisions such as investments, mergers and acquisitions, strategic changes, and crisis response. While organizations are evolving their ERM practices, many still view ERM primarily as a risk management function rather than as a contributor to strategic decision-making.

Why ERM matters now

The operating environment gives this transition urgency. Geopolitical volatility, market uncertainty and digital supply-chain dependencies are increasing pressure on regional operating models, while cyber, AI and third-party risks are becoming more connected. The World Economic Forum's 2026 Global Cybersecurity Outlook reports that 65% of large organizations identify third-party and supply-chain vulnerabilities as a leading cyber-resilience challenge, while 64% of organizations now assess AI tools for security before deployment.** For Middle East organizations, the implication is clear: ERM must connect geopolitical risk, third-party exposure, cyber resilience, AI governance and business continuity into one enterprise view, rather than treating them as separate risk domains. For Middle East organizations operating under regional Vision programs and a tightening regulatory agenda, these forces make ERM a strategic instrument rather than a compliance formality.

* Protiviti ERM Readiness Assessment Survey 2020 Middle East

** WEF Global Cybersecurity Outlook 2026

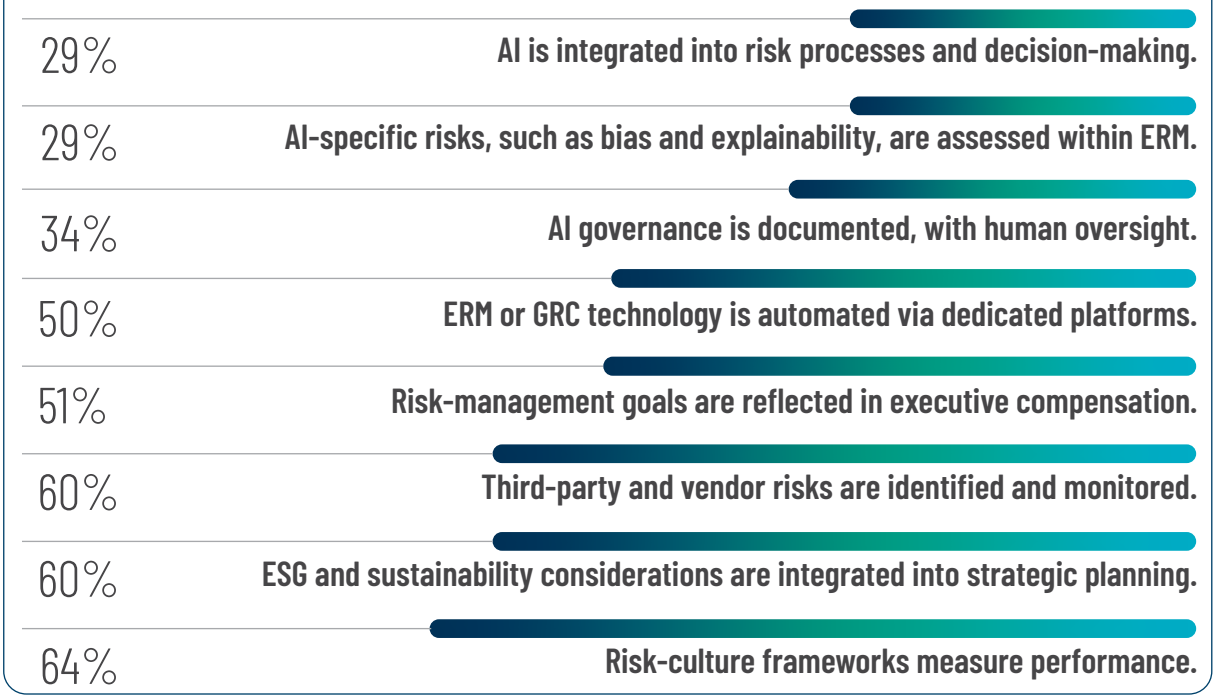
From readiness to resilience: where regional ERM stands today

What the survey shows

The survey results, when considered in light of the respondent profile, reflect the views of more than 100 senior and executive risk stakeholders, with more than half of respondents at the C-suite, senior management, or Board level. The respondent profile is also weighted toward larger and more structured organizations, including government and semi-government entities, listed companies, and large private-sector groups. The findings provide an informed view of how more mature, governance-led organizations in the GCC and wider Middle East see their current ERM capability rather than a broad measure of every organization in the market.

Core ERM strengths reported by respondents include the following

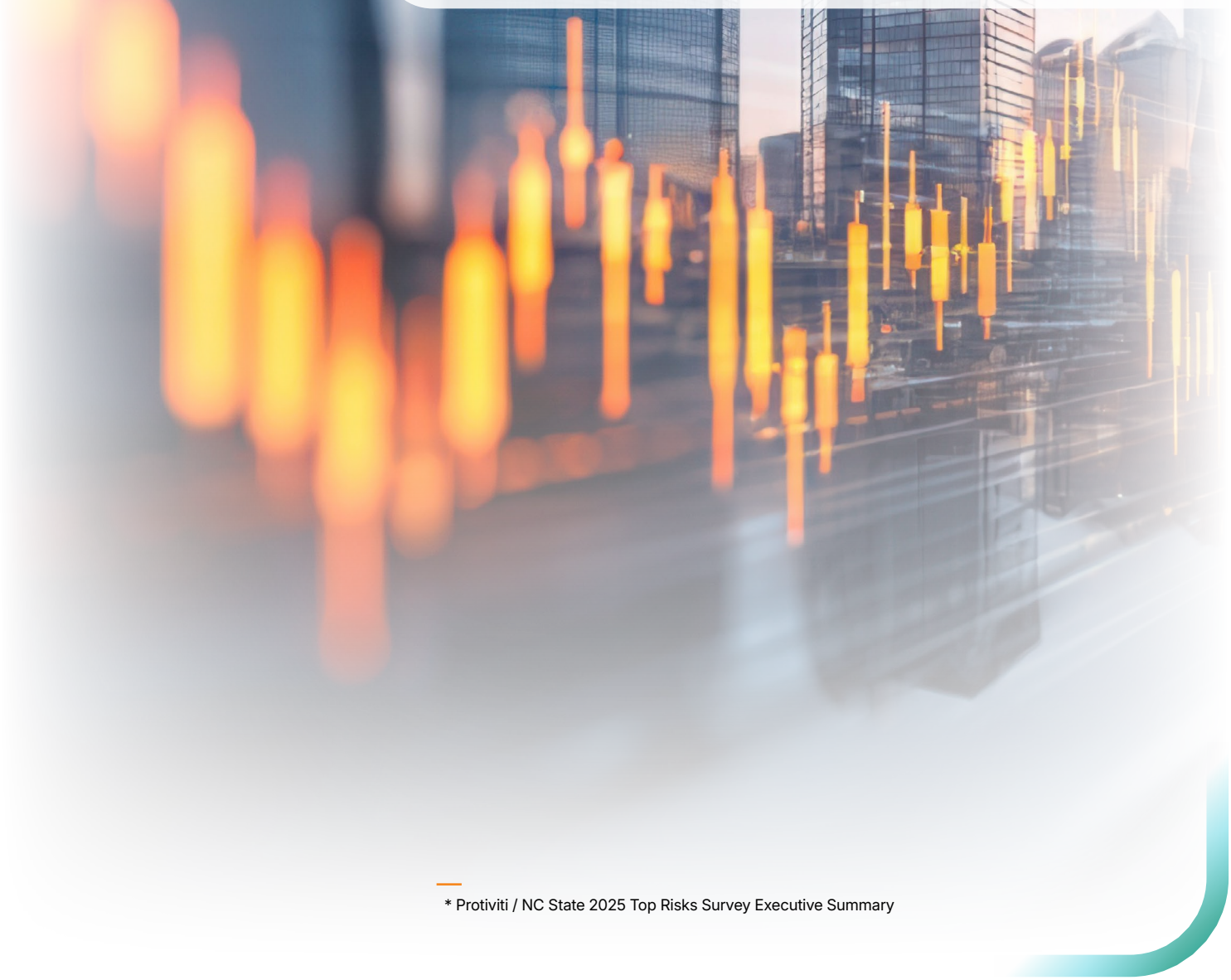
Several next-stage capabilities remain less mature, including:



Combined assurance as the connecting theme

A recurring theme in the findings is the value of combined assurance, which aligns ERM, internal audit, compliance, IT risk, and information security around a shared risk universe and reporting cycle. Currently, ERM coordinates with other assurance functions across the three lines in only 69% of organizations. Strengthening combined assurance is one of the clearest ways to turn existing structures into board-level insights on risks affecting growth, regulatory compliance, and resilience.

The Protiviti and NC State 2025 Top Risks Survey, which gathered the views of more than 1,200 board members and C-suite executives, places financial volatility, cyber risks, third-party risk and the pace of AI adoption among the most important near- and long-term concerns.* The implication is consistent for the organizations surveyed: the foundations are in place, and the task now is to embed ERM in day-to-day decision-making.



* Protiviti / NC State 2025 Top Risks Survey Executive Summary

Where ERM still needs to earn its seat at the table

This survey assessed ERM across seven pillars:

- Strategy and Governance
- Leadership and Accountability
- Data and Technology
- Talent and Capabilities
- Risk Identification and Assessment
- Risk Controls and Mitigation
- Culture and Continuous Improvement

Looking beyond the headline percentages, seven recurring themes emerge as Board and senior-management priorities. These themes explain why ERM in the region is often still positioned as a risk-management function, rather than as a strategic discipline that helps shape major decisions, capital allocation and resilience choices:

STRATEGY

ERM remains largely outside strategic management. Frameworks exist, yet the function is seldom involved in major strategic choices, transformation programs or market-entry decisions.

CAPITAL ALLOCATION

Investment and capital-allocation decisions often proceed with limited ERM involvement. Few investment processes treat risk review as a mandatory step, and most frameworks remain centered on downside risk rather than upside opportunity.

FORESIGHT

Emerging risks are reviewed periodically, but rarely stress-tested. Pandemics, geopolitical conflict, sanctions and energy-market shocks are discussed as history rather than modeled as forward scenarios.

AI, CYBER AND DATA

AI governance is the widest capability gap. Fewer than one in three organizations integrate AI into risk processes or assess AI-specific risks, and cyber, third-party and AI exposure are rarely viewed as one connected risk.

COMBINED ASSURANCE

Day-to-day integration with other assurance functions - internal audit, compliance, IT risk and information security - is still inconsistent. Coordination often exists on paper but not in practice, and third-party oversight sits outside it.

RISK OWNERSHIP

Ownership is assigned but unevenly measured. Risk-and-control self-assessment sits outside second-line stewardship in many organizations, and risk performance is only weakly reflected in reward.

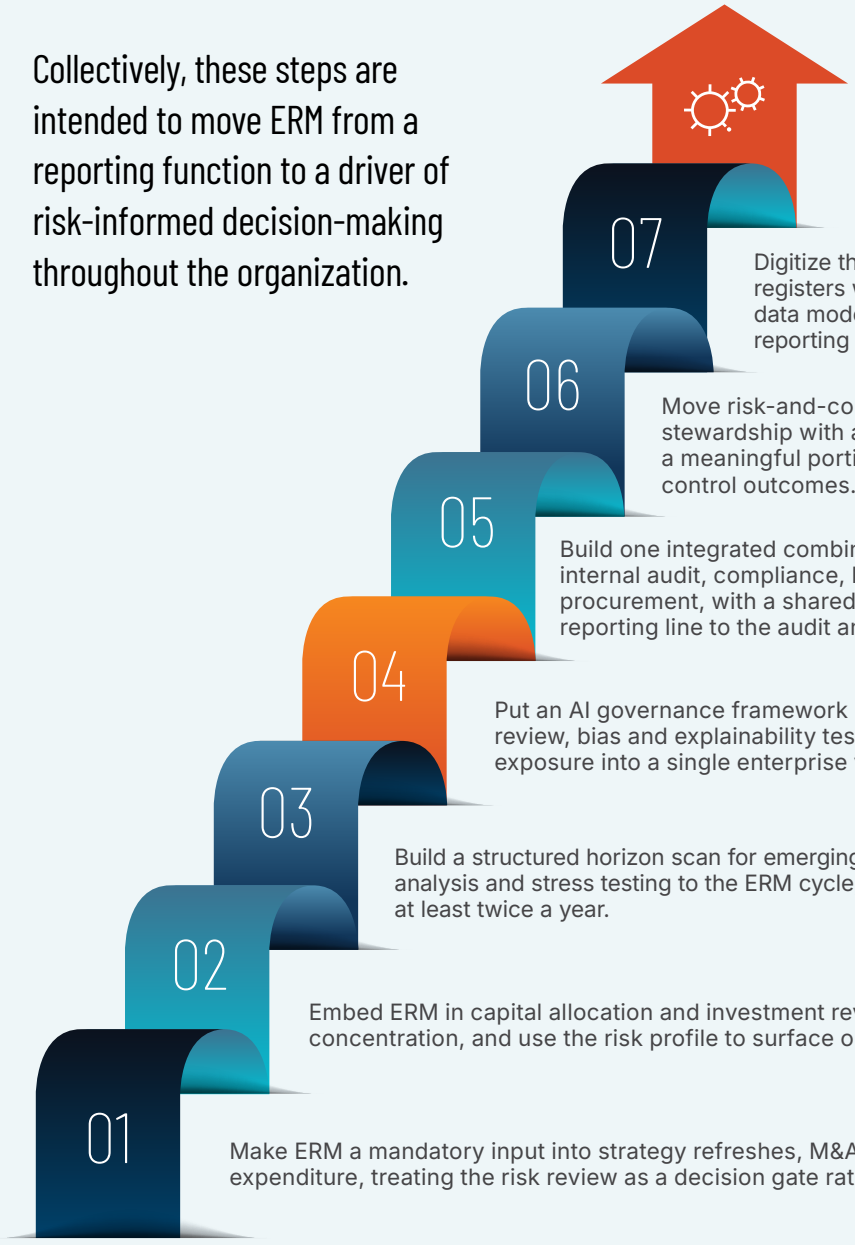
DIGITAL MATURITY

ERM technology remains largely manual. Half of organizations have no dedicated platform for identification, assessment, monitoring and reporting, which limits the speed and consistency of risk information reaching the Board.

Top actions: From a risk register to a risk-driven organization

Together, these seven themes point to seven priority actions for organizations in the region - one for each theme. The closing Call to Action develops them into a practical 90- to 180-day execution agenda with owners and milestones. In summary, organizations should:

Collectively, these steps are intended to move ERM from a reporting function to a driver of risk-informed decision-making throughout the organization.



07 Digitize the risk function, replacing spreadsheet-based registers with a dedicated ERM/GRC platform on a single data model, treated as core infrastructure rather than a reporting convenience.

06 Move risk-and-control self-assessment under second-line stewardship with a single enterprise methodology, and tie a meaningful portion of executive compensation to risk and control outcomes.

05 Build one integrated combined-assurance plan across ERM, internal audit, compliance, IT risk, information security and procurement, with a shared risk universe, calendar and reporting line to the audit and risk committees.

04 Put an AI governance framework in place - AI inventory, pre-deployment review, bias and explainability testing - and connect AI, cyber and third-party exposure into a single enterprise view.

03 Build a structured horizon scan for emerging and black-swan risks, add scenario analysis and stress testing to the ERM cycle, and review both formally with the Board at least twice a year.

02 Embed ERM in capital allocation and investment review, testing assumptions and concentration, and use the risk profile to surface opportunities, not only threats.

01 Make ERM a mandatory input into strategy refreshes, M&A, market entry and major capital expenditure, treating the risk review as a decision gate rather than an approval step.

Introduction

Why ERM in the Middle East is being reimagined

The 2020 baseline as a starting point

Protiviti's ERM Readiness Assessment Survey 2020 Middle East provides a clear reference point for measuring regional progress.* At that time, respondents were grouped into four categories: Initial Adopter, Actionable, Influencer and Leader. Most organizations were still establishing the basics: 44% were at the Initial Adopter stage and a further 35% were Actionable. Their focus was fundamental: defining risk taxonomies, establishing risk committees, setting a risk-appetite statement and appointing accountable owners. Only about 21% had reached the Influencer or Leader stages, where ERM begins to shape strategy and influence capital allocation rather than confirm compliance.

The 2020 study examined six areas: strategy and governance; leadership and accountability; talent and capability; data and technology; risk processes; and culture and continuous improvement. A consistent pattern appeared across all six. Organizations had progressed further on structural elements, such as committees and policies, than on behavioral ones. Progress was slowest in integrating risk into performance incentives and in building a genuinely risk-aware culture.

In short, by 2020 the central question was whether ERM existed. What remained uncertain was whether it was making a notable difference.

The new question: From readiness to resilience

Fast forward to 2026, and that question has changed. The current survey, drawing mainly on senior leaders across the GCC, indicates that many organizations now have the foundations of ERM in place. Risk identification is reported at 91%, 88% link ERM objectives to strategy, and 84% confirm CRO access to the Board. These are no longer points of distinction; they are becoming standard expectations.

The more important issue is what organizations now do with this foundation:

- Is ERM shaping capital allocation and major investment decisions?
- Is the Board's risk appetite reflected in operational measures and executive compensation?
- Has the risk function adapted to rapid shifts - AI adoption, greater reliance on third parties, and tighter regulation, including regional regulatory cybersecurity controls and AI-related directives?
- Has risk culture moved beyond awareness training to influence everyday behavior?

This paper contends that ERM in the Middle East has reached a key stage. The challenge now is to embed ERM more deeply into how the organization operates - integrating it into strategy, automating processes where feasible, addressing AI and third-party risk, aligning ERM with incentives, and reviewing its effect on culture. The sections that follow assess regional performance against these transforming expectations.

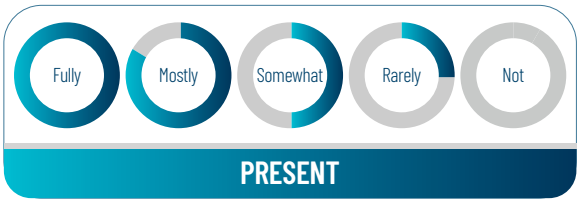
* Protiviti ERM Readiness Assessment Survey 2020 Middle East

Survey Methodology and Respondent Profile

The Protiviti ERM Survey 2026 - Middle East closed in 2026 and gathered over 100 responses from senior and executive risk stakeholders, with most responses from the GCC. While the 2020-21 baseline was organized around six areas, the current survey presents seven pillars by separating risk identification and assessment from risk controls and mitigation, allowing the report to distinguish between risk assessment practices and the actions taken to manage those risks.

Respondents rated how prevalent each ERM practice was in their organization on a five-point scale:

Fully Present, Mostly Present, Somewhat Present, Rarely Present, and Not Present.



For this report, results are presented through a presence lens. Where a practice was rated Fully, Mostly, or Somewhat Present, it is counted as a current presence; where it was rated Rarely Present or Not Present, it represents a development area. This approach gauges whether a practice is present to some degree, but it does not distinguish between early adoption and full institutionalization. This method has inherent limitations. Primarily, high presence scores reflect the existence or nominal adoption of practices but do not provide evidence of depth, consistent application, or active utilization by boards in strategic decision-making. As a result, the data may overstate the actual level of ERM maturity, since presence alone does not confirm that a practice is sufficiently integrated to influence organizational outcomes or boardrooms.

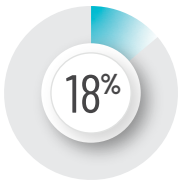
Reading the results in context

Two characteristics of the respondent base shape interpretation. First, the sample is senior: 54% of respondents sit in C-suite, senior-management or Board roles, so the findings reflect a leadership view of ERM maturity. Second, the sample is weighted toward larger organizations: 65% report more than 500 employees and 85% report an ERM program already in place. High presence scores, such as 88%, should therefore be read as the position of organizations with wide-ranging operations and more formal governance environments, rather than as evidence of universal market maturity. Percentages are based on the responses, and may vary slightly by question where a respondent did not answer a particular item.

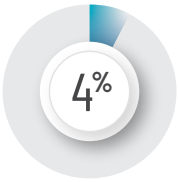
Respondent demographics

BY RESPONDENT SENIORITY

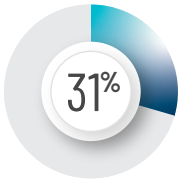
Junior Executive



C-Suite/Executive Leadership
(CEO/CRO/CFO/COO)

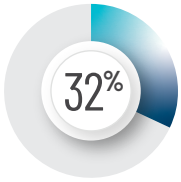


Board/
Board Committee Level



Middle Management
(Director/Department or Risk Manager)

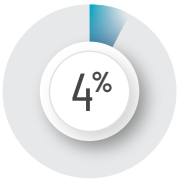
Professional/Specialist
(Internal Auditor/
Risk Champion)



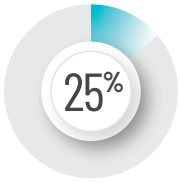
Senior Management
(MD/SVP/VP/Division Head)

Senior roles - C-suite, senior management and Board - account for **54%** of respondents.

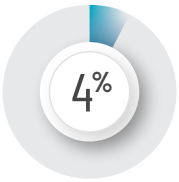
BY ENTITY TYPE



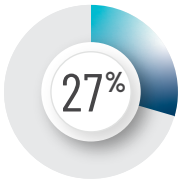
Multinational Subsidiary (MNC)



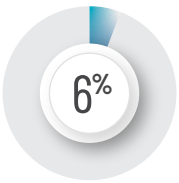
Publicly Listed



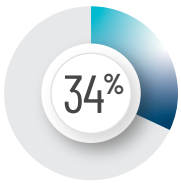
Other
(Conglomerate, Joint venture, Non-profit, Closed shareholding)



Privately Held



Family-Owned

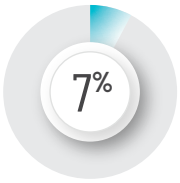


Government/
Semi-Government

Government and semi-government entities form the largest single group at **34%,** followed by privately held **(27%)** & publicly listed **(25%)** organizations. The base therefore reflects organizations that are more likely to have formal ERM structures already in place.

BY ORGANIZATION SIZE

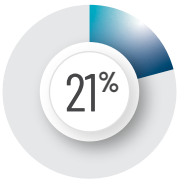
5,001–10,000 Employees



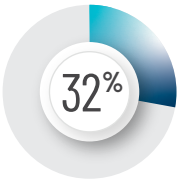
Greater than 10,000 Employees

200–500 Employees

501–1,000 Employees



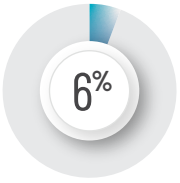
Fewer than 200 Employees



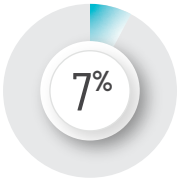
1,001–5,000 Employees

Organizations with more than **500** employees make up **65%** of the sample, confirming the weighting toward larger entities.

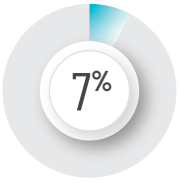
BY INDUSTRY



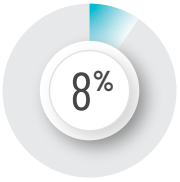
Manufacturing/ Industrial Products



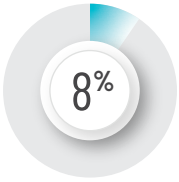
IT/ITeS



FMCG/Retail/ E-Commerce



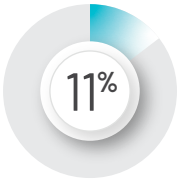
Logistics/ Warehousing



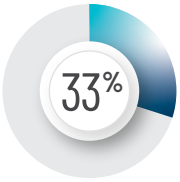
Telecom/ISP/ Broadband

Energy & Utilities

Financial Services



Banks



Other sectors

The respondent base also reflects a broad sector spread. Financial institutions, energy and utilities, logistics, telecommunications, technology, retail and manufacturing are all represented, with smaller participation from healthcare, aviation, real estate, construction, consulting and other sectors. This cross-sector mix supports a regional reading of the findings, while the report does not seek to present industry-specific benchmarks.

The growing strategic importance of ERM in the Middle East

The risk landscape in the Middle East is changing quickly. AI, cyber risk, and third-party dependencies are converging, while geopolitical tensions add further complexity. The World Economic Forum's 2026 Global Cybersecurity Outlook reports that 94% of respondents expect AI to be the most significant driver of change in cybersecurity in the year ahead, while 64% of organizations now assess AI tools for security before deployment, up from 37% in 2025.* This raises the bar for ERM functions to connect AI governance, cyber resilience and third-party exposure into one enterprise view.

Supply-chain interdependencies add another layer of complexity. The growing impact of cyber threats, third-party dependencies, and AI adoption requires organizations to integrate cyber risk, third-party risk, operational resilience, and technology governance within a unified ERM framework.*

Among surveyed organizations this integration is still developing. Only 29% report that AI is integrated into risk-management processes, 34% have documented AI governance, and 29% conduct formal AI-specific risk assessments. Third-party risk monitoring is more established at 60%, but the direction of travel is clear: the next stage of ERM maturity requires a more connected view of AI, cyber, third-party and resilience risk.

Regulators are also raising expectations. Regional regulatory cybersecurity controls strengthen requirements on cyber governance and incident response. With regional Vision programs advancing the digital agenda, technology, data, AI and resilience risks now sit at the center of strategic discussions that ERM should help lead.

ERM components should therefore not be read as isolated maturity indicators. For example, the 81% score for a Board-approved risk appetite is encouraging; however, it should be considered alongside lower scores for AI governance (34%), risk-linked compensation (51%), and measurable risk culture (64%). Most leading organizations have built solid foundations; the task now is to connect those foundations to the risks that actually affect growth, regulatory compliance, and resilience.

* WEF Global Cybersecurity Outlook 2026

Survey Results

Strategy and Governance

The Strategy and Governance pillar examines whether ERM is structurally connected to the strategic agenda — through documented objectives, an approved risk appetite, ESG integration and a requirement to consider risk before material decisions. This pillar advanced most in the 2020 baseline and continues to hold its strength in the current survey.

ESG and sustainability considerations are incorporated in strategic planning 60%

ERM risk review required before major investments, acquisitions and major decisions 73%

Board reviews and approves a written risk appetite and assessment criteria (annually) 81%

ERM objectives are formally documented and linked to strategic goals 88%

The two strongest results show that the formal architecture of ERM strategy is now widely in place. Documented objectives linked to strategy score 88%, and annual Board review and approval of a written risk appetite and assessment criteria scores 81%. These practices have moved from differentiators to baseline expectations. Compared with the 2020 study, which found risk appetite inconsistently established across the region, this is real progress in coverage.

The two softest results are more informative. ESG integration in strategic planning scores 60% presence, while a risk review before major investments stands at 73%. These two practices reveal whether ERM influences strategic decisions or simply records them. ESG integration is the clearest area for improvement in this pillar, given rising sustainability commitments and regional listing rules that increasingly expect transparency on ESG factors.

The 73% score for pre-investment risk reviews appears solid, but it provokes questions about how far those reviews affect decisions. Average presence across practices for this pillar is 76%, indicating that most organizations have some form of risk-review step before major decisions. Some, however, treat it as a binding gate capable of changing the outcome.

Relative to 2020, this is a classic move to the next stage. The earlier question was whether organizations had a written risk appetite. Now the question is whether that appetite translates into thresholds that can slow or halt an investment. For boards, the shift is from confirming that governance documents exist to seeking evidence that they are applied in real decisions — from presence to performance.

Leadership and Accountability

This pillar examines whether ERM has the required authority it needs and whether that authority is matched by clear accountability. Three practices are central: the CRO reporting line, how risk ownership is cascaded across the business, and how far risk-management performance is reflected in executive compensation.

Risk-management goals reflected in executive compensation 51%

Risk ownership assigned at every level with clear performance metrics 75%

CRO or equivalent reports to CEO with unrestricted Board and committee access 84%

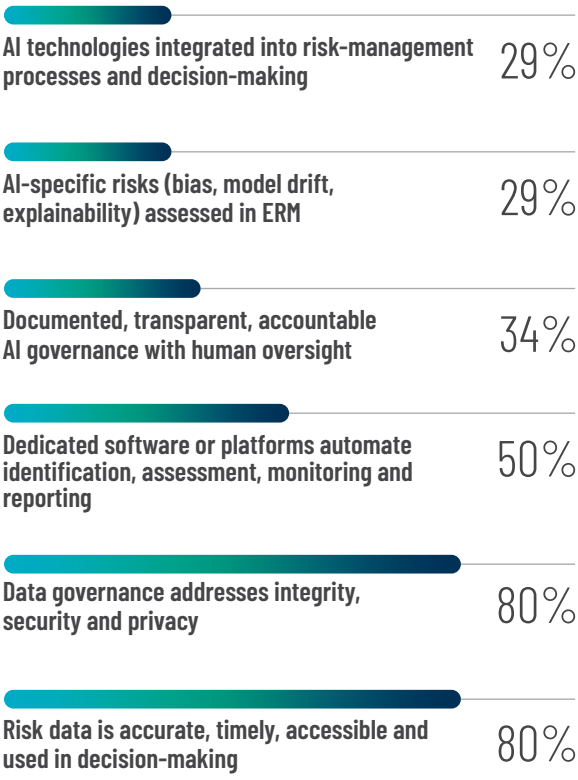
On reporting lines, the regional picture has matured. CROs (or their equivalent) reporting to the CEO with unrestricted access to the Board or relevant committees score 84%. This is a meaningful improvement on the 2020 baseline, which identified inconsistent CRO seniority and uneven Board access as structural weaknesses. Average presence across this pillar is 70%, confirming that structural authority is now broadly in place.

Risk ownership is the next-order issue, at 75% presence. This is encouraging, since most organizations report some form of cascaded ownership. Because the presence definition includes “Somewhat Present”, however, the headline figure alone does not separate organizations where ownership is genuinely embedded and measured from those where it is formally assigned but inconsistently applied. The familiar boundary between the central risk function and the first line is where boards should test for depth.

The most significant indicator in this pillar is the connection between risk management and executive compensation, with only 51% of organizations reflecting risk-management goals in compensation structures - the weakest leadership practice identified. This limited alignment diminishes incentives for executives to prioritize risk considerations in their actions. Explicitly linking compensation to risk objectives strengthens alignment with risk appetite and supports a stronger risk culture. In contrast, excluding risk from reward systems can result in predictable, less adaptive decision-making and partially explains why other behavioral practices, such as risk-aware decision-making and opportunity management, remain underdeveloped. For Middle East boards, improving the integration of risk into compensation structures is essential for embedding ERM and driving desired leadership behaviors.

Data and Technology

The Data and Technology pillar shows the widest maturity range in the current survey. It examines whether ERM is supported by reliable risk data, automated GRC technology and a defined framework for managing AI risk. The data foundation is considerably stronger than the technology and AI layer built on top of it.



There are two ways to read these results. The strongest results are positive. Both risk-data quality and data governance score 80%, indicating that many regional organizations now have a usable data foundation: they know where risk data sits, they govern it, and they trust it enough to use it in decisions. This is a meaningful improvement on the 2020 baseline, where the ERM data layer was among the weakest in the region.

The second set of findings requires close attention. ERM automation stands at 50% presence. AI embedding into risk processes is at 29%, AI governance with human monitoring at 34%, and AI-specific risk assessment at 29%. Average presence across this pillar is 50% — among the lowest in the survey. In practice, ERM technology in the region remains largely manual and spreadsheet-based rather than digitized and AI-enabled.

The contrast with global expectations is sharp. As AI becomes a major driver of cybersecurity change, organizations must enhance AI governance and embed AI-specific risk assessment within their ERM frameworks.*

COSO's 2024 guidance places responsibility for AI governance with the Board, and regional cybersecurity regulations broadly require documented governance of technology and data risks for relevant entities.** Middle East organizations are entering a more regulated and AI-intensive environment without having built the internal capability to keep pace. Strengthening data foundations is the right first step; the priority now is automation and AI-specific governance.

For boards and CROs, two actions follow. First, AI governance development areas should be addressed deliberately - not as an IT matter, but as an ERM and audit-committee responsibility, with a clear framework, assigned ownership, a model inventory and pre-deployment review. Second, ERM automation should be treated as core infrastructure. A risk function reliant on manual spreadsheets cannot meet today's expectations across cybersecurity, third-party risk, opportunity management and culture.

* WEF Global Cybersecurity Outlook 2026

** COSO Generative AI Guidance

Talent and Capabilities

The Talent and Capabilities pillar is the human-capital counterpart to the technology findings above. It examines whether the people responsible for ERM hold the certifications and experience, and the awareness and AI fluency, the profession now expects.

Risk professionals understand AI technologies and their risk impact 45%

ERM awareness and training delivered across organizational levels 75%

Risk personnel hold appropriate certifications, experience and competencies 81%

Results for certification and training are broadly positive. Certifications, experience and competencies score 81%, and ERM awareness and training across organizational levels score 75%, showing sustained investment in core risk capability across much of the region. The more important issue is AI fluency: only 45% report that risk professionals understand AI technologies and their risk implications. Within a pillar averaging 67% presence, this is the single factor most weighing on overall capability.

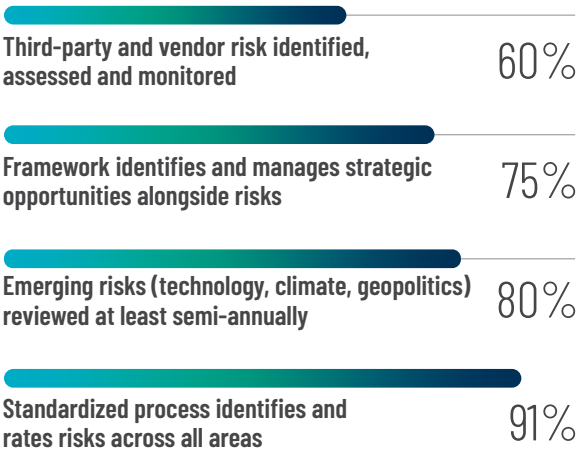
This finding matters on two related fronts. Internally, the 45% AI-fluency result sits alongside the 34% score for AI governance and the 29% score for AI integration reported under Data and Technology. Capability is developing slightly faster than implementation, but neither is keeping pace with the AI exposure regional businesses now face. Externally, the Protiviti and NC State 2025 Top Risks Survey places talent and labor costs alongside AI and emerging technology among the most significant risks for both the coming year and the longer term.*

For leaders, the implication is clear: ERM talent strategy is no longer a narrow HR concern, but a matter of strategic urgency given the accelerated adoption of AI and the evolving risk landscape described in global and regional research. Talent development has become central to the organization's ability to address deficiencies in AI governance and third-party risk management, particularly as regulatory expectations and external risks intensify. Investment in AI and data literacy across the second line and among risk-owning business leaders in the first line — including risk, compliance and internal audit — should therefore be prioritized as near-term, practical 90- to 180-day action points, as reflected in the Call to Action.

* Protiviti / NC State 2025 Top Risks Survey Executive Summary

Risk Identification and Assessment

This pillar covers the day-to-day mechanics of ERM — how well organizations identify, assess, scan and monitor risks across the enterprise, including emerging risks, strategic opportunities and third-party exposures. Core identification and assessment practices are among the clearest structural strengths the survey reveals, though the pillar also contains its two softest results — third-party risk monitoring at 60% and structured opportunity management at 75%.



Standardized risk identification — one of the least consistently implemented practices in the 2020 study — is now the strongest result in the current survey, at 91% presence. Emerging-risk scanning is also relatively strong at 80%. Average presence across this pillar is 77%, in line with the wider pattern: core risk-identification processes are now widely established.

The two practices to watch are opportunity management and third-party risk. The strategic-opportunity framework scores 75% presence: while many organizations now consider opportunities alongside risks, a meaningful number still lack a structured approach. Frameworks such as COSO ERM 2017 and ISO 31000 treat opportunity management as integral to effective ERM, not an afterthought,* so building a consistent, structured approach is where regional ERM can extend its strategic contribution.

Third-party risk represents a significant area requiring targeted improvement. With identification, assessment, and monitoring of third-party and vendor risk at only 60% presence, maturity remains insufficient considering the region's widespread reliance on cloud providers, technology vendors, managed-service firms, and outsourced operations. The WEF Outlook notes that supply-chain interdependencies are a leading barrier to cyber resilience because modern organizations depend on digitally connected suppliers, cloud providers, software vendors and outsourced services.** A cyber weakness in one part of that ecosystem can cascade into operational disruption, making third-party visibility and dependency mapping essential parts of ERM.

Given this context, third-party risk should be elevated as a Board-level priority. Boards are encouraged to require regular, formal reviews of third-party risk management frameworks, including documented inventories of critical vendors, periodic risk assessments, and integration of third-party risk metrics into overall ERM reporting. Assigning ownership of third-party risk at an executive level, and ensuring that findings from these assessments are explicitly linked to decision-making on vendor selection, contract renewal, and contingency planning, will facilitate greater depth and effectiveness in managing this complex exposure.

For management, opportunity management and third-party risk are the two clearest priorities for ERM to extend into. In both, the cost of standing still is materially higher than it was at the time of the 2020 baseline.

* ISO 31000:2018 Official Page

** WEF Global Cybersecurity Outlook 2026

Risk Controls and Mitigation

This pillar addresses how well organizations manage assurance and resilience within their ERM framework: whether risk responses are justified on a cost-benefit basis, whether controls are tested, whether assurance is coordinated across the three lines, and whether crisis-management and business-continuity exercises are realistic. These are the mechanics that turn an identified risk into a managed one.

ERM coordinates with assurance functions across the three lines 69%

Crisis-management and BCP plans documented, tested and updated 72%

Risk responses consider operational impact and cost-benefit 83%

Control effectiveness is independently tested and reported 84%

The two strongest practices demonstrate strong performance. With 83% of respondents considering operational impact and cost–benefit in selecting risk responses, and 84% independently testing control effectiveness. Together, these indicate a sound core assurance framework among leading regional organizations, though the figures do not by themselves confirm depth, and boards should test this in oversight.

The two softer results are less developed. Coordination between ERM and other assurance functions across the three lines is at 69% presence, and documented, tested and updated crisis-management and business-continuity plans are at 72%. Even at these levels, close to a third of respondents report these practices as barely present or absent. Many organizations hold plans that are not regularly tested or integrated across audit, compliance, ERM and IT risk — the clearest case for strengthening combined assurance.

An assurance layer exists, but its breadth and consistency are limited. Guidance from the World Economic Forum on cyber resilience and from COSO on AI both emphasize coordination across functions, particularly between the second and third lines.* With third-party risk monitoring at 60% under Risk Identification and Assessment, business continuity and combined assurance should become a primary focus for advancing maturity. Boards should seek integrated scenarios that address cyber, third-party and AI-related disruption collectively rather than in isolation, and should examine whether the 77% average presence reflects substantive capability or surface-level compliance.

* WEF Global Cybersecurity Outlook 2026

Culture and Continuous Improvement

Culture is the area where the 2020 study was most direct about the development required. Risk awareness existed in pockets, but a measurable, system-wide risk-culture framework was rare across the region. The current survey suggests the conversation has moved on, while the underlying capability has not yet caught up.

Risk-culture framework measures performance and drives maturity initiatives 64%

Risk communications to stakeholders are effective and regular 75%

Lessons learned from incidents update the ERM framework 81%

Incident learning (81%) and regular risk communication to stakeholders (75%) are now established in most respondent organizations - a clear shift from the 2020 baseline, when culture was the least developed area. Measured risk culture, however, remains at 64%. Leaders should still assess whether lessons are consistently incorporated into framework updates rather than addressed only occasionally.

The risk-culture framework - measuring culture, tracking it over time, and using it as a leading indicator of behaviour - stands at 64% presence. Read alongside Leadership and Accountability, where only 51% of respondents report that risk-management goals are reflected in executive compensation; Data and Technology, where AI-related practices range from 29% to 34%; and Risk Identification and Assessment, where third-party and vendor risk identification stands at 60%, the pattern is consistent. Culture is the integrating layer: where it is not measured, reinforced or linked to accountability, other ERM practices are more likely to remain procedural rather than embedded in day-to-day decisions and behaviours.

Culture is now on the agenda in a way it was not five years ago, with average presence at 73%. The question of depth remains a concern. The implication for boards is to ask three specific questions:

- Whether risk culture is measured at all;
- Whether the measurement covers all business units, not only the risk function; and
- Whether the results are used in performance and capability decisions, not simply reported.

Key Insights & Call to Action

Where the Middle East Stands

A Maturity Lens

Across the seven survey pillars, a clear maturity pattern emerges. The visible foundations of ERM, including governance structures, reporting lines, defined processes and formal risk assessment practices, are now largely in place among leading Middle East organizations. The next stage of maturity is therefore not about proving that ERM exists, but about testing whether it influences strategic choices, strengthens accountability, supports resilience and changes how decisions are made.

To interpret this progression, the report applies a practical maturity lens informed by Capability Maturity Model (CMM) logic. The maturity lens is used as a qualitative interpretation of the survey results, not as a scored certification model. It considers whether ERM practices are present, consistently applied, embedded in decision-making, measured over time and used to support resilience.

The maturity lens below builds on the seven themes introduced in the Executive Summary and translates the seven survey pillars into a Board-level view of where ERM capability is strongest today and where further progress is required. This connects the detailed survey results to the broader storyline of the report: Middle East ERM has moved beyond readiness, but its next test is whether it can convert presence into performance.

MATURITY THEME	LINKED SURVEY PILLARS	SURVEY EVIDENCE	CURRENT MATURITY READING	BOARD IMPLICATION
Strategy	Strategy and Governance; Leadership and Accountability	ERM objectives linked to strategy: 88%; CRO or equivalent access to CEO and Board: 84%	ERM is structurally connected to strategy and leadership, but the next test is whether it actively shapes strategic choices and transformation decisions.	Require ERM input at strategy, transformation and investment decision gates.
Capital allocation and opportunity	Strategy and Governance; Risk Identification and Assessment	Risk review required before major investments: 73%; framework identifies and manages strategic opportunities alongside risks: 75%	Risk insight is more established in governance than in capital allocation and opportunity identification.	Use ERM to challenge investment assumptions, assess downside exposure and identify value-creating opportunities.
Foresight and resilience	Risk Identification and Assessment; Risk Controls and Mitigation	Emerging risks reviewed at least semi-annually: 80%; crisis-management and BCP plans documented, tested and updated: 72%	Emerging-risk review is established, but forward-looking scenario planning and stress testing are applied inconsistently and are not yet a formal part of the ERM cycle.	Strengthen horizon scanning, geopolitical scenario planning, operational resilience testing and crisis readiness.

MATURITY THEME	LINKED SURVEY PILLARS	SURVEY EVIDENCE	CURRENT MATURITY READING	BOARD IMPLICATION
AI, cyber and data	Data and Technology; Talent and Capabilities	AI integrated into risk processes: 29%; documented AI governance: 34%; AI-specific risks assessed: 29%; risk professionals who understand AI and its risk impact: 45%	AI governance is the least mature capability in the survey, and capability is developing only slightly faster than implementation.	Establish a roadmap for AI governance, cyber-risk integration and AI literacy across the second and third lines.
Combined assurance and third-party integration	Risk Controls and Mitigation; Risk Identification and Assessment	ERM coordinates with assurance functions across the three lines: 69%; third-party and vendor risk identified, assessed and monitored: 60%; control effectiveness independently tested: 84%	Assurance coordination and third-party oversight are developing, but integration across ERM, cyber, compliance, internal audit and procurement remains inconsistent.	Align assurance functions around shared risk priorities, common reporting and coordinated testing.
Risk ownership and culture	Leadership and Accountability; Talent and Capabilities; Culture and Continuous Improvement	Risk ownership assigned at every level: 75%; risk-management goals reflected in executive compensation: 51%; risk-culture framework measures performance: 64%	Risk roles are clearer, but accountability, incentives, capability-building and culture measurement need further reinforcement.	Embed risk ownership into leadership behavior, performance management, capability development and culture metrics.
Digital maturity	Data and Technology	Dedicated platforms automate identification, assessment, monitoring and reporting: 50%; risk data accurate, timely and used in decision-making: 80%; data governance addresses integrity, security and privacy: 80%	The data foundation is strong, but half of organizations still run ERM on spreadsheets, which limits the speed and consistency of risk information reaching the Board.	Treat an ERM/GRC platform as core infrastructure rather than a reporting convenience; approve a target data model and a phased implementation.

The sequence matters more than any single starting point. The survey does not point to a single first step for every organization. It does point to a sequence. Combined assurance and ERM digitization determine the quality of risk information available to the Board and should be addressed first. AI governance and third-party risk are the largest capability gaps and should run in parallel, since both are subject to tightening regulatory expectation. Opportunity management and risk-linked incentives are the deepest changes, requiring framework and remuneration decisions, and should follow once the information base is reliable.

The central message of the survey is not found in any single metric. It is reflected in a consistent pattern: structural ERM is relatively strong, while behavioral integration, digital maturity, strategic influence and assurance coordination require further progress. The Call to Action therefore focuses on embedding ERM into decision-making, strengthening AI and technology-risk governance, improving combined assurance, reinforcing risk ownership and building a stronger culture of accountability. These actions are essential to move from ERM presence to ERM performance and from readiness to resilience.

Call to Action

Seven actions follow directly from the survey pattern set out in the seven pillars of the Detailed Survey Outcomes and the market context that precedes them, with each action mapped to one of the seven recurring themes. They translate the maturity lens into a practical 90- to 180-day agenda for Boards and executive teams, with each action assigned to clear possible owners. These milestones are the first steps in the 12- to 24-month agenda set out in the Executive Summary. The aim is to strengthen how ERM shapes strategic choices, capital allocation, AI and cyber governance, resilience planning, assurance coordination and leadership behavior. Together, these actions define what it means to move from the 2020 "Initial Adopter / Actionable" posture toward the "Influencer / Leader" maturity profile.

THEME	ACTION	WHAT SHOULD CHANGE	POSSIBLE OWNERS	90-DAY MILESTONE	180-DAY MILESTONE
Strategy	**Move ERM from the risk register to a strategic decision gate**	Require risk review for strategy refreshes, major investments, M&A, market entry and major programs. Translate risk appetite into decision-stage thresholds that support proceed, slow, escalate or stop outcomes.	CEO, CRO, Strategy	Embed criteria into relevant committee charters.	Document the first three decisions reviewed through the new gate.
Capital allocation	**Embed ERM into capital allocation and opportunity assessment**	Make ERM a formal part of capital allocation and investment review. Risk teams should test assumptions, evaluate downside exposure, assess concentration and identify opportunities that align with risk appetite and strategic ambition. Embed an upside-risk lens so the risk profile is used to surface opportunities, not only threats.	CEO, CFO, CRO, Strategy	Define risk-review requirements for investment and capital-allocation papers.	Apply the review to priority investment decisions and report lessons learned to the relevant committee.
Foresight	**Strengthen foresight and resilience**	Build horizon scanning, scenario analysis and stress testing into the ERM cycle, with specific attention to geopolitical disruption, cyber events, supply-chain interdependencies, regulatory change and operational resilience.	CRO, Resilience Lead, Business Continuity, Strategy	Agree priority scenarios and stress-testing methodology.	Complete a tabletop exercise and report resilience actions to the Board or risk committee.
AI, cyber and data	**Establish AI, cyber and data-risk governance**	Put in place a governance framework covering AI inventory, pre-deployment review, bias and explainability testing, third-party AI exposure, cyber-risk alignment and data-risk ownership.	CRO, CIO/ CISO, Audit Committee	Complete the AI inventory and approve the governance framework.	Complete the enterprise AI risk assessment, model standard and first round of pre-deployment testing.

THEME	ACTION	WHAT SHOULD CHANGE	POSSIBLE OWNERS	90-DAY MILESTONE	180-DAY MILESTONE
Combined assurance	**Integrate combined assurance and third-party oversight**	Align ERM, internal audit, compliance, cyber, IT risk, procurement, business continuity and operational resilience around shared risk priorities, common reporting and coordinated testing. Strengthen tier-1 and tier-2 vendor assessment for cyber, AI and operational dependency exposure.	CRO, Chief Audit Executive, CISO, Compliance, Procurement	Refresh the combined-assurance map and reassess tier-1 vendors using a cyber and AI lens.	Complete coordinated testing across selected high-priority risks and report assurance coverage to the audit or risk committee.
Risk ownership and culture	**Build risk ownership, culture and AI-capable talent**	Move from training to a measured risk-culture framework. Track risk-aware behaviors by business unit, link accountability to performance management and build AI and data literacy for second-line teams and risk-owning business leaders. Move the risk-and-control self-assessment program under second-line stewardship with a single enterprise methodology, to push risk ownership into the first line.	CRO, Chief Human Resources Officer, Business Leaders	Define culture metrics, assign business-unit ownership and launch a baseline survey.	Submit the first culture report to the Board and roll out the AI literacy curriculum to selected first-line and second-line teams.
Digital maturity	**Digitize the ERM function**	Replace spreadsheet-based risk registers with a dedicated ERM/GRC platform covering risk identification, assessment, control testing, monitoring and Board reporting on a single data model. Treat the platform as core infrastructure rather than a reporting convenience.	CRO, CIO, CFO	Complete a requirements definition and platform assessment; agree the target reporting data model.	Approve business case and begin phased implementation on the highest-priority risk domains.

From the table above, the message is clear: the fundamental elements of ERM are largely in place, but the next-stage capabilities are still developing. ERM in the Middle East now needs to connect its foundational structures with the strategic, digital, resilience and cultural dimensions that determine whether risk management influences decisions in practice. Over the next 12 to 24 months, the priority is not to rebuild the ERM framework but to strengthen its use in a market where regulators, boards, and global risk trends are raising expectations.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the Fortune 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

CONTACTS

Adnan Zakariya
Country Managing Director
Adnan.Zakariya@protivitiglobal.me

Sanjay Rajagopalan
Managing Director
Sanjay.Rajagopalan@protivitiglobal.me

Darshan Mehta
Managing Director
Darshan.Mehta@protivitiglobal.me

Ali Mohammed
Director
Ali.Mohammed@protivitiglobal.me

Our Offices in Saudi Arabia

Saudi Arabia - Riyadh
Al-Ibdaa Tower, 9th & 18th Floor
King Fahad Branch Road, Al-Olaya,
Building No. 7906, P.O. Box 3825
Riyadh 12313, Kingdom of Saudi Arabia

Saudi Arabia - Jeddah
King Abdulaziz Branch Road
Ash shati district , Building No.7524
P.O. Box 3675 , 23412 Jeddah
Kingdom of Saudi Arabia

Saudi Arabia - Dammam
Q1-5 , The Business Quarter ·
Salman Al Farisi St, Al Khalidiyyah
Al Janubiyyah, Dammam, Eastern
Province, 32221, Saudi Arabia

Our Offices in Middle East

Abu Dhabi
Emirates Real Estate Corporation
Building, 7th Floor, Office 707-711
Al Falah Street, Al Danah,
P.O. Box 32468, Abu Dhabi, UAE

Bahrain
Platinum Tower, 17th Floor
P.O. Box 10231, Diplomatic Area
Manama, Kingdom of Bahrain

Dubai
Office No. 2104, 21st Floor
U-Bora Tower 2, Business Bay
P.O. Box 78475, Dubai, UAE

Egypt
Cairo Complex
Ankara Street Bureau 1
First Floor, Sheraton Area
Heliopolis - Cairo, Egypt

Kuwait
Al Shaheed Tower, 4th Floor
Khaled Ben Al Waleed Street, Sharq
P.O. Box 1773, Safat 13018, Kuwait

Oman
Al-Ufuq Building, 2nd Floor
Office No.26, Shatti Al Qurum
P.O. Box 1130, P.C.112
Ruwi Muscat, Oman

Qatar
Palm Tower B 19th Floor
P.O. Box 13374, West Bay
Doha, Qatar

Face the Future with Confidence®

216676 - AUGUST 2026