KPMG

CHARTERED SECRETARIES
特許秘書

Risk management survey: Empowering success

kpmg.com/cn

hkics.org.hk

Contents

Foreword

Throughout the past year, businesses have been operating in a dynamic environment marked by constant change driven by global instability and the outbreak of COVID-19 that has caused significant disruption to business operations.

Companies operating in Hong Kong have had to deal with increasing uncertainty. It is therefore important for organisations to become agile in identifying, assessing and managing emerging and disruptive risks. Following from a similar 2017 survey that focused on the impact of these requirements, KPMG and The Hong Kong Institute of Chartered Secretaries (HKICS) conducted a survey in early 2020 of Hong Kong-based senior management to assess how well risk management has been embedded within businesses in Hong Kong.

As a result of increasing regulatory focus on environmental, social and governance (ESG) issues, including requirements to identify and address ESG-related risks, the survey reveals that more organisations have considered ESG-related risks in the development of business long-term strategy. However, many organisations have yet to fully integrate ESG into enterprise risk management (ERM) and collaborate with business long-term strategy. Furthermore, the survey results suggest that more organisations have formally defined their risk appetite, which is useful in guiding management in the goal-setting and decision-making processes to enhance the chances of achieving specific goals. However, the survey also shows that many organisations are still facing a number of challenges in the actual implementation and rolling out of risk appetite across departments.

The key themes emerging from the survey indicate that businesses need to ensure proper integration of ESG into ERM and business long term strategy and enhance the relevance and sustainability of the ERM exercise to unlock the true value of risk management instead of merely fulfilling regulatory requirements.

This report discusses five key imperatives to help companies develop and implement an effective enterprise-wide risk management framework. A robust framework provides companies with a disciplined business tool to align strategy, processes, people, technology and knowledge to effectively navigate through a complex and rapidly changing environment and, ultimately, remain competitive and successful.

We would like to thank all the survey respondents for their participation and contribution to this initiative.

Alva Lee
Partner, Head of Internal Audit,
Risk & Compliance Services,
Hong Kong
KPMG China

Gillian Meller FCIS FCS
President
HKICS

Message from the Head of Listing, Hong Kong Exchanges and Clearing Limited

Today it is widely recognised that risk management has a positive impact to organisations' business operations and value. The global instability and the COVID-19 pandemic have further highlighted the importance of building risk management and integrating sustainability into business strategy. Amid the pain that the virus has caused, it has also offered business large and small an opportunity to learn and prepare for the future. The social and economic challenges have emphasised the true value of identifying a business' strength and weaknesses, as well as recognising and mitigating material risks. Enshrining ESG principles in business strategy makes a company more agile and better prepared to deal with sudden change.

HKEX, as a gateway to capital markets, is uniquely placed to introduce informed corporate governance and ESG reporting policies for listed companies that are good for markets, good for companies and, ultimately, good for wider society by ensuring the transparency of corporate decisions. We started introducing various corporate governance standards and ESG reporting guidelines nearly 20 years ago, and have been offering guidelines on disclosure and reporting. It is a journey we are committed to for the long term.

While it is clear that policymakers or regulators are in a strong position to drive change, what is more powerful is for the change to come from the top-down within business organisations. The board of directors therefore, need to play a major role – they have the deepest understanding of the goals and motivations of their businesses, the cultures and nuances of their operating markets, as well as a vested interest in the long-term success of their organisations. A board should be expected to step up in driving risks and ESG agenda of their companies. The survey's findings and the guidance provided in the research report echo our belief.

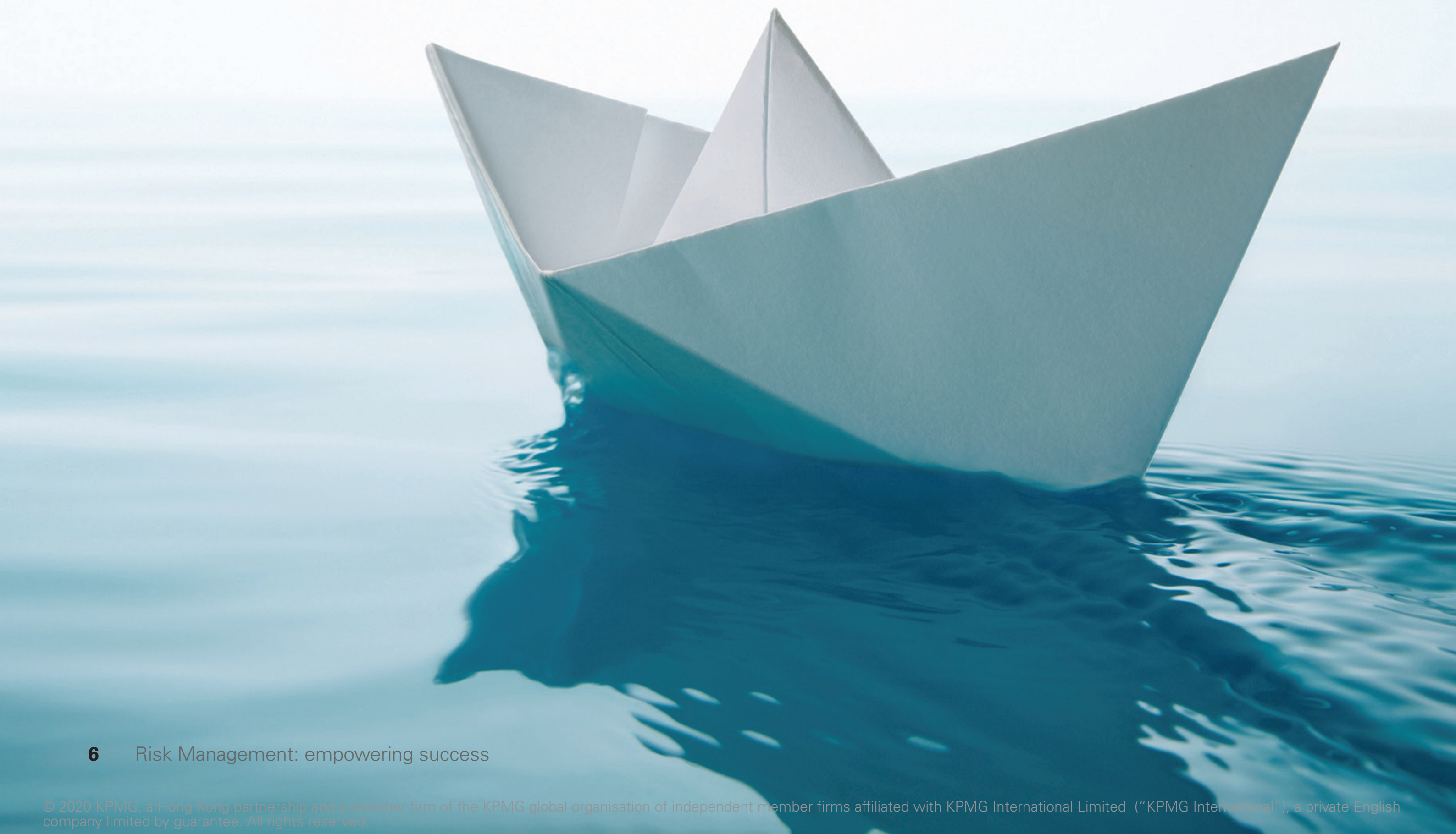
Corporates worldwide are now expected to stay on the front foot and build their resilience to confront far-reaching global challenges. Delivery on risk management and ESG measures is no longer merely a "'nice to do" or "box-ticking exercise": it has become essential for business and societal prosperity, it is demanded by investors and it is considered critical for long-term business success. It is a testimony of how the business is being run and the company's preparedness to challenges.

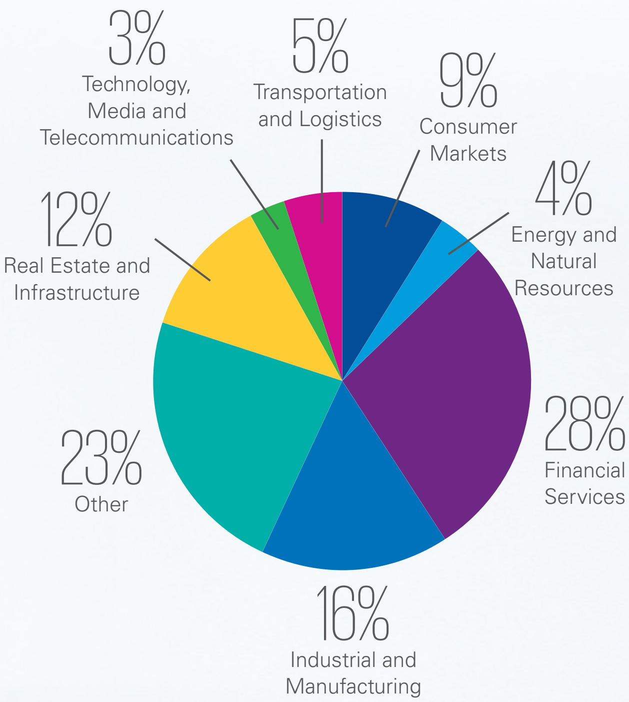
We would like to thank KPMG and HKICS for conducting the survey and producing this research report, which is informative and contains helpful practical advice on enhancing risk management and reporting. We are also encouraged that more organisations had considered ESG-related risk in the development of business long-term strategy with a formally defined risk appetite. This survey will hopefully guide businesses to focus on meeting the increasing interest and demand from investors for decision-relevant information in risk reporting.

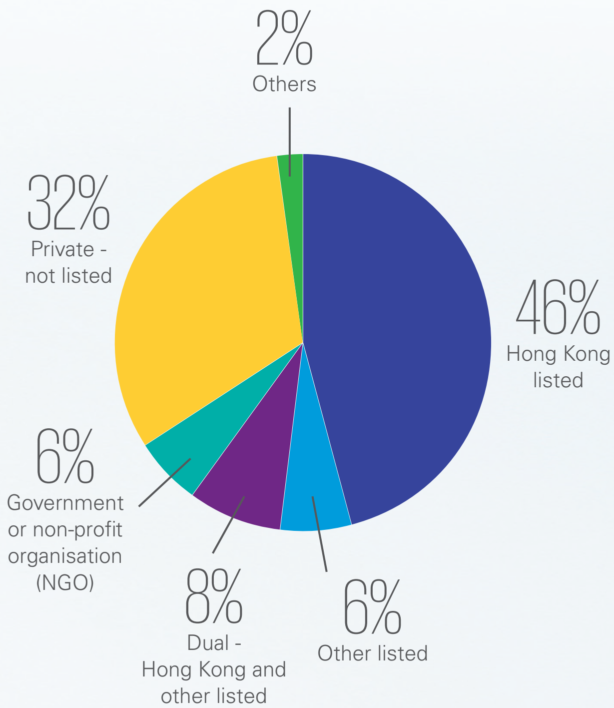
Bonnie Y Chan
Head of Listing
Hong Kong Exchanges and Clearing Limited

About the survey

In Q2 2020, KPMG and The Hong Kong Institute of Chartered Secretaries conducted a survey of Hong Kong-based senior management, focusing on governance of risk management and the risk assessment cycle. Following a similar survey conducted in 2017, this survey aims to focus on how extensive risk management activities have been embedded within businesses. This survey gathered data from 129 respondents across a range of industries and types of organisation:




3%
Technology, Media and Telecommunications
5%
Transportation and Logistics
9%
Consumer Markets
4%
Energy and Natural Resources
12%
Real Estate and Infrastructure
28%
Financial Services
23%
Other
16%
Industrial and Manufacturing


2%
Others
32%
Private - not listed
46%
Hong Kong listed
6%
Government or non-profit organisation (NGO)
8%
Dual - Hong Kong and other listed
6%
Other listed

Risk management trends in Hong Kong

- Increasing regulatory focus on ESG
- Challenges in rolling out of a risk appetite framework
- Addressing emerging risks with agility
- Process-driven risk reporting exercise
- Limited use of technology in risk management

Organisations nowadays realise the importance of risk management. Risk management allows the business to operate smoothly and be prepared for uncertainties they may face. Ideally, an effective enterprise risk management programme can help the organisation make business decisions more confidently as risk management can help build the business's long-term strategy.

Although we see a trend that organisations are starting to embed risk management into business operations to serve as a strategic tool, add value and support growth, a number of organisations still tend to focus on complying with regulatory requirements on risk management. The true value and benefits of robust risk management are still to be unlocked.

In order to assess the maturity of ERM programmes of businesses in Hong Kong, KPMG and The Hong Kong Institute of Chartered Secretaries conducted a survey in 2020 of Hong Kong-based senior management. The survey results highlighted a number of key risk management themes and trends in Hong Kong.

Trend 1: Increasing regulatory focus on ESG

Globally, there has been a growing trend of regulators stressing the importance of ESG and tightening ESG requirements.

Recent ESG requirements formulated by Hong Kong regulators

2018	2019	2020
Since 2018, SFC promotes the strategic framework for Green Finance and also collaborating with overseas regulatory counterparts to consider the development of sustainability practices in the finance sector.	HKMA introduces key measures on sustainable banking and green finance.	HKEx amended the listing rules in 2019 which require all listed companies to publish their ESG reports for financial years starting from 1 July 2020 in accordance with the revised ESG Reporting Guide.

While a number of studies[1] have found that strong ESG performance can create a number of competitive advantages including a more stable investor base, lower cost of capital and better access to financing, improved employee engagement, and customer loyalty, the prevalence of ESG-related risks that may cause significant impact to the organisation has also accelerated rapidly in recent years. Each year, the World Economic Forum publishes the *World Economic Forum's Global Risk Report*[2] to highlight the highest rated risks in terms of likelihood and impact. In 2020, in terms of assessed likelihood, all top five global risks are environmental risks and four out of the top five risks in terms of assessed impact are either societal or environmental risks. However, despite our survey showing that 55 percent of respondents take ESG-related risks into consideration, only 18 percent have fully integrated ESG-related risks into their ERM systems. This finding shows most organisations may not take sufficient consideration of ESG-related risks during the risk management process. ESG-related risks are complicated and new to organisations and by leveraging existing ERM structures, organisations can identify, assess and respond to ESG-related risks. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published a relevant ERM framework to address ESG-related risks in 2018.

[1] 'Five ways that ESG creates value', McKinsey & Company, November 2019, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Strategy%20and%20Corporate%20Finance/Our%20Insights/Five%20ways%20that%20ESG%20creates%20value/Five-ways-that-ESG-creates-value.pdf

[2] 'World Economic Forum's Global Risk Report', World Economic Forum In partnership with Marsh & McLennan and Zurich Insurance Group, 15th Edition, http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

Trend 2: Challenges in rolling out of a risk appetite framework

Setting up a risk appetite statement does not only involve theoretical discussions on the amount of risk that an organisation is willing to pursue. Instead, risk appetite has to be embedded into the business strategy and applied consistently across the organisation. However, our survey finds that many organisations may still find it challenging to incorporate the concept of risk appetite into their strategic planning or decision-making process although the Listing Rules on ERM have been effective for more than four years. Less than 40 percent of respondents have developed a risk appetite statement, communicated throughout the organisation and integrated into the business strategy and decision-making process while 40 percent of respondents have not developed or are still in the process of developing a risk appetite statement. Nearly half of survey respondents replied that they faced challenges in translating their risk appetite for individual risk types into quantitative risk limits. Over 45 percent of respondents struggle to integrate risk appetite into the strategy and 42 percent of them have difficulties in adapting system, policies and reporting to incorporate a risk appetite dimension. The challenges are not insurmountable, and we will share recommendations on how to overcome these challenges in this report. (For more details see "Imperative 2: Implementing Risk Appetite Statement")

Trend 3: Addressing emerging risks with agility

The risk identification process is the first step towards risk management and produces a comprehensive list of risks. The main objective of risk identification is to make early identification of events that may occur in the future that may cause negative impacts to the organisations. Based on our observation, businesses normally perform risk identification annually. This frequency is apparently not sufficient to capture all potential risks, especially emerging risks. Emerging risks can develop instantaneously at any time, causing catastrophic impact to an organisation. Without identifying all risks, organisations cannot make appropriate judgements or formulate any action plan for mitigating the risk. The global spread of COVID-19 and social unrest are good examples to show how disastrous a "black swan" event can be to an organisation. Therefore, in a dynamic business environment, it is crucial for a business to maintain and update a comprehensive risk profile, with wide coverage and proper identification of risks. With a timely risk identification process in place, the organisation can quickly identify risks and efficiently formulate appropriate plans to respond to potential impacts. It also allows management to set the tone at the top, communicate the appropriate risk appetite for different departments to follow and avoid misalignment within the organisation. Therefore, organisations are encouraged to take a more proactive approach to perform risk assessments, including the identification of emerging risks. However, our survey results indicate that organisations are generally reluctant to perform a dynamic risk assessment where:

- Over 80 percent of respondents perceived that their organisations were at least adequately effective in taking action on identified key risks and anticipating and managing emerging risk;
- 14 percent of respondents do not have a risk profile to capture all identified risks; and
- 38 percent of respondents only refresh their risk profile annually.

Trend 4: Process-driven risk reporting exercise

Adopting a sustainable and effective risk management system requires a continuous process of obtaining and sharing necessary information, and forming a holistic and integrated system to manage risk. Without a timely refresh of risk profiles, risk reporting simply provides information based on an existing list of risks that is well-known to management, instead of generating new real-time insights. Risk reporting will become stagnant and merely a "check-the-box" exercise to fulfil regulatory requirements rather than an insightful tool that may lead to questioning by the Board over the values of risk assessment and reporting. Unfortunately, our survey reflects that there is a common mismatch on the frequency of risk assessment and risk reporting. Per our survey results, 56 percent of respondents update the risk level of identified risks on the risk profile at least quarterly whilst only 29 percent refresh the risk profile to identify new or emerging risks faced at least quarterly. Even though quarterly risk report has been made, risk identification has not been timely performed to capture all emerging risks, especially in today's dynamic business environment. Our survey further shows that 11 percent of respondents may think there is a lack of executive buy-in and support for the risk management and 12 percent of respondents have not promoted risk management as a value creating tool.

Although it is good to see that over half of our respondents measure top risks at least quarterly, organisations are encouraged to improve the risk reporting process. Having appropriate tools and measures such as a risk dashboard and key risk indicators (KRI) are important for risk monitoring and reporting. A risk dashboard can extract, integrate, and consolidate data from multiple sources to provide insightful risk information and trends while KRIs can provide an early signal of increasing risk exposures through setting up predetermined thresholds. However, our survey found that only 46 percent of respondents have a risk dashboard in place and only 29 percent have fully incorporated KRIs into their ERM.

Trend 5: Limited use of technology in risk management

To ensure the effectiveness and sustainability of the risk management process, the application of technology with the appropriate capabilities is vital. At the most basic level, most organisations may monitor and manage risks using a simple spreadsheet. However, risk management gets to be more complicated and challenging when the scale of organisations expands, especially for large, complex and geographically distributed organisations. Having the right technology in place can provide a number of benefits throughout the risk management processes. During risk identification process, technology applications may help to process real-time information, particularly for volatile risks such as the global spread of COVID-19, and therefore, reliable and up-to-date information can be obtained efficiently to formulate the corresponding remedial actions. Also, during the risk reporting and escalation processes, risk data can be enormous and complicated, and the use of technology applications allows for a simplified process in consolidating all information collected from different teams. Significant loopholes can also be flagged more efficiently by pre-setting thresholds, escalating to the right people and helping generate more valuable insights for the organisation. However, when comparing the survey result this year with 2017, there is no big improvement in the use of technology for risk management. Results from the current survey show that only 25 percent of respondents use emerging technologies such as big data and analytics while 9 percent in 2017 were extensively using emerging technologies. This survey also reflects that the majority of respondents (67 percent) are still using Microsoft applications to capture, assess and report risk information and half of respondents do not have any plan for using any emerging technologies in their risk management functions.

2020 vs 2017 survey comparison

Top 5 Risks in 2017		Top 5 Risks in 2020
Economic environment	1	Financial risk
Financial (credit, market, liquidity) risk	2	Economic environment/ uncertainty
Regulatory uncertainty	3	Regulatory uncertainty
Cybersecurity	4	Growth and innovation
Talent management	5	Operational risk

Imperative 1:

Integrating ESG into ERM and business long-term strategy

Integrating ESG concerns into business strategies allows companies to capture trends upfront and stay alert to ESG risks in both operations and value chains.

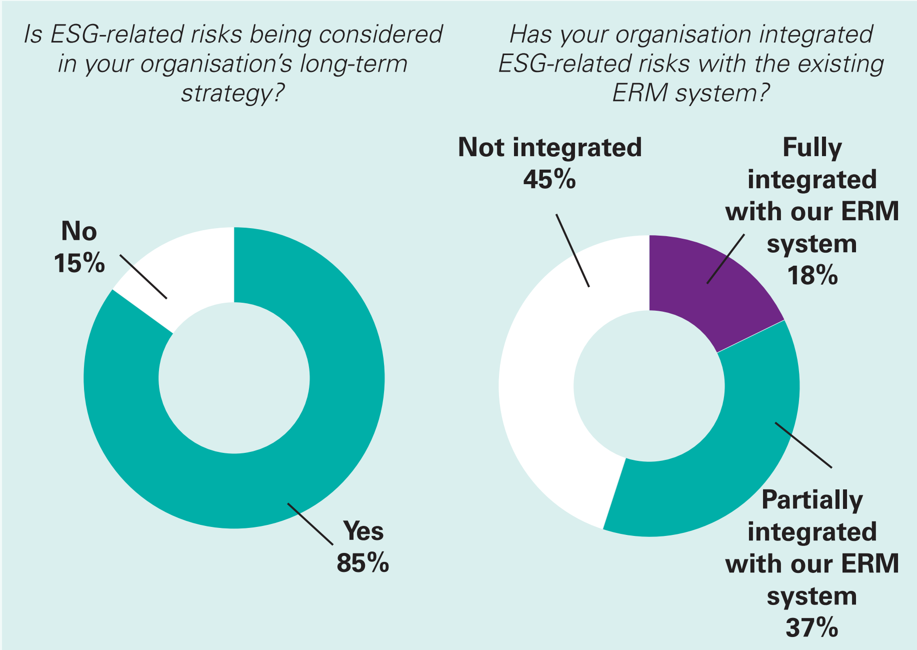
From the survey, it is good to see that there is a great increase in the number of organisations integrating ESG into ERM and business long-term strategy when compared to 2017. As many as 85 percent of respondents consider ESG-related risks in their long-term strategies, which is in line with the trend that ESG has been a major focus for regulators in recent years. Despite this increasing ESG integration, only 37 percent and 18 percent of respondents have partially and fully integrated ESG-related risks into their ERM system respectively. Although many organisations may have strategy, risk and sustainability teams, those teams mostly work in silos with minimum or limited collaboration failing to create a shared responsibility for risk ownership and develop innovative solutions to address ESG-related risks. Without a successful ESG integration, a comprehensive view of risks faced and the respective impact on the ability to deliver on strategic priorities may not be properly identified or illustrated. For risk management function, there may be a lack of subject matter experts in ESG to take ESG-related risks into consideration when formulating a risk management statement. This may lead to challenges in integrating ESG elements into risk management functions and the management of ESG risks may become a standalone compliance requirement. Organisations are expected to take a more proactive approach to manage ESG matters in response to the increasing expectations from regulators and investors.

2020 vs 2017 survey comparison

To what extent has your organisation adopted or is considering an ERM programme?

Have a partially or fully integrated ERM programme

2020 survey result



Recommendations

ESG-related risks that most organisations tended to neglect in the past have become more common and their impact and likelihood have become more significant in recent years. For example, with the increasing emphasis on green and sustainable banking, organisations' performance in ESG is likely to have an impact on their credit rating and ability to obtain financing. In addition, expectations from regulators and investors on how an organisation manages ESG issues have intensified in Hong Kong. Regulators have implemented stricter regulations on ESG while investors expect organisations in every industry to dedicate efforts to cope with ESG-related issues. Therefore, organisations can no longer ignore the impacts of ESG-related issues and should incorporate ESG into their long-term strategy and ERM framework.

The first step to integrate ESG into business is to set a common ground where the organisations and its key stakeholders can agree on the definition of ESG and its importance to the organisation. This common ground is essentially composed of different elements which allow the environment to nurture its ESG development.

Setting the tone at the top

- A top-down approach can greatly facilitate the ESG integration process of the organisation. The tone at the top sets forth the guiding principles, values and ethical climate of an organisation. If the tone set by the Board and management upholds the importance of ESG-related issues, the organisation will be more inclined to uphold the same values.
- From our survey results, despite that 85 percent of respondents considered ESG-related risks in their long-term strategy, only 31 percent have included ESG in the regular Board agenda. To fully integrate ESG into ERM and long-term strategy, it is vital for the Board to regularly discuss ESG matters to ensure proper attention.

- It is also important that the Board and management should have adequate understanding regarding the values and relevance of ESG-related issues to their business. Having their buy-in and support is fundamental to integrate ESG into the discussions on ERM.

Agreeing on a common language

- It is essential for the organisation to agree on a common language between cross-functional teams, make sure all key stakeholders are clear about ESG-related issues when working on ESG integration and facilitate regular exchanges of information between the Board and cross-functional teams.
- To enhance collaboration between cross-functional teams, different stakeholders such as risk management and subject-matter experts may work together to find the common language to discuss ESG-related issues. Cross-functional committees may be formed so that skills can be shared or transferred during the collaboration, which can then support ESG integration.

Risk assessment and measurement

- Tailoring risk assessment criteria, in terms of impact and likelihood, is important for assessing and prioritising resources for different types of risks, including financial, strategic, operational and ESG risks. It is also important to consider how ESG-related risks can be incorporated into current ERM process.
- As effective management of ESG-related risks requires input from professionals, obtaining advice or insights from experts on ESG topics and potential risk responses, such as physical risks and transition risks of climate change, may be helpful.

Risk reporting

- To facilitate collaboration between cross-functional teams, effective internal reporting channels are vital for exchanges of information and aligning understanding of all functions. They include regular escalation to the Board on risk management updates to provide a holistic view regarding risks faced by the organisation.
- External reporting includes annual reports, risk management reports and ESG reports. Ensuring consistency of information presented is essential and can prevent confusion caused to different stakeholders.

With heavier emphasis on ESG around the globe, organisations' ESG performance has been placed under the spotlight over the past years. Stronger ESG performance has been proven to be beneficial in enhancing organisations' competitive advantages.

Integrating ESG into ERM and business long-term strategy would allow organisations to better deal with ESG risks and strengthen their competitiveness.

Pat Woo
Partner, Business Reporting and Sustainability, KPMG China

Imperative 2:

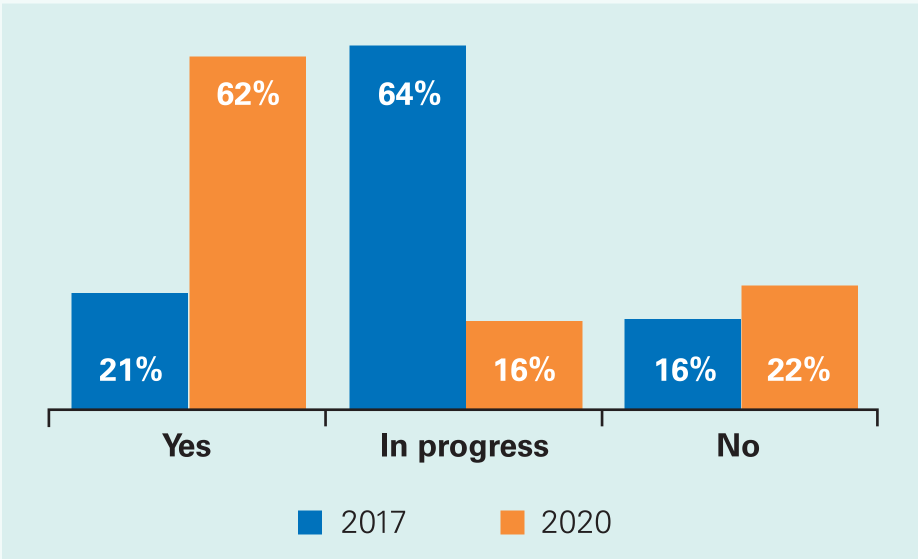
Implementing a risk appetite statement

COSO defines the risk appetite as "the types and amount of risk, on a broad level, an organisation is willing to accept in pursuit of value". A practical risk appetite statement has emerged in recent years as an essential component of the ERM Framework that can guide management in the goal-setting and decision-making processes to enhance the chances of achieving its goals and sustaining its operations. A good risk appetite framework can help management understand the organisation's risk profile and, at the same time, strike an appropriate balance between risk and return and cultivate a healthy risk culture. It is also emphasised that risk appetite applies to all organisations aiming to better understand and manage risk exposure, not limited only to the financial services industries.

Over the last several years, regulators in Hong Kong have demanded stricter requirements on risk management. For example, according to the *Guidance for Boards and Directors* issued by HKEx, when the Board discusses long-term strategic objectives, it should consider the organisation's risk appetite, risk and return trade-offs and risk management system. This is reflected in the current survey results that 62 percent of respondence have already developed a defined risk appetite in their organisations while in 2017 only 21 percent had a fully developed and implemented risk appetite statement. This is a good start to see more organisations formally defining their risk appetite.

2017 vs 2020 survey comparison

Does your organisation have a defined risk appetite statement and / or risk tolerance level?



Recommendations

Despite the abovementioned improvement, our survey also finds out that many organisations are still facing a number of challenges in the actual implementation and rolling out of risk appetite statements across departments, including consistent interpretation across the organisation, integrating risk appetite into strategy, adapting system, policies, procedures and reporting to incorporate risk appetite dimension and translating the risk appetite for individual risk types into quantitative risk limits. To address the challenges, businesses could consider the following:

To successfully implement a risk appetite statement and foster its consistent understanding throughout the organisation, often a cultural change in identifying, assessing and managing risks is inevitable. Buy-in throughout the organisation can be enhanced by pragmatically combining a top-down and bottom-up approach, which also facilitates planning to reach the desired goals.

Jens Kessler
Director, Risk Consulting, KPMG China

Consistent interpretation across the organisation

When risk appetite statements and strategy are formulated, management should clearly communicate across different functions in the organisation. Management should not rely too much on technical reports but it is crucial to cascade risk appetite throughout the organisation and provide guidance to operational functions. Facilitated discussion can be an effective tool to align the strategies and objectives of different teams, while training or workshops can also be organised to ensure that there is a consistent understanding on risk appetite. All these are useful in determining whether business units are pursuing wrong objectives or taking up too much risk in pursuing established strategies and objectives.

Integrating risk appetite into strategy

Integrating risk appetite into strategy allows the determination of level of risk associated with a strategy. The start of integration can be simple and involves in-depth discussions between the Board and management regarding the organisations' risk-taking strategy. The next step requires the establishment of risks measures such as risk appetite, risk tolerance and risk profile. It is crucial for the Board and management to understand the interplay of strategy and risk appetite.

Adapting system, policies, procedures and reporting to incorporate a risk appetite dimension

Setting up risk appetite and embracing it is not a one-off exercise. The review and revision of relevant process and documentation may begin with discussions among management regarding the external environment such as the regulatory environment, macroeconomic environment and prospects. Management may also adopt an objective-based approach, which cascades into risk considerations and closely ties to business strategy.

Translating risk appetite for individual risk types into quantitative risk limits

Parameters for measuring risk limits are important as they can impact the decision-making and strategic planning processes. A predetermined parameter can be viewed as a framework showing the goals and objectives that can facilitate the discussion between the Board and management. Parameters may be expressed as targets, ranges, upper or lower limits and categorised into different areas, such as strategic, financial, operational and regulatory compliance, etc.

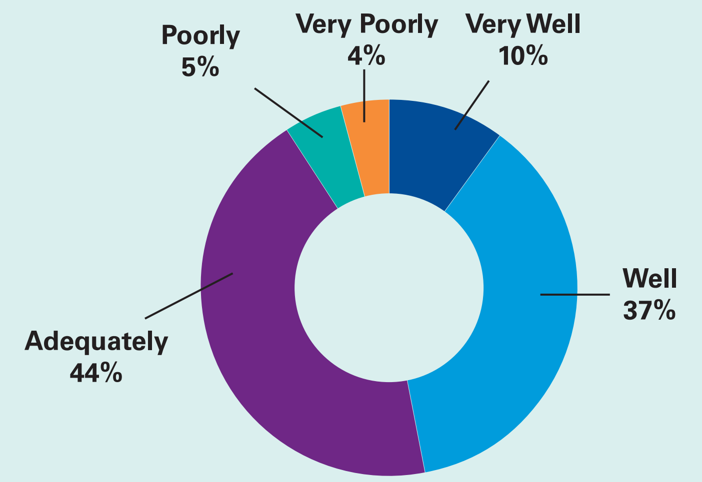
Imperative 3:

Maintaining dynamic risk assessment

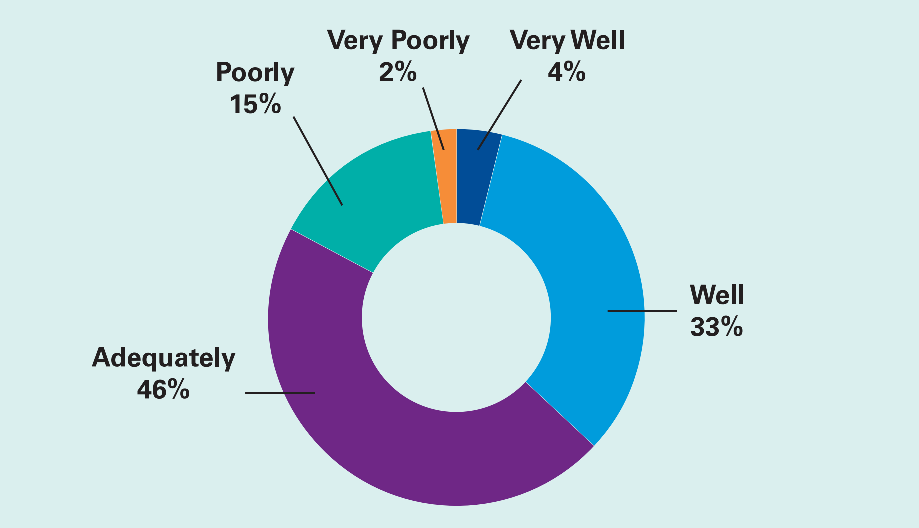
Value is a function of risk and return and risk can be interpreted as a fundamental part of the pursuit of value. Therefore, risk assessment is crucial for an organisation to identify and evaluate the impact of risks on the achievement of its goals. To achieve this, organisations need a risk assessment process that is practical and sustainable, especially in a dynamic business environment where emerging risks can develop instantaneously and cause hazardous impact to the organisations. While we observed that the majority (82 percent) of our respondents have at least a partially integrated ERM programme and over 80 percent say their organisations have taken at least adequately effective actions on identified key risks and anticipating and managing emerging risks, our survey result further reflects that 14 percent of respondents do not have a risk profile and 38 percent only refresh their risk profiles annually. This finding shows that organisations may be reluctant to perform a dynamic risk assessment. However, to unveil the full value of a risk management framework, it is crucial for organisations to develop a continuous risk assessment so that all risks, including emerging risks, can be captured in the framework. With an up-to-date list of risks maintained, more meaningful risk reports can be generated which can provide more valuable insights for management. The following case study highlights the key steps performed by an organisation to overcome the COVID-19 incident by making use of the dynamic risk assessment.

2020 survey result

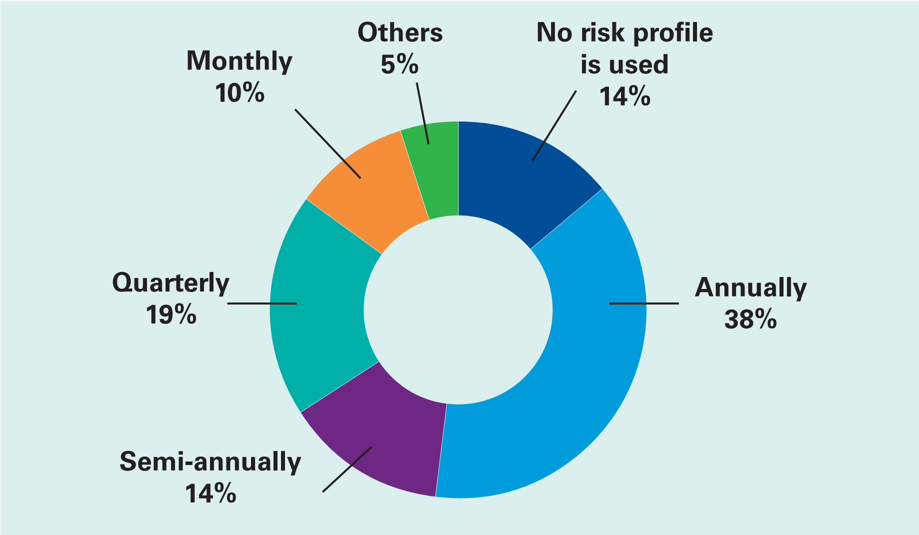
How would you rate the effectiveness of your organisation in taking actions on identified key risks?



How would you rate the effectiveness of your organisation in anticipating and managing emerging risks?



How often does your organisation refresh the risks profile including emerging risks identified?



Company secretaries are a go-to resource, and increasingly approached by businesses to facilitate enterprise risk management. They also contribute to dynamic risk assessment through their understanding of business concerns, the culture of an organisation and their ability to bring different moving parts together. Further, they are instrumental in facilitating director inductions and training on the topic as part of their applied governance functions.

Ms Edith Shih FCG(CS, CGP) FCS(CS, CGP)(PE)
Immediate Past International President, The Chartered Governance Institute
Past President, The Hong Kong Institute of Chartered Secretaries
Executive Director and Company Secretary, CK Hutchison Holdings Ltd

Case Study

In recent months, COVID-19 has had unprecedented impact that has become a significant threat to the existence of many businesses. Operations have been disrupted as organisations are unable to deploy people effectively and supply chains are being tested to an extreme extent. Under such an emerging risk, a continuous risk assessment is crucial for an organisation to timely identify all potential risks associated with COVID-19 and to formulate proper action plans to mitigate the risks. In this case study, the organisation made use of a timely risk assessment to identify all potential risks and tried to formulate practical action plans to cope with COVID-19 during these turbulent times.

Step 1: Identifying key risks

While the annual refreshing of the risk profile has been a common practice for most organisations, the organisation made good use of a timely risk assessment to identify and review key risks associated with COVID-19 across its operations and supply chains. It also agreed on which source of information could provide insight during the incident. Examples of the risks identified include cybersecurity risks and capability and capacity of work from home arrangements.

Step 2: Setting the tone at the top

With key risks identified and assessed in a timely manner, the organisation created a proper governance structure to allow the Board and senior management to make key decisions efficiently. They could make use of the results from risk assessments and formulate appropriate action plans for the whole organisation. For instance, through assessing the capability and capacity for staff to work from home, the Board and senior management could promptly implement work from home arrangement for the entire organisation.

Step 3: Communicating with key stakeholders

After mitigating actions were agreed at the Board and senior management level, the organisation communicated with key stakeholders and determined key action owners and supporting resources. The mitigation plan was effectively communicated across the whole organisation to avoid misalignment.

Step 4: Enhancing risk management practices

The key decisions and action plans were logged, and the effectiveness of each action was closely monitored. The organisation enhanced its risk management framework through leveraging the leading practice from its peers.

Imperative 4:

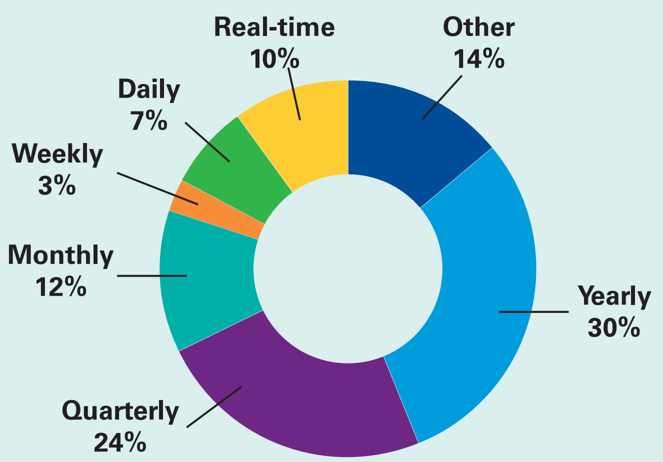
Enhancing risk reporting efficiency and effectiveness

After timely and accurately identifying risks, continuous risk reporting and monitoring are the next pain points that many organisations face.

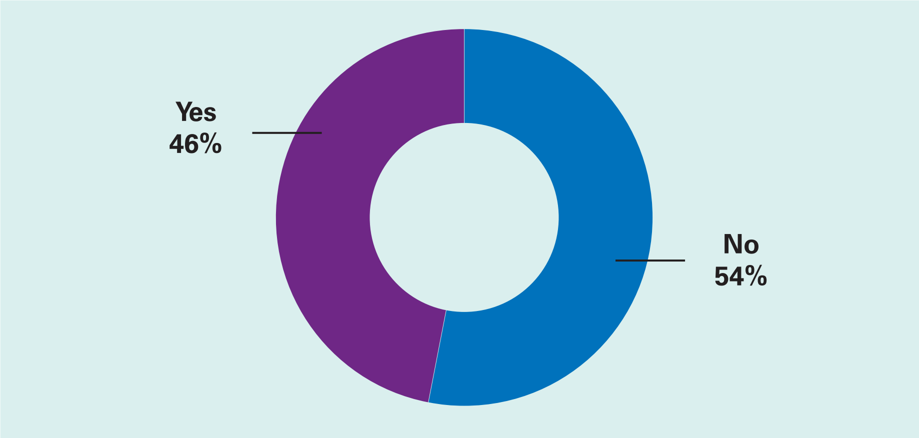
COSO has highlighted the importance of risk reporting in its COSO ERM Framework as "(r)eporting supports personnel at all levels to understand the relationships between risk, culture, and performance and to improve decision-making in strategy and objective setting, governance and day-to-day operations." From the survey, it is good to see that more than half of our survey respondents (56 percent) measure risk at least quarterly, however, appropriate measurement and reporting tools are also crucial to generate valuable insights from the raw risk data, help the management to better understand and assess the risk profile of the whole organisation. Our survey shows that most organisations may not have sound mechanisms or tools in place to measure and report risks. Less than half of our survey respondents (46 percent) have implemented risk dashboards for measuring and reporting purposes, implying that most organisations are still relying on the traditional reporting approaches that contain mainly tables and static charts. It may not be problematic at the start of risk management but when the scale of risk assessment expands and risk data gets more complicated, the traditional reporting may not be an ideal approach due to the challenges in gathering and visualising all the risk data. Without a dashboard view presenting a summarised view of risks and controls, users may find it difficult to efficiently identify exceptions and perform deep-dive analysis. To enhance risk reporting efficiency and effectiveness, organisations may consider adopting risk dashboards for risk reporting purposes.

2020 survey result

What is the frequency of measuring risks?



Does your organisation implement risk dashboards for risk monitoring and reporting processes?



How does a risk dashboard report work?

Data source

The risk dashboard can identify all systems containing the required attributes to produce reports, such as KRI management reports. It does not only include risk data from internal systems, instead other manually generated files or data sourced from external systems will also be included in the risk dashboard to establish a comprehensive database.

Data integration

Data from all source systems are integrated in the risk dashboard. It helps to consolidate all risk data and data quality issues are handled in this stage by implementing data rules. Other data anomalies are rejected in an exception table for further cleansing and processing.

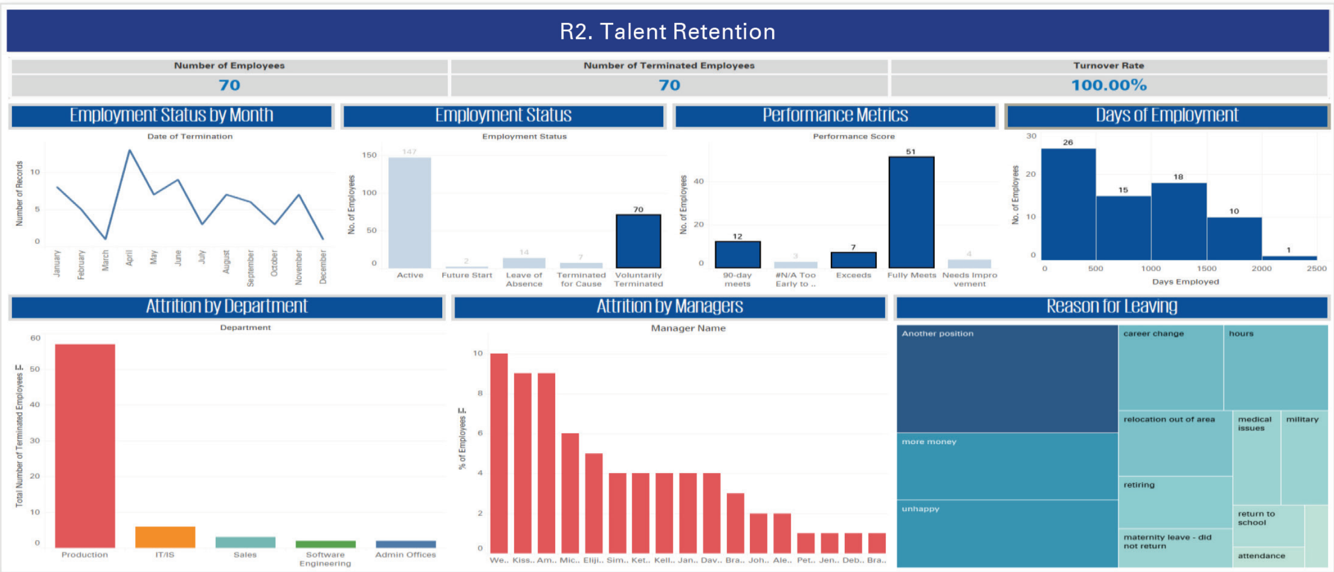
Reporting layer

The dashboard will be automatically refreshed to present risks in an interactive manner and monitor indicators (e.g. KRI) on an ongoing basis. It allows the Board and senior management to focus on the most critical risk areas and facilitates enhanced decision-making based on up-to-date risk information. Some examples of dashboard reports are shown below:

In view of the growing volume of corporate data, the use of risk reporting dashboard enhances effectiveness of risk analysis and presentation to top management. It facilitates the evaluation of alignment between the overall entity performance and overall business strategy. Moreover, efficiency of reporting can be strengthened with the use of centralised reporting tools.

Samantha Suen FCIS FCS(PE)
Past President, HKICS


Risk Dashboard
Dashboard
Group
Entity 1
Entity 2
Entity 3
Ent. Risk Mgmt. (ERM)
Group
Risk Inventory
Risk Parameters
Risk Registers
Risk Appetite
KRIs Monitoring
Reporting
Alerts
Entity 1
Risk Inventory
Risk Parameters
Group Key Risks
No Category Key Risk Lead Risk Owner(s) Residual Target
R1 Strategic Strategic Direction Risk CEO High High
R2 Strategic Changes in Government Policy CEO High High
R3 Operational Talent Attraction & Retention Risk HR High High
R4 Operational Workplace Health and Safety Risk HR High Medium
R5 Operational Brand Erosion Risk Head of Marketing Medium Low
R6 Operational Fraud and Corruption Risk BU Heads Low Low
R7 Compliance Regulatory Non-Compliance CCO Medium Medium
R8 Technology Cybersecurity Risk Head of IT Very High Medium
R9 Technology IT Infrastructure Risk Head of IT High Medium
Risk Ratings for Key Risks
Likelihood of Occurrence
Magnitude of Impact
Control Strength
90 Control in Document
Strong 80%
Moderate 18%
Weak 2%
Control Sources of Assurance
Mgmt. Assurance
Independent Assurance
CSA Performed 78%
Internal Audit Performed 47%
Other Assurance 13%
Action Plans
New Controls
Enhance Existing Controls
On Track to Complete
Delayed in Implementation
Completed in Last 6 Months
Key Risk Indicators
14 KRI follow-up actions
Last Collected on March 2019
Green
Amber
Red
Not Due
Key Tolerance
15 tolerance metrics
Breaches in Risk Tolerance
Management's View


R2. Talent Retention
Number of Employees
70
Number of Terminated Employees
70
Turnover Rate
100.00%
Employment Status by Month
Employment Status
Performance Metrics
Days of Employment
Attrition by Department
Attrition by Managers
Reason for Leaving
Another position
career change
hours
more money
relocation out of area
medical issues
military
retiring
unhappy
return to school
maternity leave - did not return
attendance

Imperative 5:

Deploying Integrated Risk Management solutions in risk monitoring and reporting

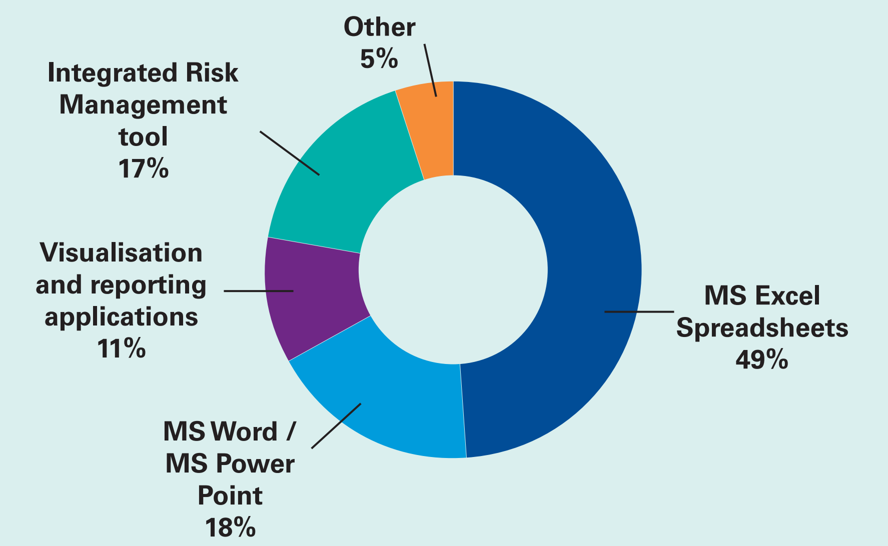
An effective risk management framework should provide management with an enhanced ability to capture, evaluate, analyse and respond to risks continuously. With the advent of technology, risk management is highly influenced by this evolution due to the reliance on risk data. While taking advantage of technologies should have been a global trend in recent years, our survey shows that the majority of our respondents still use manual ways to capture, assess and report risks. Some 67 percent of respondents are still using Microsoft Office and only 17 percent of respondents have implemented Integrated Risk Management (previously commonly known as GRC) tools for risk management.

Although simple spreadsheets may be sufficient for an organisation to start working on a risk management framework, it will be more challenging when the risk data gets larger and more complex. Organisations are constantly exposed to an endless flow of data from the ever-growing number of data collection points. Data monitoring and reporting tools become more important due to the increasing volume, velocity, variety and veracity of data. Therefore, relying only on a spreadsheet is difficult to generate insightful reports for management and organisations may encounter the following challenges given the lack of risk monitoring and reporting solutions:

- **Silos of data:** It is difficult for different departments to share common information if no centralised tools have been adopted. If the data is siloed, relevant connections between siloed data, which may provide insightful information, can easily be missed. Consequently, due to the lack of a holistic view of risk data, the organisation will face challenges in interpreting data accurately and formulating appropriate action plans.
- **Unscalable data repository platform:** As mentioned above, organisations are now facing increasing volume, velocity and variety of risk data. The existing data repository platform may not be scalable enough to support the exponential growth of data within an organisation.
- **Lack of insightful management reporting:** The use of spreadsheets to manage and analyse data may constrain management reporting activities. The spreadsheets may only provide simple analysis over risk data such as static charts and tables. When risk data become larger, it becomes hard for spreadsheets to capture the holistic picture and transform the data into insightful management reporting.

2020 survey result

Which of the following best describes the technology used to capture, assess and report risk information in your organisation?



Recommendations

To address the challenges, organisations may consider integrating technology into their risk monitoring and reporting processes to provide more powerful analysis. Integrated Risk Management is the combination of people, processes and technology to gather and aggregate risk information across the organisation in a manner that focuses management's attention and remediation in a timely manner. It is aimed at collaboration and synchronisation of information and activities. Organisations may consider deploying IRM solutions to align the Integrated Risk Management processes.

1. Ability to obtain an **overview of risks** at the enterprise level and the respective entity level
2. Ability to obtain a **summary of risk management** activities (i.e. controls, action plans, key risk indicators)
3. **Input / updates directly by domain experts** (e.g. controls performed directly by front line), thus providing clearer understanding of roles and responsibilities across the organisation
4. **Analysis of trends** (i.e. key risk indicators, risk tolerance) in a timely manner (e.g. real-time)
5. **Integration with existing risk management process** (i.e. replace tools and templates integrates seamlessly into the system)
6. **Integration with assurance processes and activities** (i.e. control self-assessment, internal audit, external audit)
7. **Integration with other organisational processes** (i.e. HR systems, procurement system) for monitoring

Data collection consolidation

An Integrated Risk Management solution is a centralised system which can collect and store results instead of dispersing the information across departments separately. All actions taken and associated results can be shared across different departments, allowing the alignment of the organisation's governance, risk and compliance processes across the three lines of defence. For example, internal audit and compliance departments can leverage risk assessment results provided by the first line of defence on Integrated Risk Management solutions. Integrated Risk Management solutions can further prevent duplication of work as departments can share risk data and results, allowing more effective reallocation of resources to better address other risk issues.

Apply consistent framework

Since the Integrated Risk Management solution is a centralised system, a common risk strategy and methodology can then be applied in a consistent framework. Following the same Integrated Risk Management framework, the alignment for greater consistency or risks and control assessment, as well as the risk reporting, can be enhanced. It helps to create consistency across the organisation so that everyone can produce consistent results using the same risk data.

Tailor-made Integrated Risk Management solutions

There are specialist Integrated Risk Management vendors that provide tailor-made Integrated Risk Management solutions to clients. To enhance the effectiveness of programmes, ERM processes and users should drive the requirements and implementation of technology solutions. On the other hand, some organisations can opt for modular solutions that allow a phased and flexible implementation. A modular solution is competitively priced compared to a tailor-made solution, yet it allows clients to pick and choose the modules they want and are ready to implement and create a bespoke solution according to their needs. As it is available for use off the shelf, the modular solution can also be implemented rapidly and configured to clients' needs within weeks.

The benefits of deploying Integrated Risk Management solutions include the effective capture and manipulation of risk data, visualised through powerful and insightful management reporting, ultimately supporting a sustainable approach towards governance, risks, and controls management. It facilitates the transformation of the risk management programme from a siloed to an integrated approach that is more proactive and strategic.

Jeffrey Hau
Partner, Risk Consulting, KPMG China

Conclusion

Our survey results show great improvement in the risk management processes of organisations, including heavier emphasis on ESG-related risks.

To optimise the benefits of risk management, organisations should become more agile in responding to emerging and disruptive risks, particularly in a dynamic business environment. An integrated approach can be adopted to ensure ESG has been taken into consideration in ERM and business long-term strategy. A well-defined risk appetite statement helps identify scenarios requiring management attention, which should be escalated through an effective risk reporting protocol. The protocol allows timely escalation and responses to disruptive risks, as well as single source of risk information being communicated. Last but not least, Integrated Risk Management solutions should be implemented to provide insights to resolve challenges and facilitating improvements in the process.

About KPMG

KPMG China is based in 26 offices across 24 cities with around 12,000 partners and staff in Beijing, Changsha, Chengdu, Chongqing, Foshan, Fuzhou, Guangzhou, Haikou, Hangzhou, Jinan, Nanjing, Ningbo, Qingdao, Shanghai, Shenyang, Shenzhen, Suzhou, Tianjin, Wuhan, Xiamen, Xi'an, Zhengzhou, Hong Kong SAR and Macau SAR. Working collaboratively across all these offices, KPMG China can deploy experienced professionals efficiently, wherever our clients are located.

KPMG is a global network of professional services firms providing Audit, Tax and Advisory services. We operate in 147 countries and territories and have more than 219,000 people working in member firms around the world. The independent member firms of the KPMG network are affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. Each KPMG firm is a legally distinct and separate entity and describes itself as such.

In 1992, KPMG became the first international accounting network to be granted a joint venture licence in mainland China. KPMG China was also the first among the Big Four in mainland China to convert from a joint venture to a special general partnership, as of 1 August 2012. Additionally, the Hong Kong firm can trace its origins to 1945. This early commitment to this market, together with an unwavering focus on quality, has been the foundation for accumulated industry experience, and is reflected in KPMG's appointment for multi-disciplinary services (including audit, tax and advisory) by some of China's most prestigious companies.

About KPMG IARCS

KPMG's Internal Audit, Risk & Compliance Services (IARCS) deploys services to make internal audit functions, enterprise risk management and compliance programmes, and risk and control management more efficient and effective. The internal audit function and risk and control management are often at the forefront in dealing with these matters. Their effectiveness and efficiency can have a major influence on corporate performance and business outcomes.

Our services include addressing topical issues for business leaders across a range of complex matters:

- Enterprise risk management (structure, risk identification, monitoring, reporting, optimising)
- IA strategic sourcing (right resources, right place, right time)
- Corporate governance
- Regulatory compliance
- Board advisory services
- Contract compliance
- Continuous auditing/monitoring
- Integrated assurance

About HKICS

The Hong Kong Institute of Chartered Secretaries (HKICS) is an independent professional body dedicated to the promotion of its members' role in the formulation and effective implementation of good governance policies, as well as the development of the profession of Chartered Secretary and Chartered Governance Professional in Hong Kong and throughout the mainland of China (the Mainland).

HKICS was first established in 1949 as an association of Hong Kong members of The Chartered Governance Institute (CGI), formerly known as The Institute of Chartered Secretaries and Administrators (ICSA) of London. It was a branch of CGI in 1990 before gaining local status in 1994 and has also been CGI's China Division since 2005.

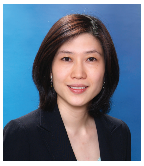
HKICS is a founder member of Corporate Secretaries International Association (CSIA), which was established in March 2010 in Geneva, Switzerland. In 2017, CSIA was relocated to Hong Kong where it operates as a company limited by guarantee. CSIA aims to give a global voice to corporate secretaries and governance professionals.

HKICS has more than 6,000 members and 3,200 students.

For more information, please visit www.hkics.org.hk.

Contact us

KPMG contacts



Alva Lee
Partner, Risk Consulting
KPMG China
T: +852 2143 8764
E: alva.lee@kpmg.com

Jia Ning Song
Partner, Financial Services Advisory
KPMG China
T: +852 2978 8101
E: jianing.n.song@kpmg.com

Jeffrey Hau
Partner, Risk Consulting
KPMG China
T: +852 2685 7780
E: jeffrey.hau@kpmg.com

Jens Kessler
Director, Risk Consulting
KPMG China
T: +852 2143 8584
E: jens.kessler@kpmg.com

Paul Cheng
Director, Risk Consulting
KPMG China
T: +852 2847 5075
E: paul.cheng@kpmg.com

Claudia Yu
Director, Risk Consulting
KPMG China
T: +852 2685 7898
E: claudia.yu@kpmg.com

HKICS contacts

Ellie Pang
Chief Executive
T: +852 2830 6029
E: ellie.pang@hkics.org.hk

Mohan Datwani FCIS FCS(PE)
Deputy Chief Executive
T: +852 2830 6012
E: mohan.datwani@hkics.org.hk

Kenneth Jiang FCIS FCS(PE)
Chief Representative
Beijing Representative Office
T: +86 (10) 6641 9368, ext. 668
E: kenneth.jiang@hkics.org.hk

kpmg.com/cn/socialmedia

For a list of KPMG China offices, please scan the QR code or visit our website:
https://home.kpmg.com/cn/en/home/about/offices.html

Publication number: HKRC20-0001

Publication date: November 2020