National Technology News & Riskonnect Research Report

Shaping the Next Decade:

Overcoming Risk and Resilience Challenges in APAC

National Technology News

In collaboration with

riskonnect
Integrated Risk Management Solutions™

Introduction

Businesses in all industries across Asia-Pacific (APAC) are facing increasingly complex risk challenges, driven by economic volatility, new and evolving regulations, climate change, cyber threats and technology disruption. The need to move beyond a reactive approach to adopt and integrate a proactive risk management strategy into operations has become crucial for organisations to overcome risk and resilience challenges arising from these ever-evolving threats.

Recognising the growing importance of a robust governance, risk, and compliance (GRC) strategy, National Technology News and Riskonnect have conducted a survey of APAC-based GRC and resilience professionals to explore how organisations are identifying, managing and mitigating key risks, adapting to meet increasing regulatory requirements, and building resilience in dynamic and complex environments.

This report analyses the key findings from the survey, identifying major trends, challenges, and best practices for governance, risk, regulatory compliance, and resilience in APAC. Additionally, the report outlines how integrated GRC platforms can help firms implement best-practice processes to manage governance, risk, and compliance to drive process efficiencies and generate insights to support decision-making.

The survey results delve into various aspects of risk and resilience, such as growing risks GRC professionals face and strategies they are using to tackle them. It highlights the growing risks associated with third parties and supply chains, discusses compliance challenges surrounding ESG initiatives, and explains how companies are evolving their approach to risk appetite and enterprise risk management.

The survey results summarise the challenges that GRC leaders face when implementing risk & resilience strategies and uncovers the key trends that are emerging in the sector.

Methodology

National Technology News and Riskonnect surveyed 100 GRC and resilience professionals based in APAC. The survey explored how the adoption of software solutions for governance, risk, compliance, business continuity and resilience can facilitate analysis and real-time data sharing to drive agility and enhance decision-making.

It also explored a range of challenges faced by organisations across Australia, New Zealand, and South-East Asia, including the obstacles faced when managing operational resilience strategies and GRC data, alongside current trends and expectations in contemporary GRC approaches.

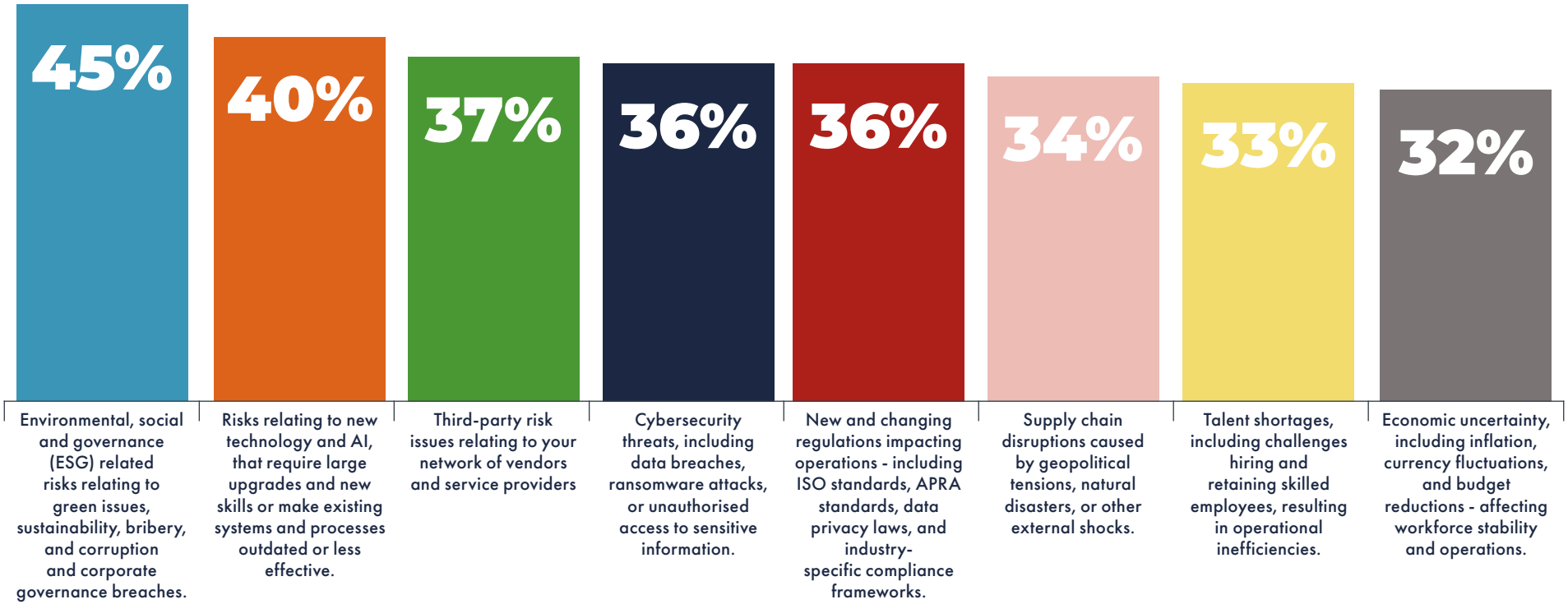
Disclaimer:

The findings and data presented in this report are based on the analysis and interpretation of available information. Please note that due to rounding, methodological variations, or other factors, some percentages and totals may not sum precisely to 100%. Any discrepancies in summation are not statistically significant and do not affect the overall conclusions of the report.

Contents

RESULTS

What are the top 3 risks your organisation is currently facing? (Select up to three)



The survey started by exploring the main risks that APAC companies are currently facing. With a maximum of three answers to choose from, respondents emphasised the presence of diverse risk infrastructure with a high number of concerns. In fact, all risks listed in the question were included in the answers of at least one-third of the respondents.

The Asia-Pacific region encompasses a wide range of countries, each with its own regulatory landscape, particularly in areas such as data privacy, ESG and operational resilience - forcing organisations to remain compliant in all jurisdictions that they operate in. Compliance obligations might be part of the reason why the most prevalent risk, chosen by 45 per cent of respondents, focuses on ESG risks related to green issues, sustainability, bribery, corruption and corporate governance breaches.

In particular, the figure may in part reflect the new mandatory sustainability reporting requirements under the Australian Corporations Act, which will be phased

in over the next three years for large entities, starting on 1 January 2025. Furthermore, both small and medium-sized entities may have to report on their GHG emissions to a large entity under the Scope 3 emissions reporting requirements if they are supply chain suppliers - further raising the bar on ESG-related risks.

Respondents also highlighted risks linked to emerging technologies and AI. While these innovations offer transformative potential, they introduce vulnerabilities – such as flawed AI decision-making, data privacy breaches, lack of skilled resources or system integration failures. Organisations relying on legacy infrastructure may face severe performance bottlenecks or incompatibilities as they modernise, elevating the strategic importance of continuous system testing and AI governance frameworks.

Some 37 per cent also cited third-party risks as a key concern, anticipating challenges in areas such as on-boarding, due diligence, contract management, regulatory compliance, performance monitoring, analytics and reporting.

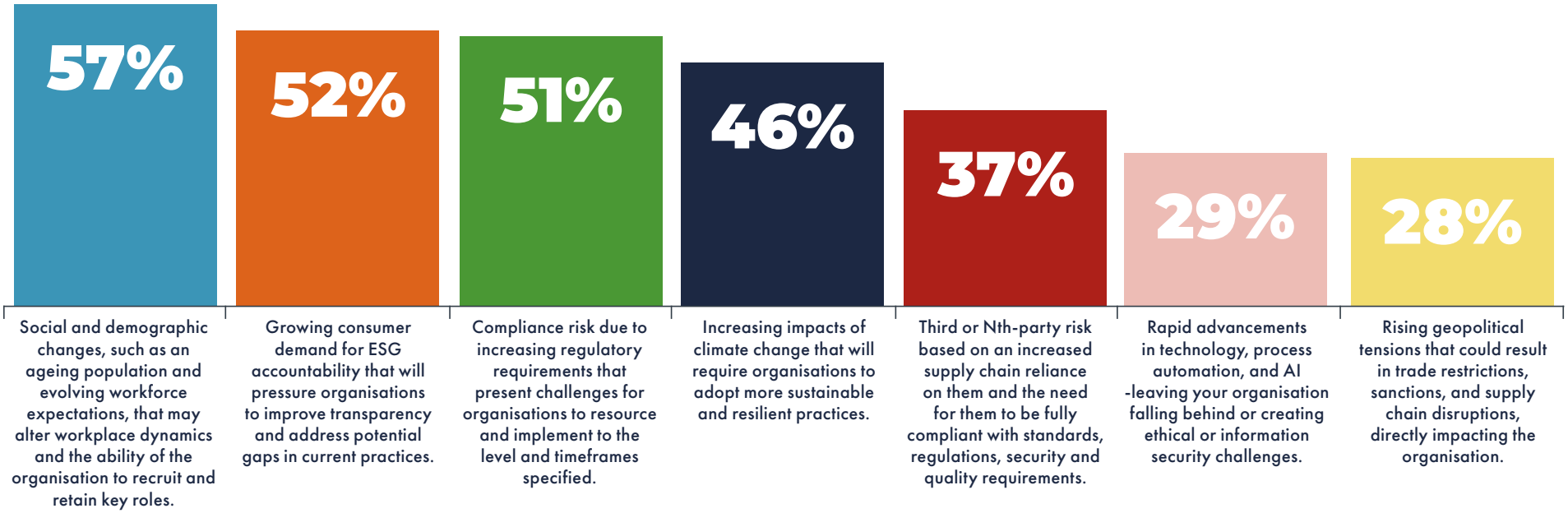
One factor likely influencing the focus areas of financial services organisations in Australia's top risk priorities is APRA's Prudential Standard CPS 230, which comes into force in July 2025 and requires companies to implement best practice processes for operational risk management, service provider management and business continuity & resilience.

Overall, the complex and evolving relationship between all the different risks listed underscores the need for a holistic integrated GRC solution to manage enterprise risk - providing a unified view across all levels of the business. Leveraging solutions that can consolidate risk data from across the enterprise, support strategic decision-making, offer real-time analytics, unite multiple teams, and promote a risk-aware culture among strategically different teams empowers firms to successfully work on reducing the most critical risks that could derail their strategy or lead to non-compliance.

2. Anticipated Emerging Risks Over the Next Decade

RESULTS

What emerging risks do you anticipate your organisation will face in the next 5-10 years? (Select up to three)



It is clear from the responses that all the listed risks are of concern to most companies, with the top three - social and demographic change, ESG and compliance risk - cited by over half of the respondents.

In this survey, more than half of the respondents (57 per cent) cited social and demographic changes, such as an ageing population and changing workforce expectations, as the top risk that may alter workplace dynamics and the organisation's ability to recruit and retain key roles. By using a risk management system that offers strategic planning and project and portfolio management, organisations can strategically prepare for changes in the workforce, developing new policies, controls and initiatives to promote staff retention, flexible working, talent acquisition, and re-training strategies that can help organisations thrive.

Over half of the respondents emphasised the growing consumer demand for ESG responsibility that will pressure organisations to implement ethical operating models and green initiatives. This emphasises that ESG is not only seen as the current top risk concern, but it is also viewed as a medium-to-long-term challenge.

Software with ESG management capabilities can support firms to collate and centralise their ESG data and report on the progress of key initiatives and programmes. Reporting outputs can be configured to align with international disclosure frameworks

such as the Task Force on Climate-related Financial Disclosures (TCFD), the International Sustainability Standards Board (ISSB), the Global Reporting Initiative (GRI), the United Nations Sustainability Goals and the mandatory sustainability reporting requirements from ASIC. These solutions can help organisations to collect, validate, and report ESG data effectively. Leading solutions can support ESG and sustainability strategic planning by linking initiatives to measurable KPIs, enabling both internal oversight and external transparency. These tools also enable firms to ensure compliance with ESG-related regulations and standards including ASIC's and the New Zealand External Reporting Board's sustainability reporting requirements.

Linked to ESG is a more general and widespread concern about compliance, with 51 respondents citing it as a major concern for the future. Increasing regulatory requirements bring new challenges for organisations, forcing them to implement new compliance processes within specific timeframes.

These are not just risks that can be managed reactively, understanding emerging risks over a 5-10-year timeframe is essential at the board-level, where wider organisational strategies will be based on this insight.

It is interesting to note that even the least selected option, risks associated with geopolitical tensions, was selected by more than a quarter of companies.

Rising geopolitical tensions – including trade disputes between China and the US, the Ukraine war, and maritime conflicts – pose serious risks to organisations operating in or dependent on APAC markets. The re-escalation of US tariffs, particularly on Chinese goods, along with potential retaliatory measures, adds further complexity to global trade, impacting costs, supply chains, and regional investment decisions. In addition, Australia and New Zealand face complex dynamics in balancing security alliances with the US through frameworks like AUKUS, while maintaining critical trade relationships with China. Singapore, as a key regional financial hub, must also navigate tensions between major powers. These tensions may manifest as trade restrictions, regulatory divergence, financial sanctions, rising costs and interest rates, or abrupt supply chain disruptions. Proactive monitoring and regional scenario modelling are critical to ensure supply continuity and compliance in such volatile conditions.

With such a broad spectrum of focus areas, it is essential for companies to be able to identify these emerging risks so they can add them to a risk register and monitor the risk level on an ongoing basis. In particular, organisations need to understand their current position and monitor fluctuations to know when to take action and implement controls. Software systems can provide forward-looking solutions for this, firms can maintain a separate risk register for emerging risks which, upon escalation, can be moved onto the main operational risk register.

3. Third-Party Risk Management Practices and Maturity

Despite nearly 40 per cent of respondents ranking third-party risks among their top concerns, only 30 per cent reported having a comprehensive and actively maintained third-party risk management (TPRM) framework. This suggests a major disconnect between risk awareness and risk maturity. Globally, according to EY's 2023 Third-Party Risk Management Survey, 54 per cent of firms use a centralised TPRM structure, while 36 per cent use a hybrid model–-indicating that the Asia-Pacific region shows slower adoption of structured third-party oversight compared to global counterparts. This gap leaves firms exposed to a multitude of downstream risks, including contract breaches, poor performance, compliance failures, cyber security issues, data breaches, and more.

The EY survey shows that organisations with centralised TPRM structures effectively managed almost twice as many third parties as those with hybrid structures. They also perform control assessments faster, with 64 per cent completing them within 31-60 days, compared to 43 per cent of organisations with hybrid structures achieving the same timeframe.

A modern TPRM framework should go beyond initial due diligence to include continuous performance monitoring and contract management. It should also incorporate automated risk scoring and tiering of suppliers; regular vendor risk assessments; regulatory, financial, and cybersecurity checks; and automated escalation and remediation workflows for poor performance, non-compliance, and escalating risks.

Cloud-based third-party risk management (TPRM) solutions enable firms to consolidate vendor data, formalise onboarding/offboarding, monitor performance against contractual terms, and flag high-risk entities through third-party risk intelligence feeds. This proactive approach to service provider risk provides ample visibility into potential problems and strengthens resilience.

Third-party risk systems create a profile for each vendor and capture critical details around costs, contracts, key contacts, SLAs, KPIs and risk profiles. Workflows automate periodic reviews and regular assessments, emergency suppliers and backup providers are captured, and the software also formalises the onboarding and offboarding process to ensure there are no hidden contractual clauses and that notice periods are respected.

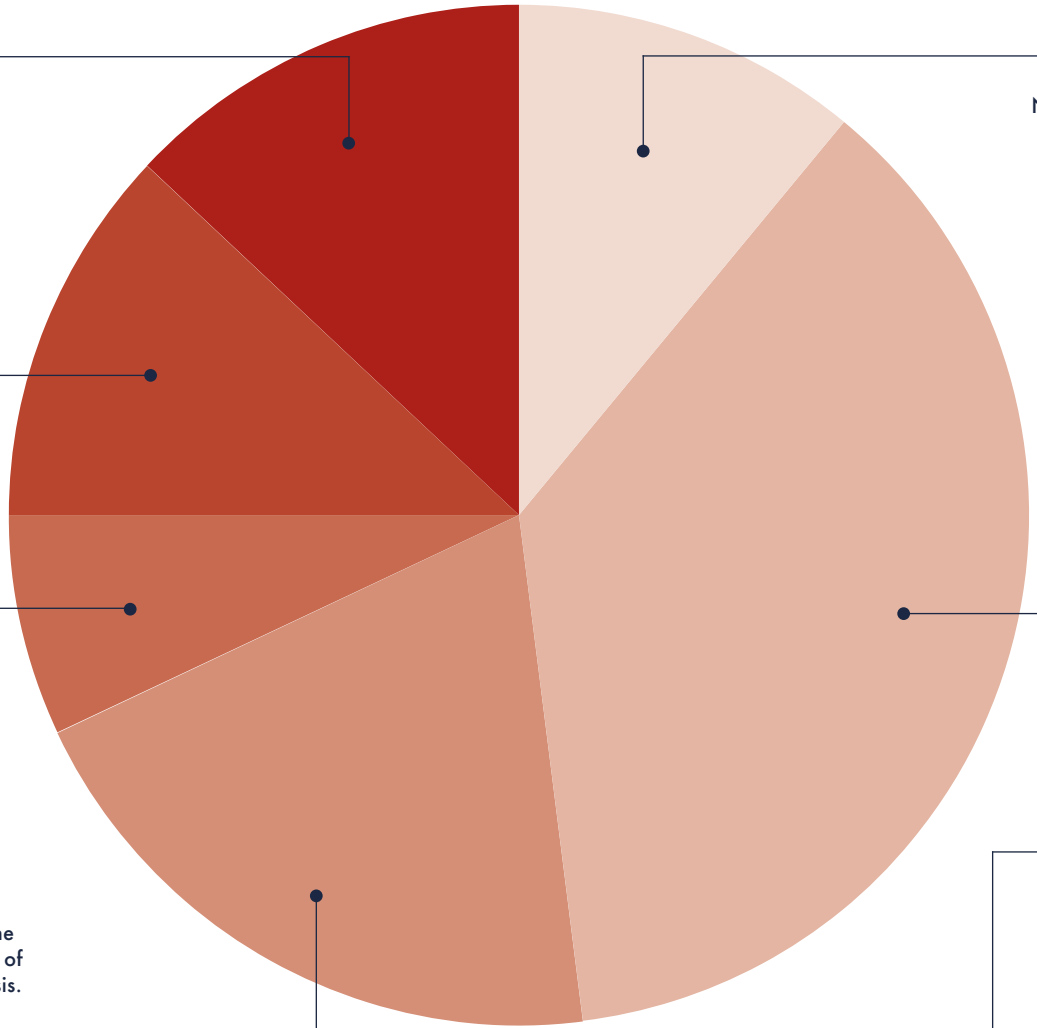
By integrating automation, these solutions streamline third-party management, formalising vendor onboarding and offboarding processes, monitoring third-party performance, maintaining emergency supplier backups, ensuring contractual compliance, and flagging high-risk suppliers for detailed evaluation.

RESULTS

How effectively does your organisation manage risks associated with third-party vendors or partners? (Select one)

RESULTS

How does your organisation currently manage business continuity and operational resilience? (Select one)



13%
We have best-practice automated BCM plans and an operational resilience strategy and have additional functionality like threat intelligence feeds and emergency notification crisis management capabilities.

11%
No plans in place.

12%
We have automated our BCM plans using software and have a comprehensive operational resilience strategy involving BIAs, a digital process model, and plausible scenario testing to identify gaps and ensure continuous improvement.

37%
We have a documented BCM plan, but that is as far as it goes.

7%
We use a BCM platform to automate the management of our BCM plans in terms of documentation, testing, and gap analysis.

20%
We have BCM plans and review them regularly and make updates. Processes are mainly manual using spreadsheets and emails.

As firms are increasingly required to implement best-practice business continuity planning processes to comply with key standards and regulatory frameworks such as ISO 22301:2019, ISO 22301:2020, APRA CPS 230 and CPS 232, a Business Continuity Management (BCM) platform has become an essential tool for organisations of all sizes as they seek to improve readiness and resilience to face unexpected disruptions.

Despite growing regulatory pressure, 37 per cent of respondents indicated they rely on manual BCM plans – usually spreadsheets or Word documents – which are time-consuming to create and manage and are often siloed and prone to human error. This is particularly concerning given the increasing adoption of international frameworks like the aforementioned standards and global best-practice operational resilience models.

During a crisis, manual plans often lack version control, real-time visibility, and defined escalation paths. This impedes rapid response, resulting in prolonged downtime - impacting operations and profits with the threat of fines, regulatory sanctions, and potential reputational damage.

A robust BCM program should include Business Impact Analyses (BIAs) aligned with operational processes; plausible scenario simulations (e.g., ransomware, regional blackouts); integrated emergency communication tools; and continuous testing and automated revision cycles.

BCM platforms enable firms to test their plans against different scenarios and vulnerabilities – ensuring Recovery Time Objectives (RTOs) are established and regularly tested, and teams are trained and prepared for real-world disruption.

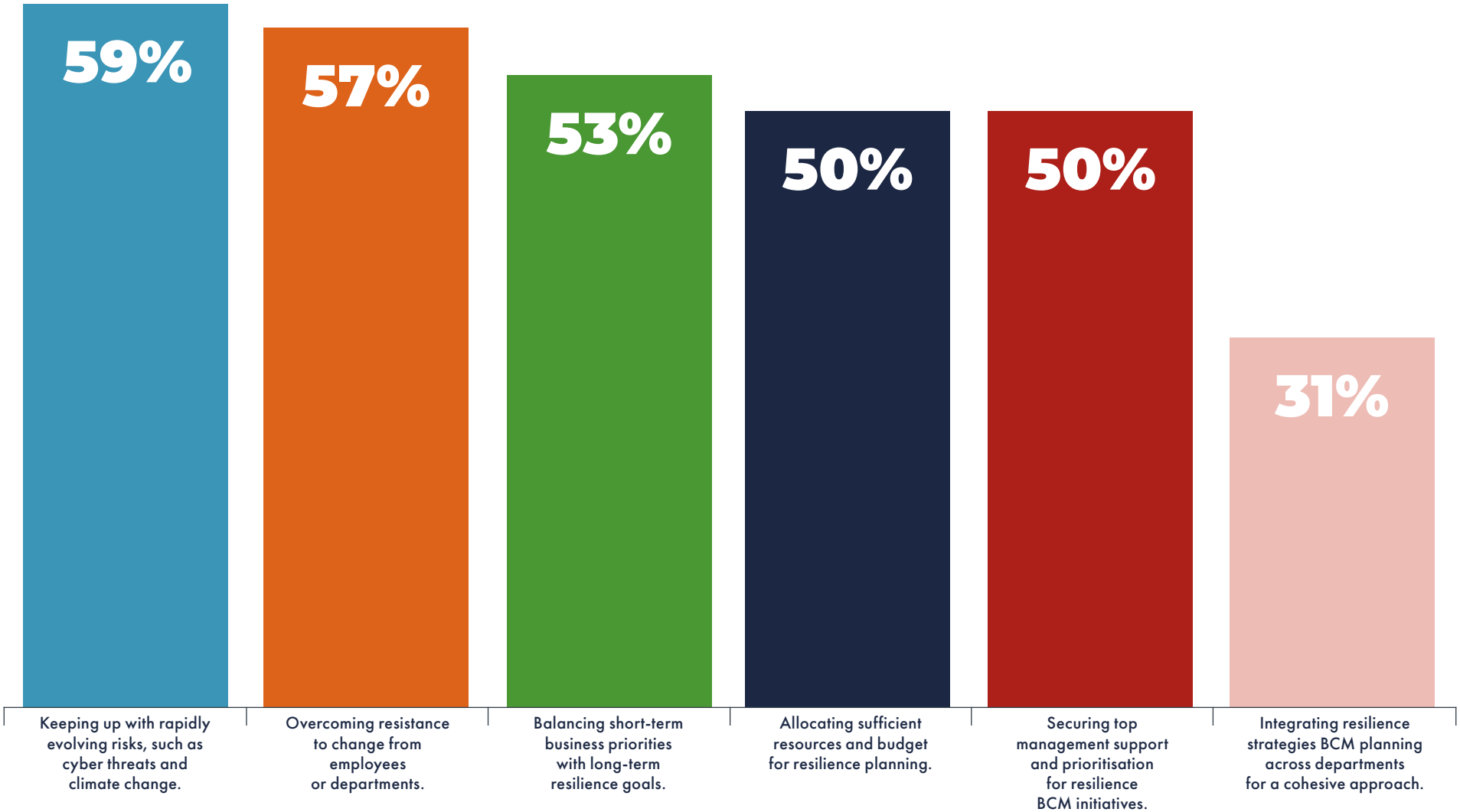
Businesses still using spreadsheets for BCM should be aware this outdated approach often leads to data silos, poor version control and a lack of robust data governance, resulting in poor data quality and compromised performance. Manual processes should be replaced by automated plans that eliminate manual tasks and ensure quality and accountability – freeing up time for improving BCM program performance.

With 11 per cent of respondents saying they had no plan in place, it is important to note that companies that choose not to implement a BCM process are at serious and potentially catastrophic risk of being completely unprepared in the face of increasing disruptions, and in some cases opening the door to heavy fines and legal action in the highly regulated APAC ecosystem.

However, it is important to note organisations are lacking robust BCM solutions worldwide. According to Riskonnect's "State of Resilience" 2025 report, 75 per cent of North American executives admit that their organisations are not fully prepared to comply with upcoming operational resilience regulations. The same report highlights that 85 per cent of EMEA executives recognise that their organisations are not fully prepared to comply with new regulations on operational resilience, highlighting a significant area for improvement globally. This underscores that gaps in preparedness are not unique to the Asia-Pacific region, but part of a broader global challenge facing organisations across all regions.

RESULTS

What are the biggest challenges your organisation faces when implementing resilience strategies? (Select up to three)



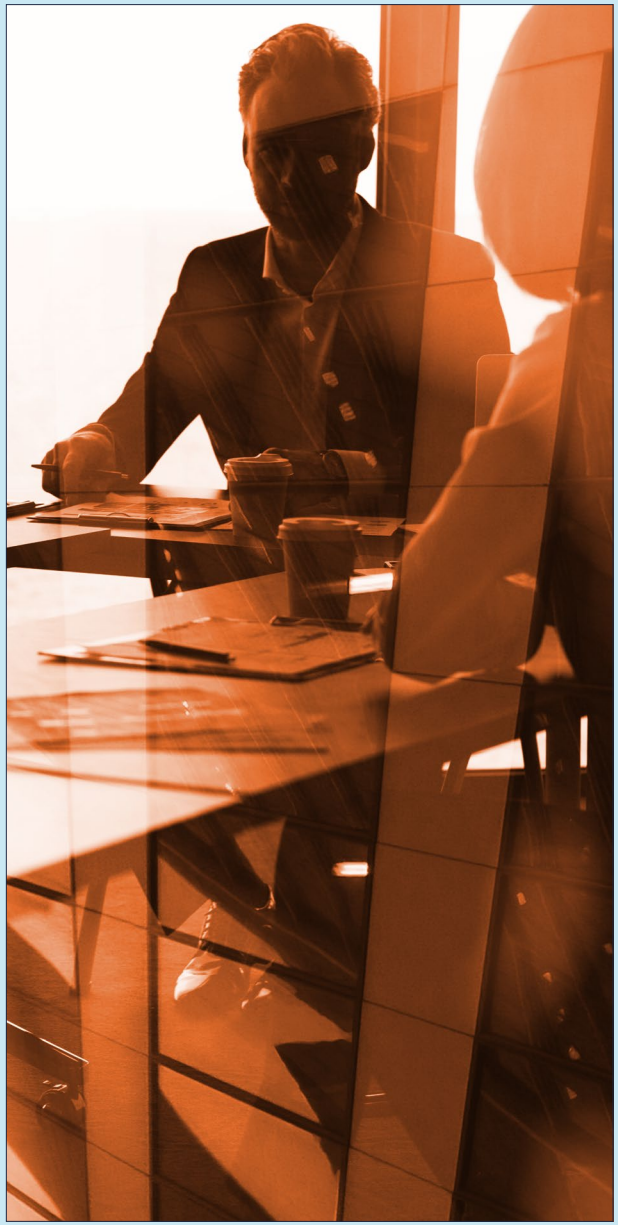
The unpredictability of growing risks such as cyber threats and climate change is cited by 59 per cent of respondents as one of the main challenges when implementing resilience strategies, making them especially critical for more than half of APAC organisations compared to more "traditional" risks.

To counter the unpredictability of these rapidly evolving risks, firms can subscribe to specialist threat intelligence feeds that integrate directly into their BCM platform. These subscription services scan sources such as news outlets, government agencies, regulators and social media to build a real-time view of an organisation's threat landscape. These solutions include real-time dashboards that help visualise potential threats, such as natural disasters, geopolitical risks, third-party risks, cyber threats, and vulnerabilities, enabling firms to conduct scenario planning that continuously adapts as new data becomes available - for example, after a breach or a climate alert.

With more than half of respondents also citing overcoming resistance to change from employees and departments as one of the main challenges faced when implementing resilience strategies, it is important to note how a BCM platform enables automation of BCM processes. It eliminates many of the administrative tasks associated with planning, testing, updating, and executing BIAs - enabling everyone from operational staff and department heads to board-level executives to get involved in the updating and testing of plans. Frontline employees can easily complete BIAs and assessments online, and team leaders can check and update BCM plans directly in the system. All staff can easily access the BCM platform with features such as single sign-on and two factor authentication, ensuring security is maintained.

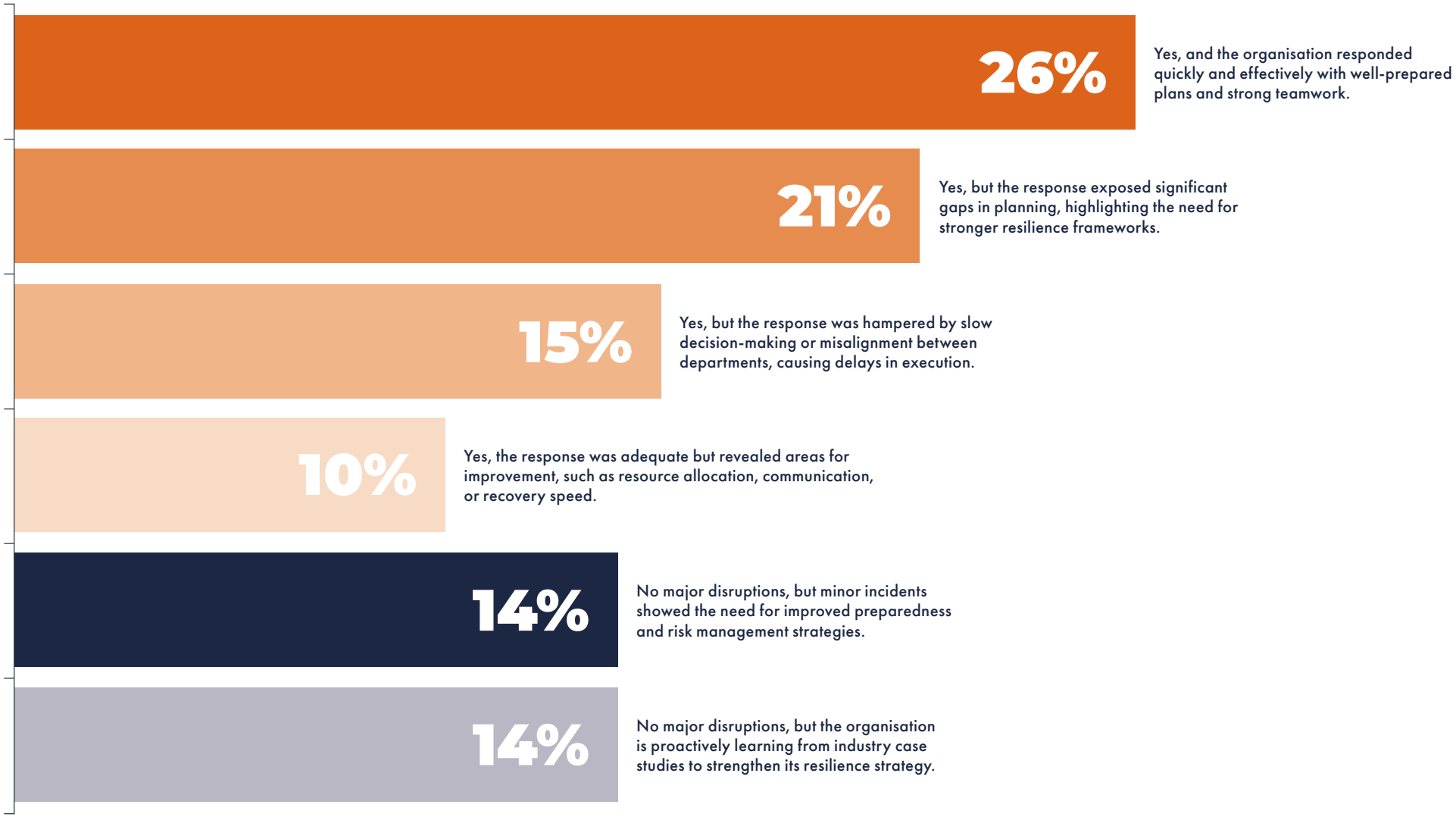
A BCM platform also addresses the issue of allocating sufficient resources and manpower. Since many companies only have a small BCM team - maybe just one or two people - other employees can help by updating plans, filling out test reports, and completing online BIAs. All of this information gets stored in the platform, so the BCM team ends up with a large amount of valuable data, even though it is mostly entered by non-BCM staff as part of their normal work.

Securing top management support and prioritisation for resilience BCM initiatives - a challenge faced by 50 per cent of respondents - could also be addressed by integrating a BCM platform that enables executive reporting for board members, enabling them to access business continuity dashboards & reports to facilitate understanding of risk exposure and potential impacts using powerful 'what-if' modelling systems.



RESULTS

Has your organisation experienced major disruptions in the last five years, and how did it respond? (Select one)



A concerning 46 per cent of respondents revealed that their response to threats needed improvement. In this group, respondents highlighted numerous areas, including the need for stronger resilience structures, misalignment between departments, delays in execution, and problems with resource allocation, communication and speed of recovery.

These problems highlight that not only do companies need up-to-date, tried and tested business continuity plans, but they also need crisis management plans. Companies should have preplanned emergency notification message templates for different types of crisis and backup communication channels so they can clearly communicate with employees during a crisis. Adopting a holistic approach that enhances communications between departments ensures that the right staff are involved, and recovery plans are clearly communicated to ensure a fast recovery rate.

Only a quarter of respondents (26 per cent) believe that their business risk management plans and incident management processes are effective in the event of a major disruption, leaving many businesses exposed.

It is not just major disruptions and crises that organisations need to consider to build resilience and reduce risk. Firms also need to capture and resolve smaller incidents, hazards and near misses to address them before they escalate. Alongside their BCM planning processes, businesses should also have a clearly defined incident management process. Most business continuity software platforms offer incident management capabilities that enable staff to easily report incidents, hazards and near misses via forms. Automated workflows and predefined rules that can escalate and categorise incidents and facilitate the implementation of corrective actions. These platforms also offer a framework to conduct root cause analysis, launch investigations and implement corrective actions to prevent further related incidents.

Incidents can trigger BCM plans based on the type of incident logged, and BCM software can automate BCM plans by notifying staff of each step in the recovery process and allowing staff to record the completion of tasks. Software ensures the recovery plan can move on to the next phase and everyone is informed.

Respondents who did not experience major disruptions still admitted to being unprepared (14 per cent), demonstrating inexperience in this area but an equal percentage of respondents said they proactively learn from industry case studies to strengthen their resilience strategy. This shows firms are actively seeking ways to learn how to improve their business continuity programmes by learning from industry best practices.

Case studies provide valuable post-event insights and should be used as guidance to build a proactive resilience strategy. To learn from case studies organisations should go beyond planning by simulating potential future risk scenarios, testing operational playbooks, and embedding real-time scenario intelligence into their business continuity and risk frameworks.

There are a range of software solutions that can help by providing simulations and trend analysis, allowing companies to test potential threats and opportunities and to assess impacts before they occur, in a much more future-oriented way.

RESULTS

How does your organisation ensure compliance with evolving regulatory requirements? (Select one)

A total of 38 per cent of respondents said they use horizon scanning technology to monitor and automate the management of regulatory changes. This is positive: automated horizon scanning helps companies monitor and interpret regulatory developments in real-time, ensuring that they are not caught off guard by regulatory updates both regionally and globally. Subscribing to these regulatory updates provides companies with early warning systems and a strategic advantage, enabling them to adapt quickly to a constantly evolving regulatory requirements.

However, a concerning 62 per cent of companies still rely on manual processes to manage regulatory changes, which wastes time by forcing teams to manually search for updates from different regulatory bodies. This leaves companies struggling to understand what has changed and how it will affect them and making it hard to determine which updates require action. This fragmented approach increases the risk of important regulatory changes being missed or identified too late - resulting in delayed or rushed implementation and potential non-compliance. Digitised compliance reporting with visual dashboards and reports can help compliance reporting by building personalised dashboards for employees of all levels to view their compliance tasks and understand their key metrics.

With 18 percent of respondents stating that compliance changes are documented in shared files - and 18 percent reporting a combination of manual tracking with basic tools to manage regulatory updates – it is crucial for these firms to understand the value of a centralised compliance management software solution.

Through automation, technology simplifies processes as each regulation is automatically mapped to all relevant processes, systems and policies. So, when the regulations change, companies know which processes, policies and procedures might be affected. This not only reduces the risk of oversight, but also significantly increases efficiency by eliminating manual tracking and enabling faster, more accurate responses to regulatory updates. A digitised compliance reporting system with visual dashboards and reports can help compliance reporting by providing personalised dashboards for employees of all levels to view their compliance tasks and understand their key metrics.

Increasing regulatory requirements – including APRA CPS 230, trade laws, anti-bribery guidance, data privacy regulations, and ISO standards – are presenting APAC firms with both resource and capability challenges. A centralised compliance management platform helps firms map obligations across jurisdictions, automate controls, and visualise compliance gaps in real time. This reduces the reliance on manual tracking, which remains prevalent despite its operational risk.

A holistic and centralised approach using software can greatly simplify compliance for complex regional and global contexts and automate the reporting of gaps or overlaps in compliance coverage by being automatically informed of when regulations change. This avoids having to monitor multiple sites for regulatory updates. Executives can log on to view compliance scores status by business unit which can help them prioritise risks and allocate resources adequately.

8. Gaps in Governance, Risk, and Compliance Frameworks

RESULTS

What are the biggest gaps in your organisation's governance, risk, and compliance (GRC) approach? (Select up to 3)

More than half of companies surveyed reported that their approach to risk was not aligned to their organisational strategy and objectives, with over a third specifying that their approach was predominantly reactive rather than proactive. A third of respondents reported insufficient resources and risk management being left to senior management – signalling the need for a more collaborative approach.

According to Norman Marks, renowned Author, Speaker, Thought Leader, OCEG Fellow, and Honorary Fellow of the Institute of Risk Management, the cost of keeping risk management and corporate strategy separate can be the success of an organisation. "Too often the risk team is seen as the department of 'no'. The department that quite literally stops people from doing what they want to do and diverts them from what they see as running the business," said Norman. He continues, "My proposition is that the term risk itself is unhelpful in bringing risk and strategy together. I know one organisation that changed their risk team to decision support. I also like to think of risk as the department of 'how'. It completely reframes the kind of support the business needs and the kind of intelligence that can be delivered."

This highlights the value of GRC platforms that can map risks to strategic objectives. These solutions

transform risk management into a strategic function, enabling firms to take calculated risks in pursuit of their objectives and mitigate any risks impacting strategic initiatives, critical projects, and operations.

For example, risks can be mapped directly to strategic objectives, KPIs, and initiatives within Riskonnect's strategy module, ensuring that leadership understands which risks could cause the strategy to fail and where to invest in controls or mitigating actions.

One of the main mistakes companies make is trying to keep risk levels low across the board to 'stay out of the red', investing time, money and attention through a 'scattergun' approach, without having a clear understanding of what matters most.

However, companies do not have an infinite amount of money and resources to reduce every single risk. Therefore, they must prioritise risks based on their impact on strategic objectives and enterprise performance, so that they can make informed decisions on where to allocate resources for best effect.

With 29 per cent of respondents admitting they still rely on manual processes, it is important to note that managing risk and organisational strategy in separate spreadsheets is challenging, as the two sets of data are isolated. In a software platform however, risks can be linked to strategic goals, operational performance, compliance obligations, and incidents. This enables risk and strategy teams to focus their efforts in the right areas to protect the business and achieve strategic objectives.

Taking ownership for risk and completing tasks that contribute to the organisational strategy should be integrated into the role and daily responsibilities of employees by management. Software enables everyone to be part of the risk management program, not just specialised risk teams. Anyone can own a risk, complete a simple risk assessment or control check, or tick off a task or action related to the organisation's strategy in the platform. While having risk professionals is important, the tool is designed to make enterprise risk management (ERM) and strategic planning accessible and integrated throughout the organisation.

It is essential to link risks to strategic and operational objectives, departments, and programs, creating responsibilities at every level. The system then allows users to assign ownership, timelines, and status updates, creating a transparent and traceable workflow for both risk and strategic management.

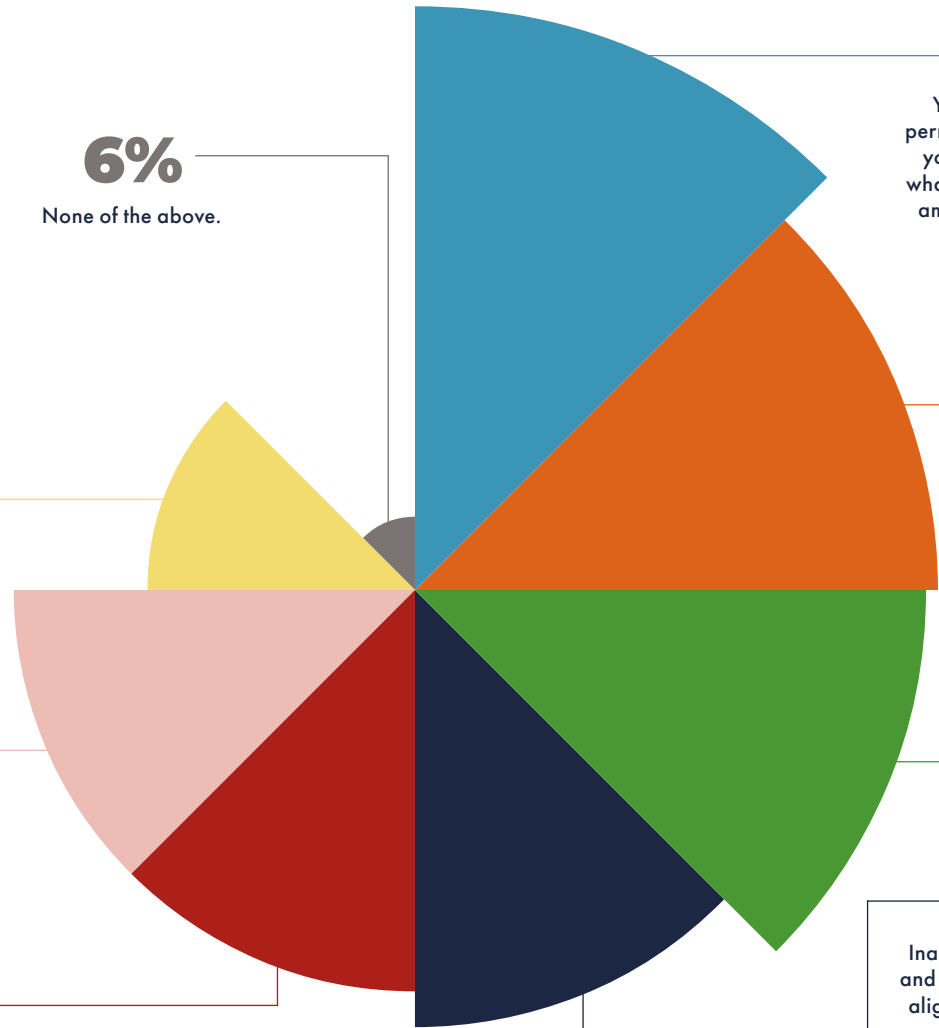
When asked what successful risk management looks like, Norman Marks concludes, "It's when each of the executives can say, 'I have the information and the confidence that I need, to make informed and intelligent decisions, to take the right risks for success'. It is even more effective when people are thinking about anticipating what might happen, getting all the information, consulting the right people, and making these quality decisions by themselves without a risk manager present to make sure it happens."

28 per cent of respondents cited compliance & regulatory change as the biggest gap in their GRC approach. This signals a need for a modern automated compliance monitoring tool to streamline and automate the process. When a regulation changes, the software assesses its impact on all departments and projects and automatically creates related actions, activities and policy updates to address it. This all-in-one automation can transform regulatory change management from a reactive task to a proactive and strategic capability.

Another 29 per cent cited managing third party risk an area to address. Many firms rely on a wealth of vendors, suppliers and third parties to run their operations, and poor performance or unethical behaviour by vendors could severely impact an organisations' ability to deliver its products and services and cause financial and reputational damage. Organisations who are concerned about this area should look to implement software with comprehensive third-party risk management capabilities. This enables them to capture critical details about each vendor centrally, automate vendor risk assessments, formalise the onboarding and offboarding process, monitor contractual performance against SLAs and KPIs, and receive updates about their suppliers via third party risk intelligence feeds. Following this structured process ensures that firms can get a centralised view of their vendors and detect and address issues and poor performance quickly before it escalates.

RESULTS

What are the main challenges your organisation faces when managing GRC data? (Select all that apply)



48%
Your process lacks a user permissions hierarchy meaning you can't see who changed what and users can access and amend data that may not be relevant to their role.

43%
Turning data into useful reports that can support leaders to make informed decisions.

42%
A lack of data governance rules, resulting in poor data quality or incomplete data, which produces inaccurate reports and can lead to unreliable decisions.

36%
Inability to effectively consolidate GRC and ESG data and report on it, hindering alignment with sustainability goals, risk management and business planning.

33%
Data is not mapped across GRC functions making it hard to link risks to the related compliance requirements, incidents or controls.

33%
Insufficient data meaning you don't have a big enough data set to run reliable reports.

22%
Lack of a centralised platform, leading to fragmented data sources.

6%
None of the above.

Only 6 per cent of respondents reported no challenges in managing GRC data—indicating widespread weaknesses in data integrity, traceability, and reporting maturity across APAC firms. Common issues include a lack of data governance protocols, insufficient user permission hierarchies, and poor linkage between risks, compliance obligations, and incidents.

Incomplete or unreliable data hampers leadership's ability to prioritise threats, allocate resources, or evaluate control effectiveness. It can also lead to non-compliance, failed audits, escalating risk levels, misinformed decisions, and strategic blind spots.

Integrated GRC platforms address these challenges by providing features such as role-based access to controls and audit trails, automated data entry, data mapping across GRC domains, and real-time dashboards with advanced analytics. Business intelligence tools can further enhance these platforms, enabling management teams to analyse performance, identify root causes, and forecast risk, helping to improve efficiency and effectiveness in assessment, actioning, monitoring and reporting.

In GRC platforms, you can see data's source meta-data based on the users' logins ensuring accountability, enabling users to only see data relevant to them so they are not overwhelmed by copious amounts of data. This system enables them to execute tasks and actions via their own personalised dashboard, promoting accountability and ensuring that all tasks are completed on time.

GRC software also simplifies and automates monitoring and reporting. Teams can view details and analysis around risk exposure, control effectiveness, emerging risks, incidents and their causes, compliance status, and policy attestations at the touch of a button. Often, GRC solutions offer Microsoft Power BI reporting integration, so organisations can visually summarise and categorise performance and enable data drill-down for analysis. All these reporting options support timely and informed decision-making. And the automation saves a lot of time on creating manual reports - freeing up resources to focus on activities to better manage risks, align to organisational strategy, and bolster governance and compliance efforts.

Ultimately, an effective GRC platform provides the means to manage a multitude of challenges relating to GRC data, allowing staff at all levels to actively collaborate on the right issues and initiatives at hand.

10. Approaches to Defining and Applying Risk Appetite

The results reveal a concerning picture of how organisations currently manage decisions relating to risk appetite.

While 33 per cent of respondents said they had defined and communicated a risk appetite statement in line with strategic objectives, almost half of respondents said they did not have an adequate approach to risk appetite and tolerance.

Some 20 per cent of respondents emphasised that their risk appetite statement is not applied consistently across business units. Additionally, over a quarter of respondents indicated that risk appetite is not integrated into the organisation's decision-making processes, suggesting that they are managing risk in isolation without a clear understanding of how much risk the company is willing to accept in certain areas.

The fact that nearly half of respondents lack a consistent or up-to-date risk appetite framework highlights a serious vulnerability: without clear risk boundaries, organisations are effectively making strategic decisions blindly in relation to the level of risk that is acceptable.

Risk Appetite Statements (RAS) should consider a number of important elements including: the nature of the business and attitudes towards risk, the existing risk profile, the organisation's risk capacity and risk tolerance. When developed and implemented properly, a RAS can support management and board-level discussions on the trade-off between opportunity and exposure, and guide decisions on investment, pricing, and innovation. It can also trigger automated escalation if risk thresholds are breached. It is good practice to periodically review the RAS—especially where regulatory, technological, environmental, societal or geopolitical shifts alter risk exposure and affect the organisation's willingness to accept or tolerate risk.

Digital risk appetite and tolerance tools enable real-time monitoring of risk exposure, with customisable tolerance bands and automated alerts enabling firms to set and monitor risk levels relative to their risk appetite in real time. Organisations should avoid allowing their RAS to become a document that is separated from their risk framework and unable to be successfully implemented and embedded in their risk management process. Companies should define clear tolerance levels and associated Key Risk Indicators (KRIs) for each risk and establish a process to alert risk managers when they are getting close to exceeding these levels. If the risk cannot be managed within the set tolerance levels with existing controls and available resources, additional resources may be required.

The results highlight the need for organisations to not only define and communicate their risk appetite, but also to integrate it into their risk management framework and process, with clear tolerance thresholds, associated KRIs and effective risk monitoring, reporting and escalation.

If these factors are not addressed, the organisation's RAS risks becoming an ineffectual box-ticking exercise rather than a key strategic tool.

RESULTS

How would you describe your organisation's current approach to risk appetite and tolerance? (Select one)

Conclusion

The Asia-Pacific region presents a challenging risk landscape, with organisations facing a convergence of geo-political and economic volatility, regulatory change, societal change, climatic extremes, technology disruptions and escalating cyber risks. The survey underscores the impact of these concerns at an organisational level, revealing that while social and demographic changes, ESG, and compliance risks top the list, with over half of respondents expressing concern, even the less prominent risks were acknowledged by more than a quarter of the surveyed companies. This widespread concern necessitates a decisive shift from reactive to proactive and integrated risk management and business resilience strategies.

To navigate this complexity, decision-makers should prioritise the adoption of integrated GRC platforms. These solutions provide the strategic capability, analysis and insight needed to transform risk management from a tactical exercise into a core, strategic business function. By automating and integrating risk, strategy, compliance, business continuity and resilience, these platforms deliver an enterprise-wide view of GRC, supporting decision making and optimising resource allocation, and strengthening governance. This proactive approach enhances operational resilience and equips organisations to anticipate and adapt to dynamic environments.

The survey highlights that over half of the surveyed companies (51 per cent) recognise that compliance risk due to increasing regulatory requirements will present a major challenge for organisations to resource and implement to the level and timescales required. This statistic further emphasises the urgent need for a proactive approach to compliance management.

Furthermore, the survey highlights the critical importance of addressing emerging priorities. In particular, the growing consumer demand for ESG accountability, identified by 52 per cent of respondents as a key emerging risk, necessitates the implementation of dedicated ESG management tools to ensure transparency and effective sustainability reporting. Similarly, given the prevalence of third-party risks, identified as a top three risk by 37 per cent of respondents, TPRM solutions are essential for monitoring performance, detecting threats, and mitigating vulnerabilities within the enterprise. The survey also revealed significant gaps in TPRM maturity, with only 30 per cent of organisations reporting a comprehensive and actively maintained TPRM framework.

Inaction is not a viable option. To ensure sustainable growth and maintain a competitive edge in the APAC region, business leaders must embrace a proactive, data-driven, automated and integrated approach to GRC. Decision-makers should prioritise investment in integrated GRC platforms that incorporate specialised solutions for risk management, organisational strategy, business continuity & resilience, regulatory compliance, ESG and TPRM. This strategic investment will not only mitigate risk but will also unlock opportunities for enhanced agility, growth, resilience, and ultimately, long-term success.

About Riskonnect

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organisations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise. More than 2,500 customers across six continents use our unique risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts across Australia, New Zealand, Asia, the Americas and Europe. To learn more, visit **www.riskonnect.com**

About National Technology News

National Technology News (NTN) is a key brand for technology purchasers and vendors in the UK, evolving from the successful inaugural National Technology Awards in 2017. As a dynamic multi-channel news and events brand, NTN provides comprehensive coverage and direct access to key technology decision-makers across UK businesses. We deliver insights through a daily-updated website, targeted e-newsletter, active social media channels, and an extensive podcast series. NTN drives industry engagement through three flagship annual awards: the National Technology Awards, Payments Awards, Retail Systems Awards, and FStech Awards. Throughout the year, we host strategic roundtables and conferences that explore critical industry themes including digital transformation, payments innovation, cybersecurity, data compliance, regulatory developments, and emerging technologies. To learn more, visit **www.nationaltechnology.co.uk**

NTN National Technology **News**

In collaboration with

riskonnect
Integrated Risk Management Solutions™