KPMG

The Journey to ERM 2.0

A Guide for the Public Sector in Singapore

Contents

KPMG

Foreword

Many Public Sector organisations in Singapore today have done very well in implementing and sustaining an Enterprise Risk Management (ERM) framework over the years.

ERM is not a static exercise but a continuous journey to improve an organisation's ability to anticipate and manage its risks.

This publication shares trends and the evolution of risks and risk management practices, as well as key insights, into how Public Sector organisations can continuously improve and mature their ERM practices.

Our inputs tap on KPMG's extensive experience through the years partnering the Public Sector in Singapore to provide practical guidance and considerations to unlock further value from ERM as a programme.

We also provide perspectives on the latest ERM initiatives and activities that organisations have started to embark on both globally and in Singapore.

It should be noted that there is no 'one size fits all' ERM programme. ERM is best tailored to the context of your organisation, taking into account factors such as size, nature of operations, resources available, among others.

We hope that this publication provides readers insights on charting a sustainable ERM journey where continuous reinforcement and improvement remain central cornerstones of the programme.

Introduction

Objectives

The risk landscape is changing. Organisations today are faced with increasing and evolving risks from various sources. In addition, demands for greater governance and transparency are growing, both from regulators and the public-at-large.

In this publication, we share insights with Public Sector Organisations in Singapore on:

- ERM practices, maturity and focus areas in the Public Sector in Singapore today
- Latest ERM trends and good practices globally and in Singapore
- Tips, considerations and guidance when taking the next steps in the ERM journey
- How Public Sector organisations can build a practical ERM roadmap focused on continuous improvement

This publication takes reference from local and global risk management and governance standards, including:

- ISO31000: 2018
- COSO ERM (2017)
- Board Risk Committee Guide 2016

Statutory regulations and legislations should take precedence over the guidance provided in this publication as applicable.

References, guidance and considerations provided are not meant to be prescriptive or exhaustive. A sustainable and effective ERM programme should be tailored to individual organisations, taking into consideration organisational objectives, resources, structure and context.

Quick View of the Latest ERM Standards

COSO

The COSO ERM Framework was updated in 2017, outlining key considerations and emphasis on ERM from a strategic perspective. Some insights from this latest COSO publication include providing greater clarity and alignment with the business landscape (e.g. growing value proposition of Information Technology in the digital age today) as well as the importance of integrating ERM with strategy and performance management. The 2017 version also re-emphasises and acknowledges the critical role of culture in ERM.

ISO31000

First published in 2009, the ISO31000 has been used widely as a reference by many organisations to guide ERM efforts. The 2018 update reiterates the key principles set out in the original publication and lends additional focus to the following areas:

- Integration of risk management into all aspects of the organisation's activities, starting with governance, including oversight by top Management personnel
- Importance of clear and effective communication and consultation when dealing with stakeholders
- Emphasis on continuous improvement as the key to effectively managing risks, including a stronger focus on maintaining an open and principle-based approach to managing risks
- Customising risk management to the individual specific needs and requirements of each organisation

ERM 1.0 vs ERM 2.0

In the first few years of an organisation's ERM journey, the focus should remain firmly on establishing the foundations of a sustainable ERM programme, or what is termed as 'ERM 1.0'. The key objectives at this stage should typically include:

- Establishing a clear and defined framework, including ERM objectives, governance structure, roles and responsibilities
- Structured process to identify, assess, monitor and refresh key risks to the organisation with involvement from senior stakeholders
- Protocols in place for periodic risk reporting to Senior Management and Board levels, including reporting frequency, content and responsibilities
- Sound risk awareness and understanding across all stakeholder groups within the organisation

As organisations mature beyond the foundations set out in 'ERM 1.0', the focus should progressively shift towards the following key features of 'ERM 2.0':

- Unlocking further value of risk management to support strategic and operational decision-making processes
- Continuously driving efficiency in ERM processes
- Exploring new perspectives in risk identification and assessment efforts to reduce risk 'blind spots'
- Adopting a data-driven approach to risk management for enhanced precision in risk assessments and timeliness in risk monitoring
- Risk management well embedded in day-to-day operations, mind-set and behaviours of stakeholders across the organisation

ERM Maturity in the Public Sector

KPMG

The concept of ERM is not new to the Public Sector in Singapore. From KPMG's experience, most Public Sector organisations have achieved good success in implementing and sustaining an ERM programme over the years. At the same time, Public Sector organisations are constantly exploring ways to further drive effectiveness and efficiency in their ERM programmes. Some of the common feedback on areas of improvement from senior stakeholders include:

"We need to look beyond ERM as an academic exercise…"

"How do we minimise the 'blind spots' we are facing?"

"How can we monitor risk on a more real-time basis?"

"…Helping Board and Management to focus on 'what matters'…"

"Need to embed risk thinking in operations and culture…"

"…Driving efficiency through technology… but we must not be 'slaves to technology'…"

Note: Quotes have been para-phrased for the purposes of publication

Figure 1 summarises the typical ERM areas where Public Sector organisations do well. It also covers components which may not yet be in common practice:

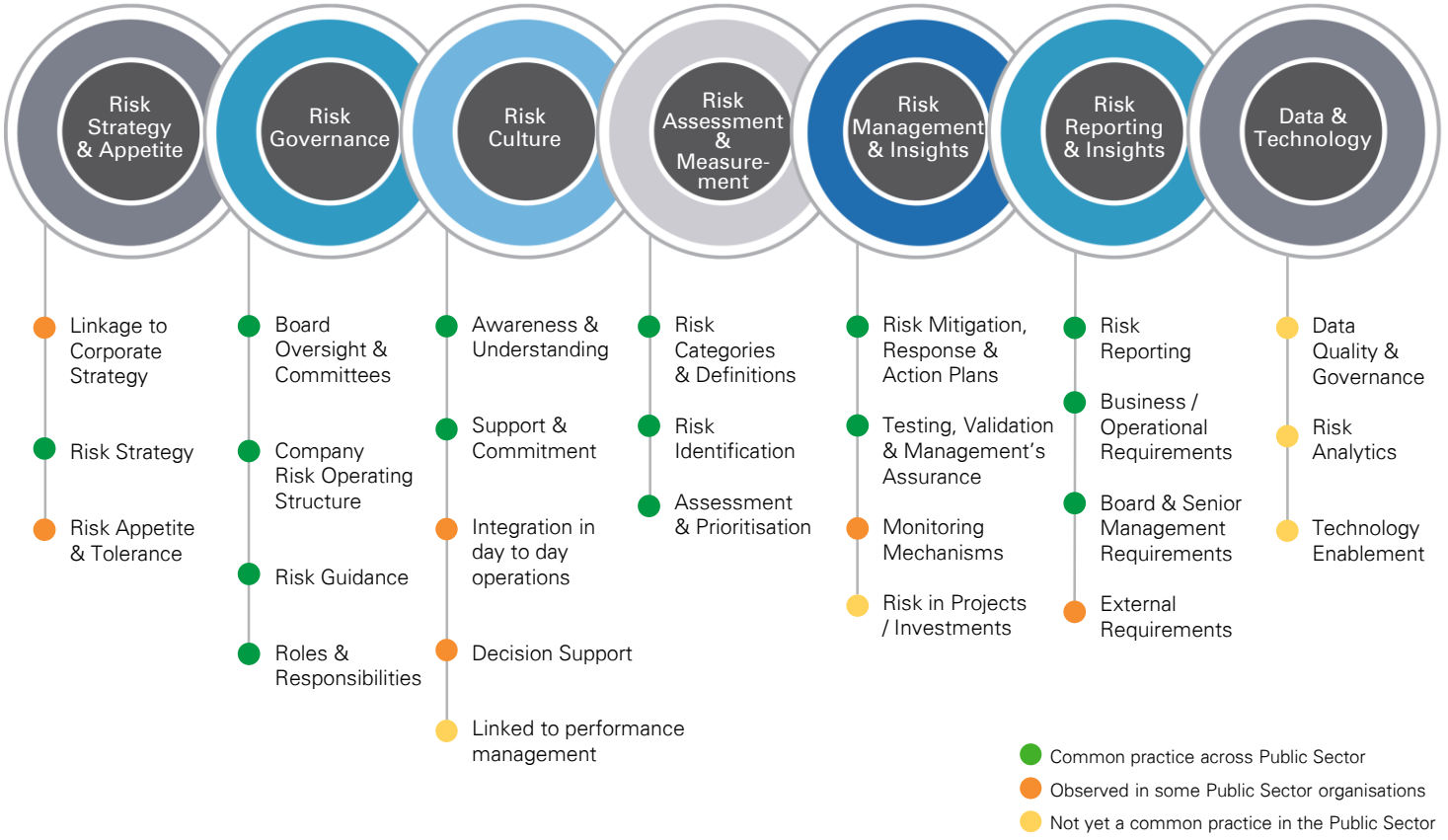


Figure 1: ERM Maturity in the Public Sector based on KPMG's '7 Pillars of ERM'

Common ERM practices across the Public Sector

Areas that the Public Sector is doing well include risk governance, process of risk assessment, and periodic risk reporting. The foundations of ERM are largely in place and sustained in many Public Sector organisations, in particular:

- Maintaining a documented ERM policy or framework which includes ERM objectives, risk governance structure, detailed roles and responsibilities, as well as other guidance
- Performing the risk identification and assessment process periodically to ensure that risks remain updated and relevant to the organisations' context. Typically, in-depth risk identification and assessment is refreshed on an annual basis
- Periodic reporting of risk information to Senior Management and Board (including relevant sub-committees), typically on a quarterly basis. Most commonly observed risk information reported included changes in risks, controls, noteworthy issues and incidents, among others

Risk management practices which we have observed apparent in organisations with more mature ERM programmes, or are work-in-progress for many, include the following:

- Establishing risk appetite and tolerance for key risk areas to guide decision-making, as well as align risk management to strategic planning
- Using Key Risk Indicators (KRIs) as early warning mechanisms to monitor exposures of key risk identified, reported in a timely manner to Senior Management and Board as appropriate. KRIs are most useful in providing 'quick trigger' monitoring and reporting mechanisms to highlight exceptions in a pre-emptive and timely manner for appropriate follow-up
- Viewing risk management and assurance from an integrated perspective, for example, using the risk profile of the organisation as a starting point to develop Internal Audit and other assurance work plans. This typically will provide Senior Management and Board with improved assurance and comfort that risks are being well-managed, as well as optimising resource allocation
- Continuously building risk awareness, appreciation and culture, cascaded down to operations. Risk awareness and appreciation, from our observations, is typically stronger at Senior levels within Public Sector organisations. Cascading to operational levels still tends to be a key work-in-progress area within these organisations

ERM components which Public Sector organisations have started considering and discussing but not yet a common practice include:

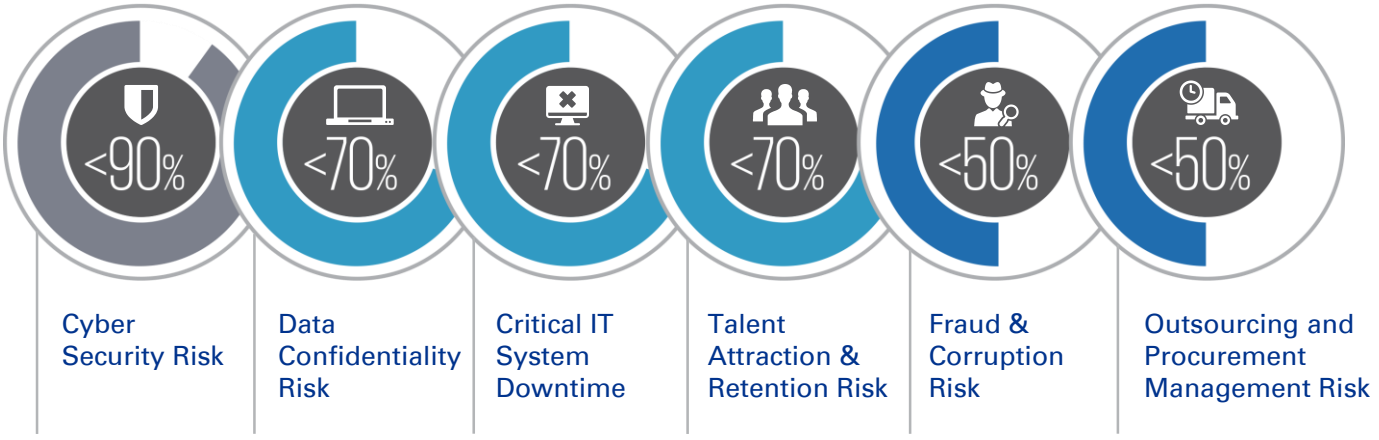
- Use of technology to support and enable ERM, for example, system-based templates to input and update risk information, as well as automated risk dashboards to provide real-time risk information to relevant parties
- Leveraging data within the organisation to provide more precision and insights throughout the risk assessment process. For example, using recent data as a starting reference when evaluating the likelihood and impact of risks
- Reinforcing the importance of risk management by linking ERM or risk-related activities to performance management, to further drive the desired risk culture and behaviours in the organisation

Common Top Risks in the Public Sector today

KPMG

Figure 2 outlines the most common top risks and concerns within Public Sector organisations today, based on our observations:

Common Top Risks identified by Public Sector organisations*



**Based on KPMG's portfolio of Public Sector Clients*

Other common concerns include:

- Stakeholder Engagement and Relation Risk
- Grant Administration and Governance Risk
- Workplace Health & Safety (e.g. abuse by public)
- Policy & Programmes Effectiveness Risk
- Project Management Risk

Figure 2: Common Top Risks identified by Public Sector organisations

There has been a rapidly increasing focus from Boards and Senior Management on cyber security and data confidentiality risks and issues, especially in light of recent incidents in Singapore. Other common top risks identified and discussed include downtime of critical IT systems, as organisations leverage more and more on technology, as well as talent attraction and retention risk which has been a continued concern for many Public Sector organisations.

This is also in line with recent Auditor-General's Office (AGO) reports, where weaknesses in information technology controls had been a significant focus area in previous audits – most recently in Financial Year 2016/2017 and 2017/2018. AGO acknowledged that the lack of attention is of concern in view of the public sector's high dependency on IT systems and data for Government operations, and the fast-evolving IT security threats.

Some of the common weaknesses identified included no monitoring of privileged users' activities in IT systems, and lapses in managing user accounts and access rights.

Annually, KPMG performs an in-depth Root-Cause Analysis on the key findings and issues raised. Results from the analysis were compared with the past AGO reports since its genesis (Year 1990) to detect key trends and solutions to prevent the recurrence of similar issues from arising. From the analysis, repeated root causes had been observed. Root causes include: (i) lack of monitoring; (ii) compliance with controls not prioritised at various supervisory levels; and (iii) insufficient robust procedures. As such, it is crucial for each organisation to start reviewing the adequacy and effectiveness of its existing framework and how to improve and mature it.

ERM 2.0 in the Public Sector – Key Building Blocks

KPMG

With the continuously evolving risk landscape and risk management standards, many Public Sector organisations have started to ask the question – What are some of the initiatives that can be considered to further mature my ERM programme?

The latest ERM good practices and hot topics among Boards and Senior Management seem to converge on a few pertinent questions:

- How can we continuously streamline the ERM process to improve user-friendliness and efficiency, while improving the timeliness and quality of risk information reported?
- Are we able to leverage on various sources of existing data and information to further improve the robustness of our risk identification, assessment and monitoring process?
- How can we use the valuable outputs from our ERM process to continuously guide and challenge strategic decision-making?
- Can we minimise potential 'blind spots' in our risk identification and assessment efforts?
- How can we continuously and effectively drive the right risk behaviours across the organisation?

In this section, we aim to answer the questions above by sharing some of the latest ERM trends and initiatives we have seen in the industry which may be considered by Public Sector organisations (Figure 3).

It must however be re-iterated that the suggestions in this publication are only a reference. Organisations are reminded to ensure that their ERM roadmap is progressive and tailored to individual needs and context in their drive towards 'ERM 2.0'.

Figure 3: Latest ERM trends and initiatives

5.1 Risk Inter-connectivity

The concept of risks influencing one another is not new. Over the past two decades, the world has become increasingly inter-connected, from the physical environment to virtual networks. The speed of information flow and travel has also rapidly increased. The risks organisations face, as a result, correspondingly increased in connectivity as well. However, many organisations are still at the exploratory stage in this regard, and the large majority have not yet established a structured process to evaluate the interconnectivity of key risks they face.

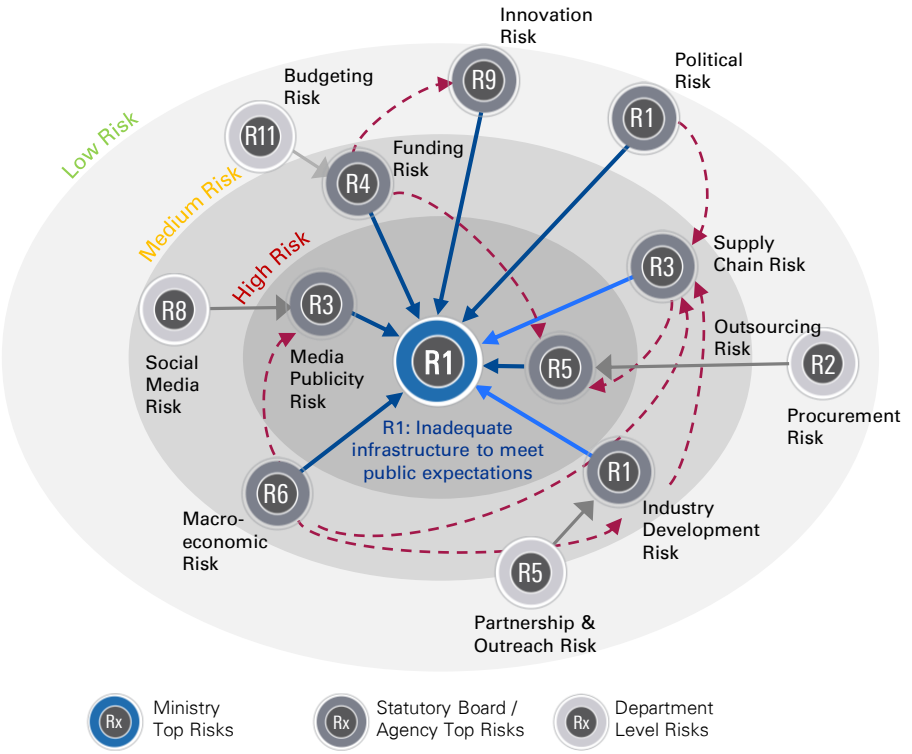
Organisations at the forefront of risk management practices are starting to talk about risk networks instead of risk profiles, prioritising risks with an interconnected perspective in addition to the traditional risk matrix measuring likelihood and impact. In the Public Sector context, organisations may evaluate not only intra-organisation risk interconnectivity, but inter-organisation risk interconnectivity as well. For example, risks faced by a Ministry could very well be closely connected with risks faced by related Statutory Boards and Agencies.

Risks can be inter-connected in various ways. A risk may have a causal or consequential relationship with another, risks may also have common causes or drivers. Risks exposures, where there is a connection, can be either positively or negatively co-related. Positively co-related risks increase or decrease in risk exposure correspondingly, while an increase in exposure of a risk will result in a decrease in exposure of negatively co-related risks.

It is also important to note that connections between risks can have varying degrees of strength. Strong co-relations between risks indicate a higher probability of interactions should one risk materialise.

Besides exploring the inter-connectivity between risks, another dimension of risks that can also be considered is risk velocity, which can be defined as the time taken for the full impact of the risk to affect the organisation should it materialise. Evaluating risk velocity may give organisations insights into the state of preparedness that should be maintained to react to potentially high velocity risk events.

A sample illustration of how risk interconnectivity and velocity can be analysed and visualised is set out in Figure 4:



- Have we identified and **documented risk causes comprehensively** and appropriately?
- Are there **potential 'snow-balling' effects** between risks?
- Do our **initial likelihood and impact ratings** reflect the reality of risk exposures?
- How much **reaction time** do we have should one of our key risks materialise?
- How can we **optimise resource allocation** for risk management through understanding of risk interconnectivity?
- Are the **key controls adequately established** to mitigate these systemically significant risks?

Figure 4: Analysing and visualising risk interconnectivity and velocity

KEY INSIGHTS AND BENEFITS

Some key additional insights which Management can draw from evaluating risk interconnectivity and mapping out the organisation's risk network include:

- Risks which significantly influence other key risks faced by the organisation may need to be monitored and managed closely, focusing on managing the likelihood of this risk materialising by putting in place preventive controls and early-warning risk monitoring mechanisms
- Worst-case scenarios may also be identified by evaluating which are the risks most affected by other risks faced. Organisations may need to ensure that response controls and plans are in place to contain the situation should these risks materialise
- There may also be clusters of risks which are highly connected to each other. This may create a 'snow-balling' effect between risks where, due to the highly inter-connected nature of clusters, multiple risks may materialise and be exacerbated in quick succession should one of the risks within the cluster occurs
- Organisations may often reap side benefits from encouraging such conversations on risk interconnectivity, in particular improved communications and progressive breaking down of 'silos' between functions or departments
- Common mitigating strategies and controls across risks can also be identified and prioritised to further optimise allocation of risk management resources

GETTING STARTED

Public Sector organisations may start by taking reference from their current top risks identified to explore risk interconnectivity. Through various methods such as surveys and engaging with stakeholders on an individual or focus group basis, collect input on potential connections between risks.

Once input has been collected, it is important that key stakeholders have the opportunity to moderate and calibrate outcomes to agree on an organisation-wide view of interconnectivity.

5.2 Linking Risk Management to Strategy

In line with the latest changes in ERM good practices, including the 2017 revision to the COSO ERM Framework, Boards and Senior Management are lending increasing focus on enhancing the linkage between risk management and strategic decision-making.

Many organisations today still find it challenging to put into practice the continuous linkage and feedback between risk management and strategy. Strategic objectives are often used as starting points for risk identification and assessment, but the feedback of risk information and considerations back into strategic decision making processes is typically where Public Sector organisations still face some inconsistencies.

However, in instances where organisations have successfully established a structured and consistent process to integrate risk management with strategy, we have observed marked improvements not only in the robustness and speed of risk-based decision-making, but also breakthroughs in the understanding and appreciation of risk management among stakeholders.

Figure 5 illustrates how the linkage between risk management and strategic decision-making can work in practice, and the key enablers to consider in terms of people and process.

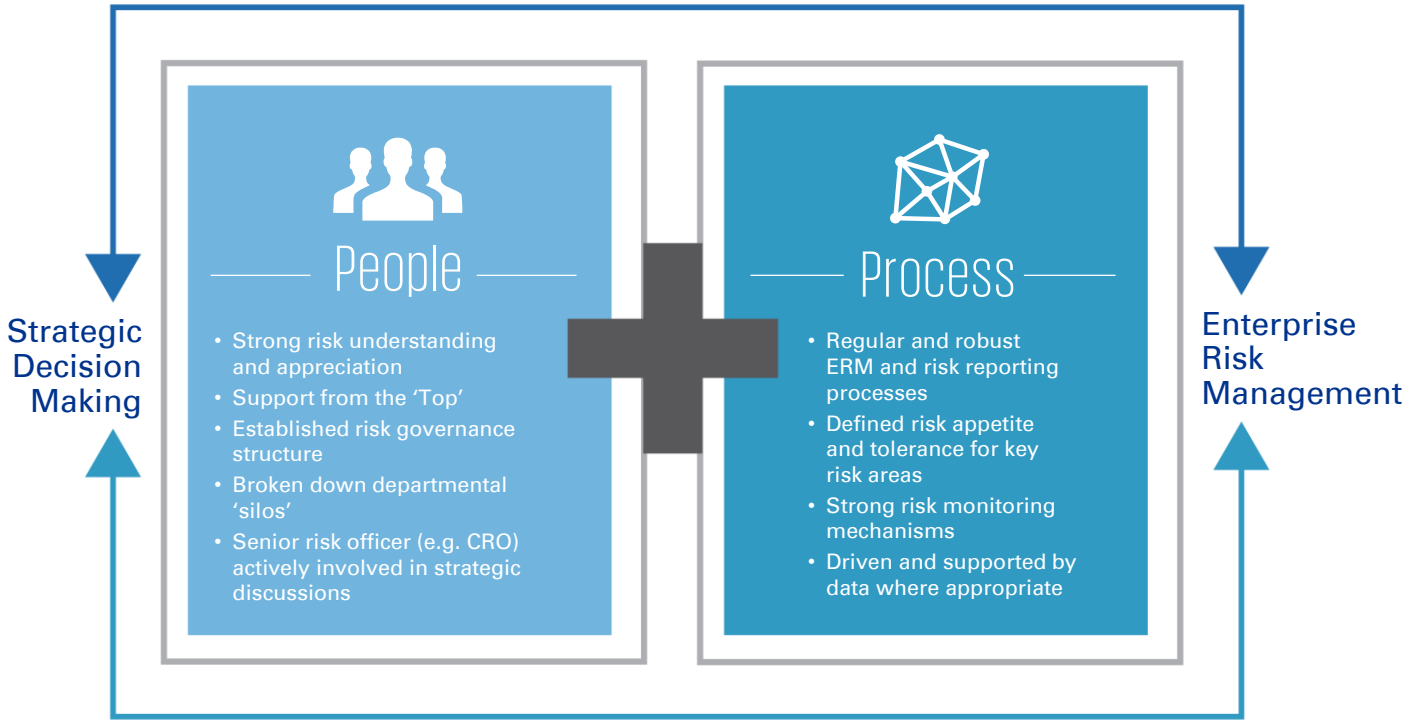


Figure 5: How risk management and strategic decision-making can work in practice, and key enablers to consider for people and process

In the Public Sector context, organisations should not only consider their respective vision, mission and strategic objectives, but look at strategic direction from the whole-of-government perspective as well. Ultimately, the Public Sector's main role is to serve the needs of the public as a whole. Each Ministry, Statutory Board and Agency has a unique role to play in fulfilling this strategic direction. Keeping the whole-of-government perspective may also help organisations think of risks beyond individual 'silos' to consider how organisations can co-ordinate better to manage risks which may be inter-connected or related.

To effectively link ERM with strategic decision-making, the set up and role of the risk management function can be considered central. The Chief Risk Officer (CRO), or equivalent, of the organisation has an important role to play not only in leading risk discussions, but often providing differing views to challenge Senior Management at key junctures within the strategic planning or decision-making process. Hence, it is critical for the CRO to be a senior member of Management, with sufficient depth of knowledge in both risk management and operations of the organisation. The CRO also needs to be kept informed and actively involved in all aspects of strategy formulation and decisions for this approach to be most effective. It is also important that this integrated approach to ERM and strategic decision-making should not remain static. The feedback loop should be sustained and nurtured through continuous discussions, monitoring and healthy debate among key stakeholders.

KEY INSIGHTS AND BENEFITS

Key insights and benefits of integrating ERM and strategic decision-making are manifold, including:

- Reduced potential blind-spots through a risk-based approach to strategic planning and decision-making processes taking into account different perspectives
- Increased confidence in decision-making supported by risk assessments and considerations
- More aligned and relevant risk identification and assessment process, taking into account latest vision, mission and strategic objectives
- Reduced bias (e.g. groupthink) in strategy and risk discussions with more perspectives to 'challenge the norm'

Getting Started

Public Sector organisations may start considering enhancing the linkage between risk management and strategy by involving the ERM function in platforms for strategy discussions and decision-making, where appropriate.

Where strategic information may be deemed highly sensitive, a member of Senior Management should take on the role of actively providing risk perspectives in such strategic discussion platforms.

From the longer term perspective, organisations should also think about evaluating both risk management and strategic decision-making processes to identify key touch points for integration, as well as consider the need for a senior Risk Officer resource to facilitate risk discussions at strategic levels.

5.3 Tech-Enabled ERM

Organisations today are investing more in technology to augment processes and operations, driving increased efficiency, transparency and value-add. ERM, in the same manner, has emerged as a potential candidate for technology enablement in many Public Sector organisations. Although only the minority have invested and implemented in an automated tool to support their ERM programme, this has become an increasingly popular topic for discussion among leaders of organisations in recent times.

In addition, Boards and Senior Management are increasingly stepping away from long-form risk reports but expecting key risk information to be presented to them in a dashboard view with a 'one-look' summarised view of risks and controls, coupled with the ability to deep-dive into details where there are exceptions as required.

Some of the key features and benefits that a tech-enabled ERM programme can bring to organisations are illustrated in Figure 6:

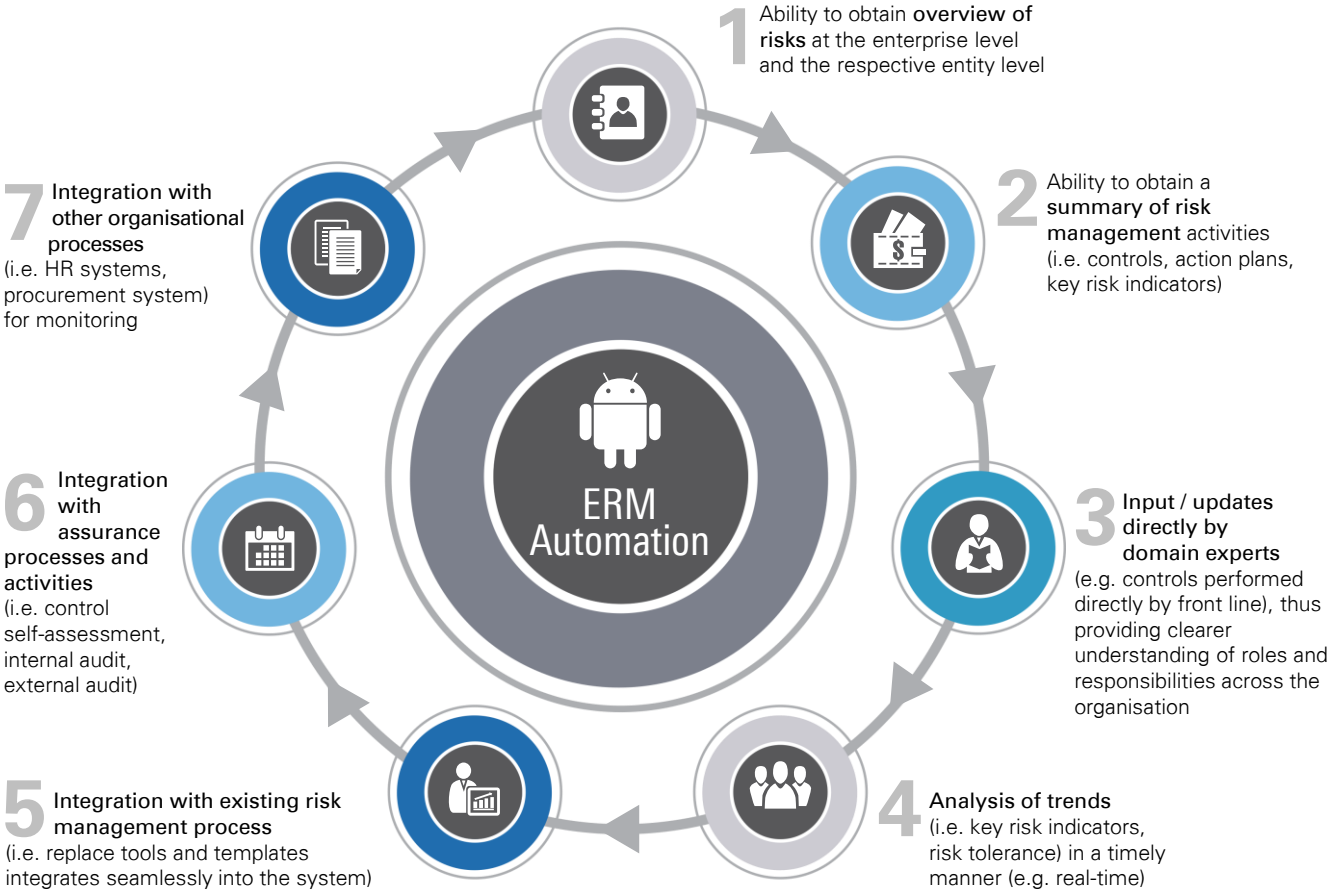


Figure 6: Key features and benefits that a tech-enabled ERM programme can bring to organisations

Technology is a key enabler to build a connected and integrated ERM framework. ERM processes can be enhanced, for example, with more timely and accurate reporting of information from operations and improved consistency of risk management practices among others. In other words, technology allows organisations to deploy 'sensors' within operational processes and functions, perform analysis on data and information collected, in order to improve timeliness of risk escalation and management.

Technology can also enable organisations to prepare and report risks in an interactive dashboard format. Risks are updated almost real-time and supported by data and indicators monitored on an ongoing basis. This not only allows Boards and Senior Management to focus on the most critical risk areas, but also allows for enhanced decision-making based on most updated risk information. Figures 7 and 8 provide illustrations on how interactive risk dashboards may look.

Figure 7: Illustration of interactive risk dashboard

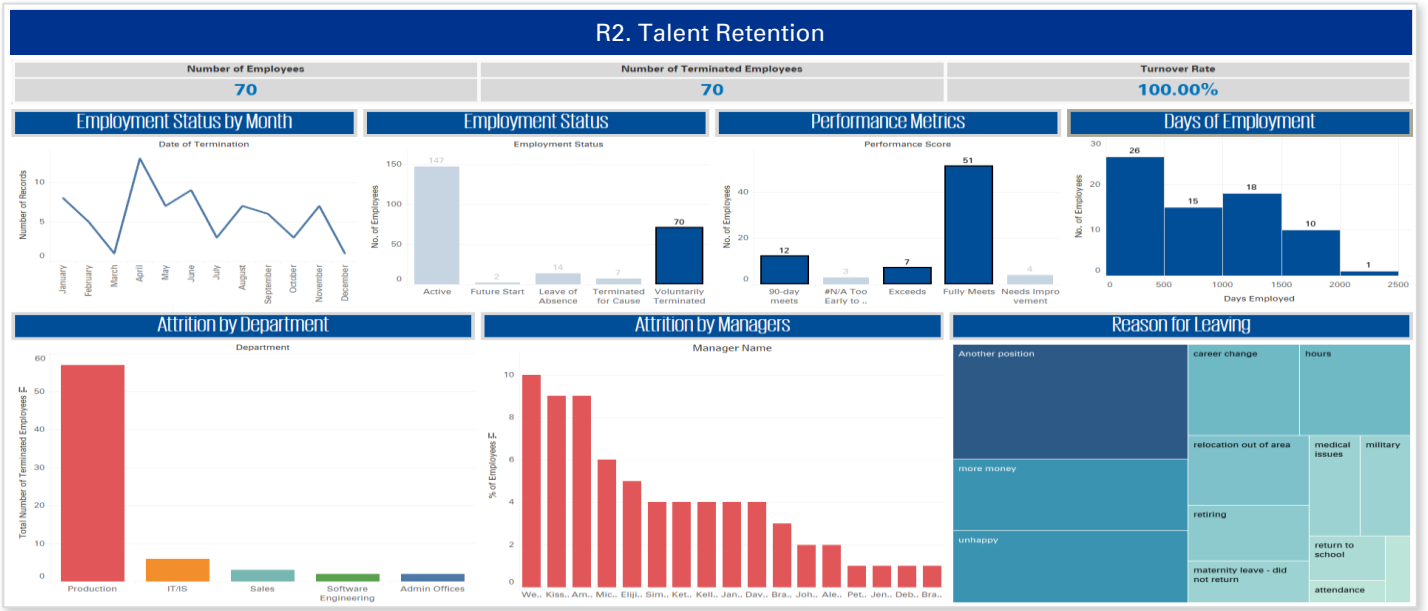


Figure 8: Illustration of interactive risk dashboard

Despite the numerous benefits of technology enablement in ERM, common roadblocks that still remain in most Public Sector organisations include cost considerations and overall ERM maturity.

As technology advances, cost of automation is likely to fall. The key consideration of whether to purchase an off-the-shelf system, or build a customised solution still remains. Organisations are strongly encouraged to consider the pros and cons of both models to make an informed decision. Some of the common pros and cons of off-the-shelf and custom built solutions include:

Off-The Shelf	Custom Build
Recurring license fees required Recurring license fees needed for continued use of software	**No recurring license fees** No recurring license fees for continued use as you own the IP
Lack of control over development Users have little to no control over the developer's development roadmap	**Full control over development** Users will have full control over development roadmap
Limited to pre-built analyses Customisations may not be possible or will require exorbitant fees	**Fully customisable analyses possible** Customisations can be done by in-house developers
Conform to design & functionalities Need to conform to existing design and functionalities	**Customised design & functionalities** Fully customised to suit your business and workflow

Before seriously considering investing in a technology solution to support ERM, organisations should ensure that the basic foundations of ERM have been put in place, stabilised and sustained, including:

- Risk governance structure, roles and responsibilities
- ERM process (including documentation)
- Periodic and ad-hoc risk reporting protocols
- Continuous communication to build risk awareness and understanding among stakeholders

In most cases of effective technology-enabled ERM programmes, the ERM process and users drive the requirements and implementation of the technology solution, rather than the solution dictating how ERM processes should be performed.

Public Sector organisations are strongly encouraged to consider technology enablement as part of their ERM roadmap, but maintain a progressive approach in order to extract maximum value from their investments.

KEY INSIGHTS AND BENEFITS

The potential key benefits of a technology-enabled ERM programme is widely understood and acknowledged in most Public Sector organisations, including:

- Increased efficiency and user-friendliness of the ERM process, which may also have a positive impact on risk awareness and appreciation among stakeholders
- Improved timeliness and focus of risk reporting to appropriate parties for risk-informed decision making
- Organisation-wide perspective of risk management and assurance with supporting data and information from various operational and governance activities
- More optimal use of ERM resources in the organisation. For example, freeing up the CRO (or equivalent) from spending too much time on administrative 'business-as-usual' ERM tasks to focus more on advising Senior Management and supporting strategic decision-making

GETTING STARTED

Public Sector organisations are strongly encouraged to perform a review and benchmarking exercise of their existing ERM programme against latest ERM standards and good practices. This could involve ERM processes, tools and templates, reporting protocols, risk culture, among others.

Once stakeholders are satisfied with the robustness and effectiveness of the ERM programme in place, short and long term objectives for ERM technology enablement should be set out with cost-benefit analysis done before sourcing for potentially suitable systems and tools.

5.4 Breaking through the barriers of Risk Culture

It is critical to start building risk awareness, understanding and culture among stakeholders from the onset of ERM framework development. Good risk awareness has been largely established in most Public Sector organisations today, especially at Board and Senior Management levels. At operational levels, risk awareness and understanding may manifest more on specific topics, such as health and safety, data confidentiality risks, among others.

Figure 9 outlines the key pillars of risk culture:

Figure 9: Key pillars of risk culture

Risk awareness is generally strong in the Public Sector. But many organisations still find it challenging to further mature risk culture from strong awareness to true appreciation of the value proposition of ERM and ultimately drive the right risk behaviours. For many Public Sector organisations, risk management is only selectively integrated with some aspects of operations, such as project and grant management, among others.

In sustaining their ERM programmes, most Public Sector organisations have periodic initiatives to continuously build risk culture within key stakeholder groups. Most common approaches include face-to-face ERM training and workshops, e-Learning programmes and topical communication emails.

Some organisations have also started considering fresh approaches to garner further interest in ERM, for instance:

- 'Risk Awareness Day / Carnivals' with interactive booths and activities to encourage mass participation. This approach is most useful to communicate basic risk messages to large numbers of stakeholders
- Lunch-talks or breakfast sessions with invited external experts to share risk management 'hot topics'
- Online Risk Management newsletters to share latest trends, case studies and infographics on a periodic basis
- Customised highly interactive risk 'master classes' for small groups of participants (e.g. Risk Managers)

Many Public Sector organisations have started to conduct risk culture assessments, both internally and by appointing external consultants to provide an independent view. Risk culture assessment is traditionally one of the most challenging elements in ERM to assess and benchmark. They typically involve the use of anonymous survey tools, as well as closed-door focus group and interview sessions with key stakeholder groups, to gather input. Other tools and approaches used by organisations to assess risk culture are illustrated in Figure 10:

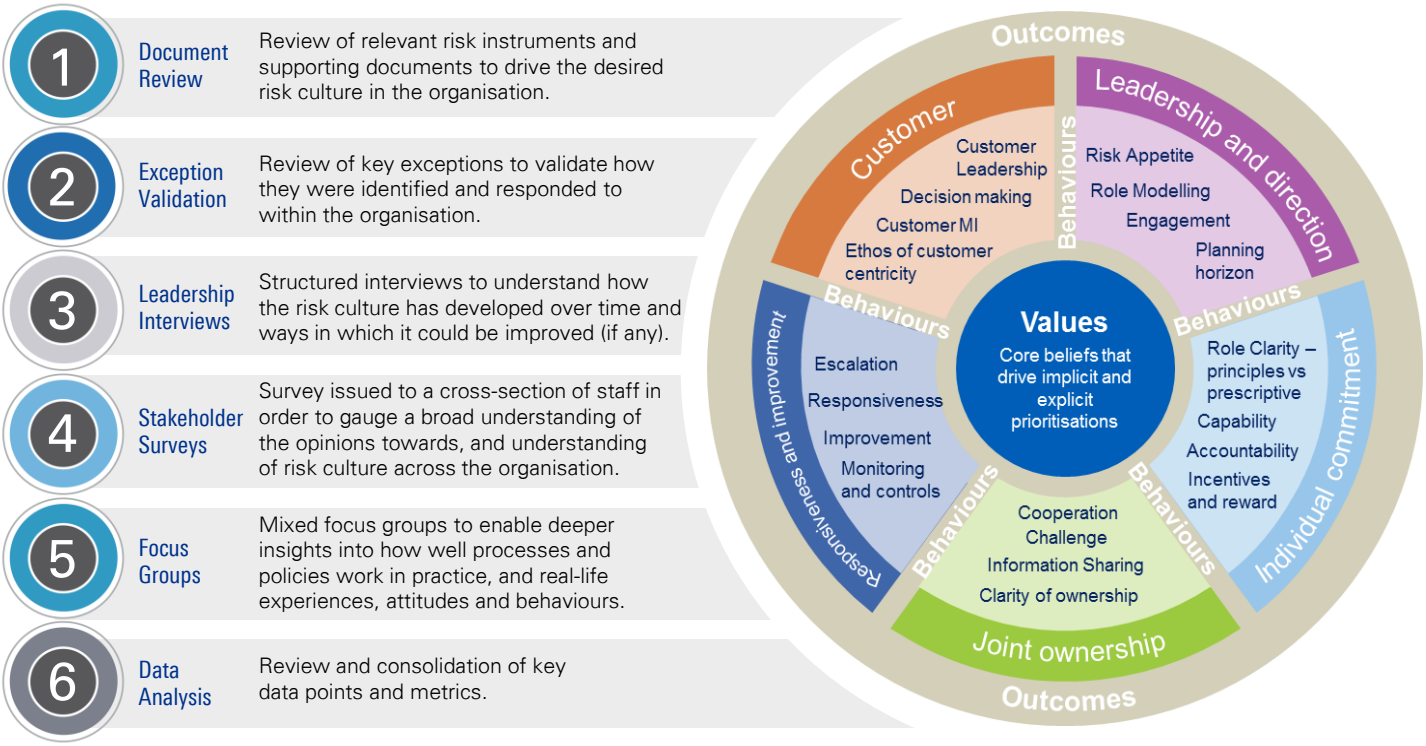


Figure 10: Some tools and approaches used by organisations to assess risk culture

Another aspect of risk culture that organisations have started to consider is the threat of bias and mental traps in risk discussions. Stakeholder engagement and discussions form a significant part of the approach to risk identification, assessment and monitoring processes for many Public Sector organisations.

As stakeholders become increasingly focused on in-depth risk discussions, it may sometimes be difficult to constantly maintain a high degree of objectivity. Participants tend to fall into one or more of the following mental traps during risk discussions:

- Recency effect – Placing greater emphasis on the most recent information we have received, which may not always be the most critical, to make decisions.
- Anchoring bias – An illogical tendency to "attach" ourselves to information we first see or hear during a discussion
- Uncertainty effect – An over-aversion to uncertainty which may sometimes lead to a risky prospect is valued less than its worst possible outcome. This may result in the over-emphasis or overreaction to risk events
- Status quo bias – A preference for things to remain the same by not making changes even though the status quo may not be the best course of action

The good news is, by just ensuring stakeholders are aware of the threats of bias and mental traps, objectivity in risk discussions can be improved significantly. ERM functions, as facilitators of risk discussions, should keep in mind the need to regularly remind participants of these threats through briefings or pre-meeting preparations before major risk discussions.

Risk culture is widely viewed as the most critical enabler to a successful and sustainable ERM programme. To continuously strive towards a culture where desired risk thinking and behaviours are 'business-as-usual' for stakeholders, there must be continuous efforts to emphasise the role of ERM and incentivise good risk practices in line with organisational objectives.

KEY INSIGHTS AND BENEFITS

Key benefits of continuously building and emphasising the right risk culture within the organisation can include:

- Enhanced robustness and efficiency of ERM processes including risk identification, assessment, monitoring and reporting
- Improved co-ordination and co-operation between functions as risk discussions often encourage stakeholders to break down the 'silos'
- Improved long-term sustainability and achievement of strategic objectives through comprehensive and ongoing considerations of risk matters

GETTING STARTED

For Public Sector organisations that currently have ongoing initiatives to build risk awareness and culture, they could consider periodic risk culture assessments through various means to identify and address any 'blind spots'.

Organisations are also encouraged to continuously keep a look out for innovative ways to build sustained interest in ERM and communicate risk messages, in addition to traditional means such as ERM seminars and training.

Building Your Practical ERM Roadmap

KPMG

Building your ideal ERM programme requires a progressive approach, tailored to individual organisational context and objectives. Figure 11 outlines a typical ERM roadmap for Public Sector organisations focused on sustainability and continuous improvement:

Figure 11: A typical ERM roadmap for Public Sector organisations focused on sustainability and continuous improvement

Stage 1 typically involves setting the foundations of an ERM programme, including risk identification processes, as well as establishing the overall ERM framework including objectives, governance and responsibilities.

Once the ERM framework and process has been established and sustained for a period of time, organisations may start to move into Stage 2, where the focus shifts to extracting further value from ERM through integration with other risk management and assurance activities, as well as exploring other ERM 'add-ons' to augment the ERM programme in place. Stage 3 focuses largely on the move towards a technology-enabled and data-driven ERM model.

Organisations at this stage typically have sustained ERM for a period of time, with a strong risk culture permeating across the organisation from operations to the Board. Due to the acknowledged importance of ERM to the organisation at this stage, stakeholders tend to be more comfortable investing resources to ensure that ERM efforts provide maximum value to stakeholders in line with objectives.

Organisations are also strongly encouraged to seek independent perspectives to review and benchmark ERM practices against the latest risk management trends and standards at key junctures of their ERM journey. Such review and benchmarking exercises are to ensure continued relevance and effectiveness of the programme and to minimise any duplication and wastage of efforts.

When mapping a tailored ERM roadmap, it is critical for Public Sector organisations to keep in mind the following considerations:

- Tone and support from the 'Top' – As with any initiative an organisation embarks on, support from the Board and Senior Management is of utmost importance. Senior stakeholders are encouraged to regularly communicate important risk messages, seek feedback from operations, as well as to 'lead by action', in order to drive continued focus on good risk management
- ERM resources and investment – Investment and resources will inevitably be required to sustain and continuously improve ERM practices within the organisation. It is important to keep in mind that cost-benefit analyses should always be considered to ensure optimal resource allocation to ERM. Resources to be considered include both internal and external resources
- Role of the ERM function – Everyone in the organisation has a role to play in ERM. However, the role of the ERM function is critical to the success and effectiveness of the programme. Although the Head of the organisation is ultimately responsible for risk management, having a senior or Chief Risk Officer in the organisation can provide invaluable support to the Senior Management Team. Responsibilities of a Risk Officer can be manifold, ranging from providing risk management advice and providing the contrarian view to challenge the Senior Management Team, facilitating in-depth risk discussions, to partnering operations in process improvement initiatives, among others. As such, the Risk Officer should not only be the ERM expert of the organisation, but should also have good knowledge of the organisation

In the Public Sector today, a minority of organisations have catered resources for a CRO position. Most risk management functions within the Public Sector have 2-4 staff with dual or multiple responsibilities ('double-hatting'), while a few have set aside dedicated headcount for risk management. Public Sector organisations are strongly encouraged to consider the need for a senior dedicated Risk Officer function to spearhead efforts towards ERM 2.0.

KEY REFLECTION POINTS FOR PUBLIC SECTOR ORGANISATIONS

1. Where are we in our ERM journey?
2. What are the areas we have done well and what needs further improvement?
3. How have we progressed in terms of risk culture?
4. Have we catered for sufficient ERM resources to meet our objectives?
5. Are we ready to take the next steps towards 'ERM 2.0'?
6. What are the potential key roadblocks to further mature our ERM programme?

Conclusion

In general, Public Sector organisations in Singapore have progressed in taking the first step in their ERM journey with the foundations of ERM well established. However, the risk landscape and public expectations are continuing to evolve.

We strongly recommend the Public Sector keeps in mind considerations to further mature and continuously improve ERM practices within the organisation. The suggestions in this publication offer a starting point for organisations that are considering the next steps in their ERM journey.

We have shared the key building blocks of ERM 2.0 in the public sector and some tips to build a practical ERM roadmap. These take into account the latest ERM trends globally and in Singapore.

There is no one 'best' ERM framework that suits all organisations. Individual organisations will need to take the time to examine and evaluate their risk context and objectives, maturity, as well as uniqueness of their business, before charting out their bespoke ERM roadmap to optimise the value that ERM can bring.

External help may be required for advice on aligning the ERM journey with local and global risk standards, and with industry best practices.

Ultimately, continuous reinforcement and improvement will be critical to a successful and sustainable ERM journey.

Contact us

Jonathan Ho
Head of Internal Audit, Risk & Compliance
Head of Enterprise Market
T: +65 6411 8336
E: jho1@kpmg.com.sg

Tea Wei Li
Partner
Risk Consulting
T: +65 6411 8114
E: wtea@kpmg.com.sg

16 Raffles Quay #22-00
Hong Leong Building
Singapore 048581
T: +65 6213 3388

kpmg.com.sg