



Enterprise Risk Management Toolkit for Charities and Institutions of a Public Character (IPCs)



Table of Contents

Foreword	1
Introduction	2
Background	
Objectives	
Embedding risk management practices in your charity	3
The ERM framework	
KPMG's ERM methodology	
Challenges and critical success factors to implementing ERM	
Common key risks in the charity sector	5
Common key risks highlighted	
Appendix A: Establishing the ERM process	6
Key Principles	
Identify Risks	
Assess and Manage Risks	
Monitor and Report Risks	
Appendix B: Developing and documenting the ERM framework	12
Key Principles	
Risk Strategy	
Risk Governance	
Enterprise Risk Management Process	
Risk Reporting Requirements	
Appendix C: Building risk awareness and understanding	16
Key Principles	
Tools to Build Risk Awareness	
Appendix D: Top risks by sector	17
Top Risks	
Sample Risk Assessment for Common Top Risks	
Sample Risk Assessment for Funding Risk	
Sample Risk Assessment for Non-compliance with Personal Data Protection Act (PDPA)	
Sample Risk Assessment for Non-compliance with Established Laws, Regulations, and Code of Governance Risk	
Sample Risk Assessment for Conflict of Interest Risk	
Sample Risk Assessment for Employee Risk	
Sample Risk Assessment for Adverse Events Risk	
Appendix E: Sample operational risk registers by sector	24
Sample Risk Register for Arts	
Sample Risk Register for Social and Welfare	
Sample Risk Register for Education	
Sample Risk Register for Health	
Sample Risk Register for Religious	
Sample Risk Register for Sports	
Sample Risk Register for Community	
About Us	31
Contact Us	

Foreword

Establishing and implementing an Enterprise Risk Management (ERM) framework for the first time can be a daunting task for any organisation, and especially for Charities.

This 2016 ERM Toolkit for Charities and Institutions of a Public Character aims to share practical ERM insights, and recommended methodologies and approaches with organisations currently registered as Charities in Singapore.

Jointly produced by the Charity Council, KPMG in Singapore and National University of Singapore (NUS) Business School, this toolkit sets out the best practices and key foundations for building an efficient and sustainable ERM programme within Charities across various sectors.

It will also provide Charities with a set of guidelines and practical considerations when starting off their ERM journeys, including establishing the ERM process, framework, governance, etc., and help the Management and Board to play a greater oversight role in ensuring the adequacy and effectiveness of risk management and internal controls.

It must be reiterated, however, that ERM should be viewed from the perspective of a sustainable journey where continuous reinforcements and improvements are paramount to the success of the programme.

We would like to thank the individuals and Charities for their time and invaluable contributions to the development of this toolkit.

Gerard Ee

Chairman
Charity Council

Irving Low

Head of Risk Consulting
KPMG in Singapore

Professor Ho Yew Kee

Principal Investigator

Introduction

To meet with the growing demands for greater governance and transparency, Charities are urged to use ERM as a tool to provide their Management and Board with enhanced information and oversight on the Charity's risk and control environment.



Objectives

This toolkit aims to provide practical guidance to Charities on the implementation and sustenance of Enterprise Risk Management (ERM), including guidance on the following:

- ERM process (e.g. risk identification, assessment etc.)
- ERM governance (e.g. risk governance structure, roles, responsibilities, etc.)
- Risk reporting process and format
- Building risk awareness and understanding within the Charity

This toolkit takes reference from local and global Risk Management and governance standards, including the following:

- ISO31000:2009

- COSO
- Risk Governance Guidance for Listed Boards (RGG)
- Board Risk Committee Guide 2016

Statutory regulations and legislations (e.g. Charities Act and regulations and sector specific regulations) should take precedence over the guidance provided within this toolkit as applicable.

This toolkit aims to provide guiding principles and references, and is not meant to be prescriptive or exhaustive in nature. Individual Charities should consider and tailor their approach to ERM development and implementation, taking into account the Charity's objectives, structure and context.

Embedding risk management practices in your charity

The ERM framework

A structured approach and framework around ERM related processes and governance is critical to the success of ERM in any Charity.

The ERM Framework typically provides the guidance and boundaries within which ERM related activities should be carried out, and usually includes the following key components:

- Risk strategy – Provides the overall ERM strategy and direction of the Charity
- ERM process – The process by which risks are identified, assessed, monitored and reported across the Charity
- Risk governance – Clearly defined structure, roles and responsibilities for the operationalisation and oversight of ERM within the Charity

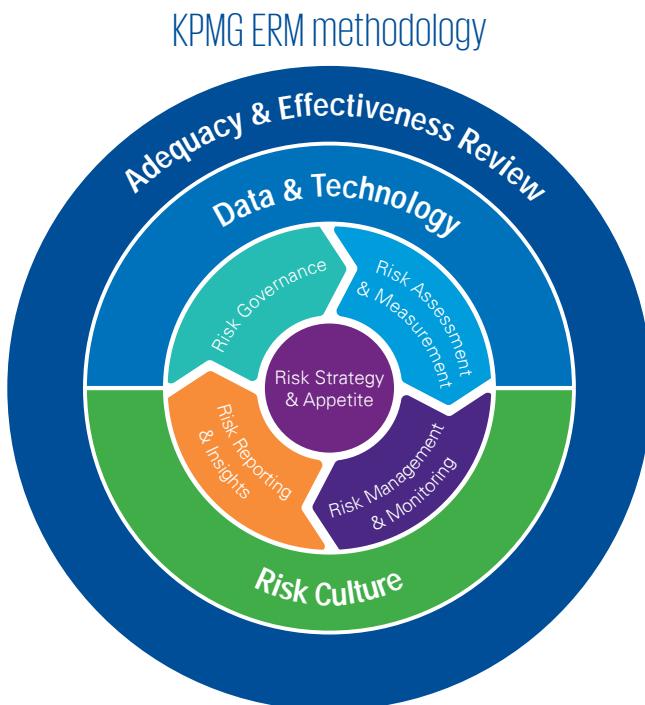
It is important that the ERM Framework is tailored to the unique requirements, circumstances and context of each Charity. The Framework should also be regularly reviewed and communicated to all stakeholders within the Charity.



KPMG's ERM methodology

KPMG's proprietary ERM methodology defines the key pillars that a robust ERM framework should include. This methodology is aligned with leading global practices (e.g. ISO 31000, COSO, Singapore Code of Corporate Governance) and builds on years of practical experience developing, implementing and reviewing ERM programmes across Charities.

The actual approach and pace on implementing ERM typically varies significantly across Charities based on considerations such as size, resources, industries and objectives. Larger Charities may be able and willing to invest in building a comprehensive ERM framework to reap optimal benefits from such a programme, while others may only strive to establish and sustain basic ERM foundations.



Challenges and critical success factors to implementing ERM

In the recent survey¹ of risk management practices in the Charity sector in Singapore, respondents were asked what they felt were the challenges faced in implementing and conducting risk management activities in their Charities. More than 70 percent cited the lack of risk management expertise and insufficient human resource as key challenges faced. Other top challenges highlighted include insufficient financial and technical resources, as well as lack of a formal ERM process and framework.

An ERM Framework can still be effectively built and sustained

within a Charity despite facing limitations in human, financial and technical resources. It becomes all the more critical for Charities to prioritise risk management resources to focus on what matters and establish strong foundations in terms of prioritising and assessing key risks to the Charity, defining risk accountabilities and responsibilities, as well as building basic risk awareness and understanding across stakeholders.

Typically, the most essential yet challenging factors involve building risk awareness and understanding,

as well as promoting the 'right' risk management mindset across all levels of the Charity, from Board to general staff. Risk awareness, understanding and capabilities have to be progressively built from the on-set to ensure maximum learning and buy-in.

Refer to Appendices A to C for further guidance on establishing an ERM process and framework, as well as building risk awareness and understanding across your Charity.

¹ Influencing Risk and Risk Culture; Charity Council, KPMG, NUS Business School; 2017

Common key risks in the charity sector

Common key risks highlighted

In the recently conducted survey of risk management practices in the Charity sector in Singapore, respondents were asked to rank what they felt were top risks faced by their Charity. The below table summarises the top risks highlighted by respondents.

Refer to Appendix D for further breakdowns of top risks identified by sector.

Of the various categories of risks, operational risks are typically the category where top risks and concerns may vary more across sectors. Refer to Appendix E for sample operational risk registers by sector.

Common key risks in the Charity Sector

Risk Category	Risk	Risk Description
Financial	Funding risk	Inability to meet short term financial obligations arising from decreases in funding.
	Accounting and reporting risk	Inaccurate / unreliable / untimely data used for financial and accounting reporting, resulting in material misstatements in financial information.
Compliance	Non-compliance with established laws and regulations risk	(A) Failure to comply with legal, regulatory or contractual requirements and significant breach of code of ethics and conduct or accepted industry practices. and/or (B) Unfavourable changes in regulatory guidelines and statutes that may have a high impact on business strategy, operations, funding and safety requirements, etc.
	Risk of violation of Personal Data Protection Act (PDPA)	Risk of non-compliance in PDPA.
	Conflict of interest risk (e.g. related party transactions not at arm's length)	Less favourable transactions entered into by management with related vendors.
	Professional liability risk	Risk of hiring unqualified professionals in the support of the charity.
Technology	Risk of losing confidential data	Unauthorised leakage / disclosure of confidential / sensitive data. Cost of damage to donors, other relationships, and the business resulting from a breach of data privacy.
	Risk of data corruption	Corruption of data resulting in loss of key data necessary for decision making and reporting.
Operational	Employee risk (e.g. retention, disgruntled employees)	Inability to attract and retain the right talent with the required skill-set and competencies to take over key positions, which may result in disruption to operations, loss of institutional knowledge, and inability to achieve long term strategic thrusts.
	Adverse events risk (Internal and external)	Failure to effectively manage and/or respond to force majeure crisis (e.g. haze, serious pandemic, typhoons, floods), or man-made events (e.g. terrorist attack) resulting in interruption to business.

Appendix A: Establishing the ERM process

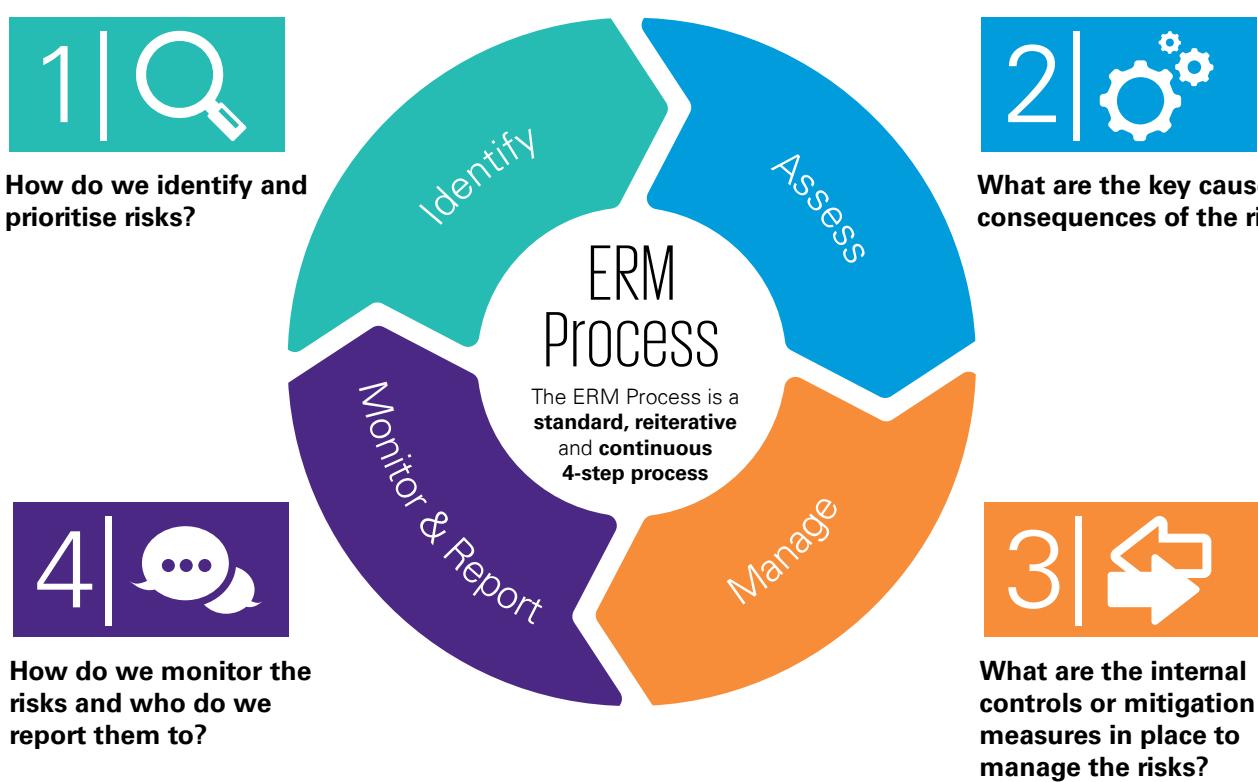
Key Principles

It is recommended for Charities to put in place a basic ERM process, including the following steps:

- 1. Identify risks – Finding, recognising, and describing the risks (including short to long term, and emerging risks) that may have an impact on the strategic objectives.**
- 2. Assess risks – Prioritising and understanding key risks to the Charity, including likelihood and potential impact of the risk to the Charity.**
- 3. Manage risks – Understanding controls or activities undertaken by management to respond to, mitigate or manage risk by reducing its impact, its likelihood of occurrence, or both.**
- 4. Monitor and report risks – Risks should be reviewed on a periodic basis, providing Management and Board with an up-to-date perspective on key risks faced by the Charity.**

The ERM process should be a reiterative process that is refreshed periodically or as necessary should there be material changes in the operating and business environment.

The diagram below outlines the 4-step ERM process, aligned to ERM standards and good practices including ISO31000, COSO, BRC Guide etc.



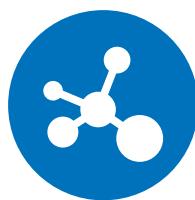
Identify Risks

Before commencing the risk identification exercise, it is important to set the boundaries and scope for which the ERM process will be applied in the Charity (e.g. In-scope departments, divisions, subsidiaries etc.).

After setting the context, the next step will be to develop a comprehensive list of risks relevant to the Charity (i.e. risk universe). The risk universe should

include all current and potential risks which may impact the Charity's ability to achieve its mission, vision or strategic objectives, including strategic, operational, IT, compliance and financial risks.

Sample Risk Universe



Strategic Risks

- Key Man Risk
- Stakeholder Engagement Risk



Financial Risks

- Fraud and/or Corruption Risk
- Procurement Risk



Compliance Risks

- Regulatory Compliance
- Data Confidentiality Risk



Operational Risks

- Pharmaceutical Management
- Cyber Security Risk
- Talent Attraction and Retention
- Critical IT System Downtime

Prioritising the 'Tier 1' risk profile

Once the risk universe has been developed, each risk should be prioritised by rating the probability of the risk occurring (likelihood) and the potential impact (consequence) should the risk occur. This is usually conducted through a risk workshop involving key stakeholders, with the main objective of discussing and coming to a consensus on the top, or 'Tier 1', risks faced by the Charity.

It is recommended that, to focus on what matters and familiarisation, Charities should keep to a maximum of six to eight risks in their Tier 1 profile for the first exercise.

Rating Risks

In order to ensure a consistent understanding of what may constitute a top (or 'Tier 1') risk, Charities should set a common set of risk parameters, or 'yardsticks' to measure risks. Risk parameters typically include measures for both likelihood and impact, with further guidelines on measuring various aspects of impact such as financial, operational and reputational factors. Risks may then be mapped into a risk matrix based on likelihood and impact to assess the overall risk rating.

Sample Likelihood Parameters:

Likelihood Descriptors	(1) Rare	(2) Unlikely	(3) Possible	(4) Likely	(5) Almost Certain
Prior risk incidents in industry	Did not happen in the industry	Has happened once in the industry	Happened several times in the industry	Happens regularly in the industry	Is a common occurrence in the industry
Probability	< 5%	Between 5% and 25%	Between 26% and 50%	Between 51% and 75%	> 75%

Sample Impact Parameters:

Impact Descriptors	(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Severe
Financial Impact Parameters					
Financial loss / impact	< X1%* of income	X1% to X2%* of income	X2% to X3%* of income	X3% to X4%* of income	> X4%* of income
Operational Impact Parameters					
Unplanned outages for critical IT systems	Critical IT system outage for < 2 Hours*	Critical IT system outage for 2 - 4 Hours*	Critical IT system outage for 5 – 12 Hours*	Critical IT system outage for 13 - 24 Hours*	Critical IT system outage for > 24 Hours*
Reputational Impact Parameters					
Perceived damage to reputation	Adverse media coverage and/or internet activity resulting in minimal reputational damage amongst a selection of key stakeholders	Adverse media coverage and/or internet activity resulting in some damage to reputation amongst a selection of key stakeholders	Adverse media coverage and/or internet activity resulting in short-term (< 1 week)* damage to reputation across all key stakeholders	Adverse media coverage and/or internet activity resulting in medium-term (1-2 weeks)* damage to reputation across all key stakeholders	Adverse media coverage and/or internet activity resulting in prolonged (> 2 weeks)* damage to reputation across all key stakeholders

*Note: Criteria should be tailored based on each Charity's respective business context.

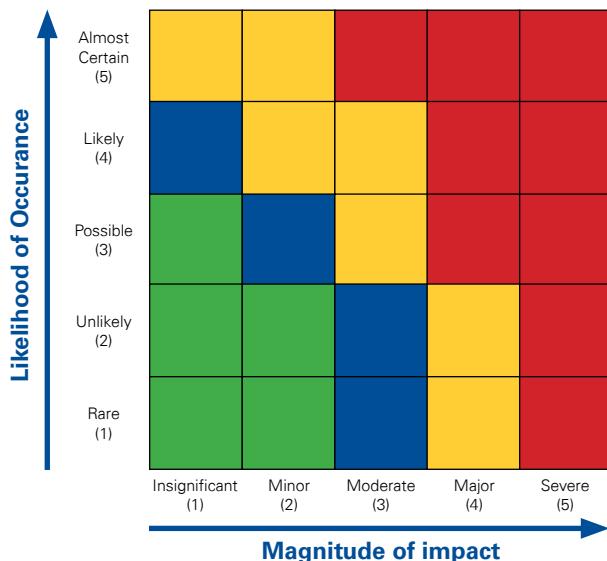
Risk Matrix

Based on the risk parameters, the likelihood and impact for each risk identified may then be plotted onto a risk matrix. The sample below shows a commonly used 5x5 risk matrix. Charities can however tailor the risk matrix to individual needs and requirements.

Risks are graphically depicted on the matrix with the areas in red representing a high likelihood and high impact zone, typically associated with risks that directly hinder the achievement of the Charity's objectives and require more attention in comparison to those with a low likelihood and low impact (green areas).

Charities may choose to rate each risk either at the 'Gross' or 'Residual' level, or to show both, depending on their ERM objectives and maturity.

- Gross risk level: Level of risk before taking into consideration controls in place to manage the risk.
- Residual risk level: The current or existing level of risks, taking into consideration controls or measures management currently has in place to manage the risk.



Appointing Risk Owners

Risk Owners should be appointed for each 'Tier 1' risk identified, with the main responsibility to assess, review and manage assigned risk(s) on an ongoing basis.

The appointed Risk Owner should be the person in the Charity who is best-placed to manage the risk and has the relevant knowledge, resources, and authority (e.g. of a certain seniority) to deal with the risk.

Assess and Manage Risks

After the identification and prioritisation of risks, it is recommended that efforts be focused on understanding and analysing the 'Tier 1' risks of the Charity. It is the responsibility of Risk Owners to complete the risk assessments for respective assigned risks, typically facilitated by the ERM function.

Documenting risk registers

It is a good practice to document risk assessments to promote staff accountability and for future reference.

Sample Risk Register:

Risk Register																	
R1	Talent Attraction and Retention Risk	Risk Category	Operational	Risk Owner	Head of HR												
Risk Description																	
Inability and/or failure to attract and retain key personnel with the appropriate and required skill-set / experience / competency resulting in potential failure to meet business objectives																	
Potential Key Risk Drivers			Potential Key Risk Consequences														
<ul style="list-style-type: none"> Less attractive compensation packages / benefits as compared to other companies Lack of strong 'corporate culture' and 'brand' to attract quality key personnel 			<ul style="list-style-type: none"> Inability to grow and achieve strategic objectives Inability to garner support and buy-in from industry players and public on organisation's projects and initiatives Increased management effort in the replacement of key personnel and increased training costs 														
Risk Assessment - Rating																	
R1 Inherent Risk <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Likelihood</td><td>Likely (4)</td></tr> <tr> <td>Impact</td><td>Major (4)</td></tr> <tr> <td>Rating</td><td>Very High</td></tr> </table> R1 Residual Risk <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Likelihood</td><td>Possible (3)</td></tr> <tr> <td>Impact</td><td>Moderate (3)</td></tr> <tr> <td>Rating</td><td>High</td></tr> </table>	Likelihood	Likely (4)	Impact	Major (4)	Rating	Very High	Likelihood	Possible (3)	Impact	Moderate (3)	Rating	High	<p>Likelihood of Occurrence</p> <p>Magnitude of impact</p>				
Likelihood	Likely (4)																
Impact	Major (4)																
Rating	Very High																
Likelihood	Possible (3)																
Impact	Moderate (3)																
Rating	High																
Existing controls / mitigating measures																	
Ref	Description		Responsible Party		Remarks												
R1.C1	Board recruitment channel, referrals / top management contacts / relationships within the charities sector and external providers (e.g. recruitment agencies and executive search firms).		HR														
R1.C2	Credentials and background checks are performed on all staffs where possible 2 referrals are required (including written referrals).		HR														
R1.C3	Compensation benchmarking survey (covering all levels of staff, local, overseas and key personnel) towards the competitors conducted annually.		HR														
Areas for Improvement																	
Ref	Description		Responsibility		Timeline												
R1.A1	Develop a larger talent pool: Continue identifying talents through the High Potential Assessment Exercise and offer them trainings to improve their key skills ("Leadership, Analysis & Judgment, Managing Complexity and Achievements & Values Driven") and coaching from Heads of Departments and above.		HR		FY 2017/18												

Key components of risks

The following key components of risk should be considered and documented in a risk register:

Risk causes – circumstances or situations, which may arise internally or externally, that can potentially result in the risk occurring.

Risk Event	Examples of Risk Causes
 Fraud and/or corruption Risk	<ul style="list-style-type: none"> • Collusion between staff and external parties • Non-compliance to policies and procedures • Inadequate segregation of duties
 Data Confidentiality Risk	<ul style="list-style-type: none"> • Staff negligence (e.g. misplacement of documents, thumb drives etc.) • Inadequate IT controls around user access • Breach in information security

Risk consequences – Potential impact resulting from the occurrence of a risk, which may be expressed in several aspects (e.g. Financial, Operational, Reputational, etc.).

Risk Event	Examples of Risk Consequences
 Fraud and/or corruption Risk	<ul style="list-style-type: none"> • Negative media publicity and loss of stakeholder confidence • Financial loss / loss of assets • Operational disruptions due to investigations
 Data Confidentiality Risk	<ul style="list-style-type: none"> • Negative media publicity and loss of stakeholder confidence • Financial loss due to lawsuits against the Charity • Operational disruptions due to investigations

Controls – Controls are processes, systems, or any other measures in place to reduce the likelihood or impact of the risk, or detect indications of the risk occurring such that follow-up actions can be taken to reduce the likelihood or impact of the risk.

Types of controls: There are three different types of controls as follows:

 Preventive Controls	 Detective Controls	 Responsive Controls
<p>Designed to help reduce the risk from occurring</p> <p>E.g. Standard Operating Standards on approving authorities for procurement matters</p>	<p>Designed to uncover risks upon their occurrence</p> <p>E.g. Random ground checks are conducted by the programme teams on the partners</p>	<p>Designed to take corrective action and reduce the impact of the risk</p> <p>E.g. Crisis Communication Plan to manage the expectations of the affected stakeholders upon a crisis</p>

Areas for Improvement – Measures which need to be taken to strengthen the current control environment (e.g. strengthen existing controls, develop additional controls), so as to reduce the current level of risk to an acceptable level. Responsibility and timeline for the completion of each action plan should be assigned for the purpose of implementation and tracking its timely completion.

Examples of areas for improvement:

Ref	Description	Responsibility	Timeline
R1.AP1	Develop a larger talent pool: Continue identifying talents through the High Potential Assessment Exercise and offer them training to improve their key skills ("Leadership; Analysis & Judgement; Managing Complexity; and Achievements & Values Driven") and coaching from Heads of Departments and above.	HR	FY 17/18
R1.C2	Develop an Online Performance Management system for 360 Feedback, Goal Setting and Mid-Year Review.	HR	Q2 FY 17/18

Monitor and Report Risks

The Code of Governance for Charities and IPCs (2017) recommends that “the Board should ensure that reviews are conducted from time to time on the Charity’s controls, processes, key programmes and events”².

The internal and external environment of any Charity is constantly changing. ERM, similarly, cannot remain static. The risk universe, ‘Tier 1’ risk profile and risk registers should be monitored and reviewed at least annually to ensure continued relevance of ERM to the Charity.



² Code of Governance for Charities and Institutions of a Public Character (2017) issued by Charity Council

Appendix B: Developing and documenting the ERM framework

Key Principles

The ERM Framework provides the structure and guidance for the manner in which ERM activities should be carried out, in order to promote a common understanding and consistent ERM practices within the Charity. The Framework should minimally include documentation of the following components:

- Risk strategy – ERM direction and objectives typically set by the Board and Senior Management
- Risk governance structure, roles and responsibilities – Allocation and establishment of risk related responsibilities, accountabilities and structure across the Charity

- ERM process, tools and templates – Guidelines and tools to conduct and document the ERM process
- Risk reporting requirements – Protocols and format to report key risk information to Senior Management and Board

The completed ERM Framework should be validated by the Board and Senior Management to set the right tone at the top, and reviewed on a periodic (recommended annual) basis to ensure continued relevance to the Charity.

Risk Strategy

The Risk strategy provides the overall direction and objectives of ERM from Management to promote alignment of ERM efforts within the Charity.

Considerations when developing the overall risk strategy of the Charity may include the following:

- ‘Tone from the top’ that Management intends to set with respect to ERM in the Charity
- Key benefits that Management and Board hopes to reap from the ERM programme
- Realistic and achievable objectives taking into account ERM resources available to the Charity



Example of ERM objectives:

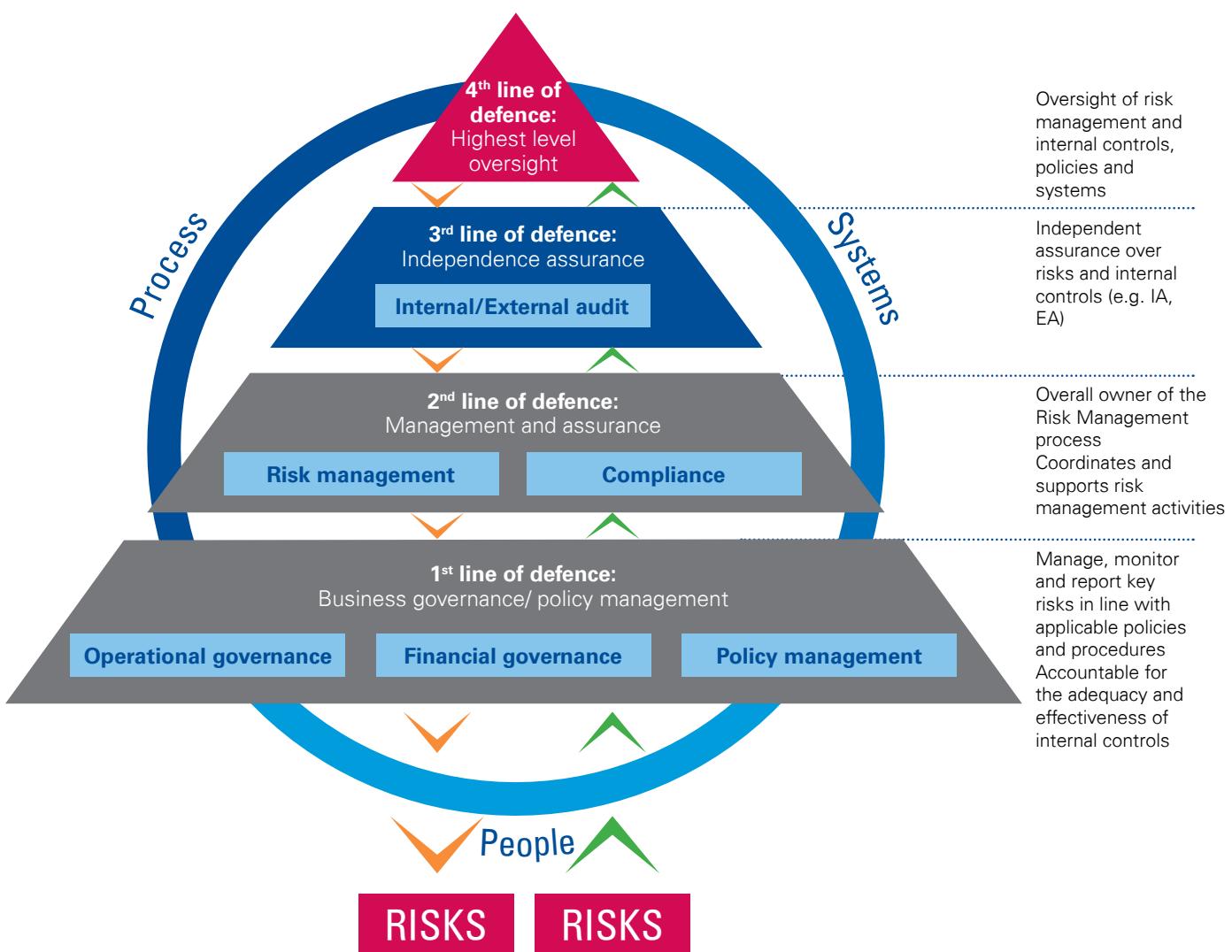
- Establish and maintain good governance and a sound system of internal controls;
- Facilitate the achievements of the organisation’s objectives and goals through better identification of opportunities, threats and managing them;
- Develop a common understanding of risk across multiple functions to manage risk cost-effectively on an enterprise-wide basis;
- Ensure compliance with the relevant regulatory and legal requirements;
- Develop and embed a strong risk culture;
- Encourage desired risk taking behaviours;
- Support risk-based decision-making; and
- Improve the organisation’s preparedness and resilience to unexpected events.

Risk Governance

The diagram below illustrates KPMG's 'four lines of defence' model which defines the key principles of a robust risk governance structure. Robust risk management and internal control systems rely on the formal establishment and linkage of the four lines of defence, with clear definition, interaction and segregation of roles and responsibilities.

Line management and supervisors responsible for carrying out daily operations must be the first line of defence against risks, playing a crucial role in managing them through adhering to policies and procedures, reporting risks as appropriate and

ensuring that controls are carried out as intended. The Board is ultimately responsible for the oversight of Risk Management and internal control systems within the Charity. The Code of Governance for Charities and IPCs (2017) also highlights the need to segregate the roles of the Board and Management, recommending that "a clear distinction should be made between their Board's role and their operational work"³, particularly in Charities where Board members for valid reasons, need to supervise the day-to-day operations of the Charities more closely (Basic II).

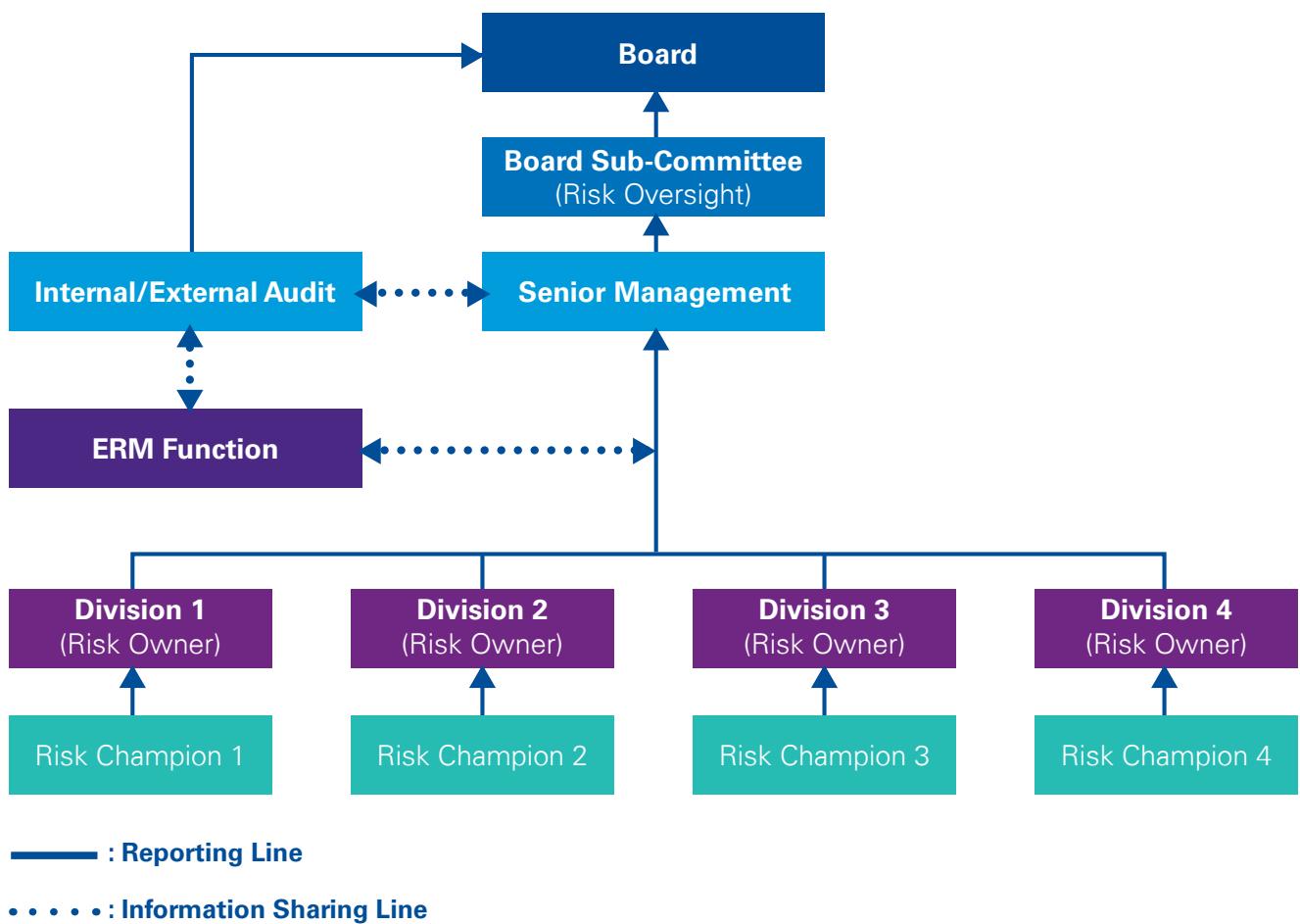


In order to better inculcate risk accountabilities and ensure appropriate segregation of duties between the four lines of defence, it is critical to establish a risk governance structure with clearly defined roles as well as indication of reporting and information sharing lines.

³Code of Governance for Charities and Institutions of a Public Character (2017) issued by Charity Council

Example of risk governance structure:

The risk governance structure should also be accompanied by defined and documented risk roles and responsibilities, outlining the key activities and responsibilities to be undertaken by respective parties (indicated in the risk governance structure) with respect to ERM.



Example of risk roles & responsibilities:

Audience	Roles & Responsibilities
 Board	<ul style="list-style-type: none"> Provides the overall guidance and advice on ERM matters, assisted by the Board Sub-Committee; and Appoint, and delegate the ERM oversight responsibility to the Board Sub-Committee.
 Senior Management	<ul style="list-style-type: none"> Provide guidance and direction on ERM and is responsible for implementing the ERM policy and framework; Set and instil the right culture throughout the Charity for effective risk governance; Ensure that the risks relevant to the Charity are properly identified, assessed and monitored; and Review the top risk (Tier 1 Risks) profile and ensure the mitigation responses are consistent with the risk appetite.
 Internal / External Audit	<ul style="list-style-type: none"> Provide independent assurance on the adequacy and effectiveness of the internal controls for the key risks; and Share insights with the ERM Function and Senior Management on significant issues and findings from the audits conducted, to feed into the risk management process.
 ERM Function	<ul style="list-style-type: none"> Maintain the ERM policy framework in line with industry better practices and the Charity's operating environment; Act as internal 'ambassador' and knowledge resource for ERM; Foster a corporate risk culture through adequate training and communication sessions; Liaise / coordinate with Risk Owners and Risk Champions on risk-related matters to obtain an enterprise-wide view of risks; and Prepare periodic risk reporting to the Board Sub-Committee and Board.
 Risk Owner	<ul style="list-style-type: none"> Identify, assess, monitor and report potential risks in their areas of responsibility; Complete / review risk registers (risk assessment etc.) for all Tier 1 Risks; and Monitor and report changes to existing risks or risk profile to Senior Management.

Enterprise Risk Management Process

Guidelines and tips on conducting the ERM process within the Charity should be documented in the ERM Framework (See Appendix A for more details on establishing the ERM process). Tools and templates that support the ERM Process (e.g. Risk parameters, matrix, registers etc.) should be included and documented as well.

Risk Reporting Requirements

Key reporting requirements to be included in the ERM Framework should minimally include:

- Frequency of periodic risk reporting to Senior Management / Board
- Key content to be reported (e.g. latest risk profile, summary of risk registers etc.)
- Responsible parties for reporting (e.g. Risk Owners, ERM function etc.)

Appendix C: Building risk awareness and understanding

Key Principles



People are often considered one of, if not the most, critical enabler of a successful and sustainable ERM programme in any Charity.

Risk management is the responsibility of everyone within a Charity, and all stakeholders need to minimally be aware of and understand 'how ERM works' in their context.

As ERM matures, it is critical to continuously build risk awareness, understanding and buy-in across all levels of stakeholders to ensure that ERM knowledge within the Charity remains relevant and up-to-date.

Tools to Build Risk Awareness

Various tools can be employed to effectively build risk awareness and understanding, especially in the context of Charities:

Workshops / Seminars



Traditionally, the main platform used to build risk awareness and understanding in a Charity is through face-to-face risk workshops / seminars. Depending on the group of stakeholders attending, the curriculum may be tailored to ensure optimal learning outcomes. Length of each workshop / seminar may range from 1.5 hours to a full-day session, depending on learning objectives.

E-learning Platforms



E-learning platforms are most useful to build risk awareness for Charities with a large number of staff at offsite locations on a regular basis. These platforms also provide more flexibility to staff who work regularly on a shift or rotation basis.

Newsletters and Posters



Periodic newsletters and posters are most useful for regular reminders and reinforcements of risk and risk management messages. Content in newsletters and posters should be kept direct and short, to ensure maximum reach to stakeholders.

Risk awareness, understanding and culture needs to be progressively and continuously built, especially as ERM in the Charity matures. It is recommended to conduct at least one ERM 'refresher' course annually to keep stakeholders apprised on latest ERM initiatives and updates, as well as recap on key risk and risk management concepts.

For Charities starting out on their ERM journey, it is recommended to consider using a mix of ERM

workshops and E-learning platforms to build risk awareness in a cost-efficient yet effective manner. A minimal number of ERM workshops may be conducted for key Staff such as Senior Management to provide an interactive learning platform, while E-learning can be used as a quick and efficient tool to build basic risk management awareness and knowledge among general staff.

Appendix D: Top risks by sector

Top Risks

The table below summarises the common top risks for each sector.

More details and guidelines on typical risk drivers, consequences and controls observed for the common top risks are presented in the following section.

Name of Risk	Sector						
	Arts	Community	Education	Health	Religious	Social & Welfare	Sports
Funding Risk	●	●		●	●	●	●
Risk of violation of Personal Data Protection Act		●	●	●	●	●	●
Non-Compliance with established laws and regulation risk		●	●	●	●	●	●
Conflict of interest e.g. related party transactions not at arm's length	●		●		●		●
Employee risk e.g. retention, disgruntled employees			●	●			●
Adverse Events Risk (Internal and External)	●		●				

Sample Risk Assessment for Common Top Risks

Note: The content outlined below are suggestions based on KPMG's experience with risk assessments completed for similar risks in Charities. The information presented is not meant to be exhaustive. Risk registers should be tailored to individual Charities to ensure the relevance and value of risk assessment exercises conducted.

Sample Risk Assessment for Funding Risk

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R3	Funding risk	Category	Financial	Risk Owner	Typically finance-related personnel / function in charge of fundraising																																					
Risk Description																																										
Inability to meet short term financial obligations arising from decreases in funding.																																										
Risk Causes / Drivers			Risk Consequences																																							
<ul style="list-style-type: none"> Lack of communication with key non-government partners and/or corporations Negative media / publicity adversely impacting the charity's reputation and funding 			<ul style="list-style-type: none"> Heavy reliance on government sources of funding Greater need to utilise charity's reserves to carry out operational activities Inability to purchase adequate equipment / replacement of equipment 																																							
Risk Assessment - Rating																																										
<p>Typically <u>moderate</u> likelihood and <u>high</u> impact risk, especially in Singapore's context.</p> <p>Most Charities in Singapore rely (to an extent) on non-Government funding to supplement the costs from activities, holding events and carrying out day-to-day operations.</p>			<table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Almost Certain (5)</td><td>Yellow</td><td>Yellow</td><td>Red</td><td>Red</td></tr> <tr><td>Likely (4)</td><td>Blue</td><td>Light Yellow</td><td>Light Yellow</td><td>Red</td></tr> <tr><td>Possible (3)</td><td>Green</td><td>Light Blue</td><td>Yellow</td><td>Red</td></tr> <tr><td>Unlikely (2)</td><td>Green</td><td>Light Green</td><td>Light Blue</td><td>Yellow</td></tr> <tr><td>Rare (1)</td><td>Green</td><td>Green</td><td>Dark Blue</td><td>Yellow</td></tr> <tr><td></td><td>Insignificant (1)</td><td>Minor (2)</td><td>Moderate (3)</td><td>Major (4)</td><td>Severe (5)</td></tr> <tr><td></td><td colspan="5" rowspan="2" style="text-align: center;">Magnitude of impact</td></tr> </table> <p style="color: red; font-weight: bold; margin-top: 10px;">Risk typically rated in this zone</p>			Almost Certain (5)	Yellow	Yellow	Red	Red	Likely (4)	Blue	Light Yellow	Light Yellow	Red	Possible (3)	Green	Light Blue	Yellow	Red	Unlikely (2)	Green	Light Green	Light Blue	Yellow	Rare (1)	Green	Green	Dark Blue	Yellow		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)		Magnitude of impact				
Almost Certain (5)	Yellow	Yellow	Red	Red																																						
Likely (4)	Blue	Light Yellow	Light Yellow	Red																																						
Possible (3)	Green	Light Blue	Yellow	Red																																						
Unlikely (2)	Green	Light Green	Light Blue	Yellow																																						
Rare (1)	Green	Green	Dark Blue	Yellow																																						
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)																																					
	Magnitude of impact																																									
Existing Controls / Mitigating Measures																																										
Ref	Description		Responsible Party	Remarks																																						
R3.C1	Establish a Media Response policy.		Corporate Communications																																							
R3.C2	Monitoring of fund utilisation and allocation.		Fundraising																																							
R3.C3	Compensation benchmarking survey (covering all levels of staff, local, overseas and key personnel) towards the competitors conducted annually.		Fundraising																																							
Areas for Improvement																																										
Ref	Description			Responsibility	Timeline																																					
	Areas for improvement are typically identified as necessary to further strengthen controls.																																									

Sample Risk Assessment for Non-compliance with Personal Data Protection Act (PDPA)

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R3	Risk of violation of Personal Data Protection Act (PDPA)	Category	Compliance	Risk Owner	Typically a Data Protection Officer (DPO) or equivalent personnel / function
Risk Description					
Risk of non-compliance with PDPA					
Risk Causes / Drivers			Risk Consequences		
<ul style="list-style-type: none"> Lack of awareness amongst staff on data confidentiality (e.g. requirements under PDPA) Unintentional revealing of information to unauthorised parties 			<ul style="list-style-type: none"> Public complaints Loss of public confidence Reputation damage from negative media reports Regulatory fines 		
Risk Assessment - Rating					
<p>Typically, <u>moderate</u> likelihood and <u>high</u> impact risk, especially in Singapore's context.</p> <p>As operational staff have access to often sensitive or confidential information, poor oversight or lack of good practices when protecting or securing confidential data may present the opportunity for this risk to occur.</p>			<p>Risk typically rated in this zone</p>		
Existing Controls / Mitigating Measures					
Ref	Description		Responsible Party	Remarks	
R3.C1	All staff are required to attend and complete a mandatory PDPA course upon joining the charity.		DPO		
R3.C2	Non-Disclosure Agreements (NDA) are signed by third parties or external vendors to prevent unintentional / intentional leakage of confidential or privileged information / data.		Legal		
R3.C3	Compensation benchmarking survey (covering all levels of staff, local, overseas and key personnel) towards the competitors conducted annually.		IT		
R3.C4	Clauses which require vendors to comply with PDPA when handling sensitive information is included in standard contractual terms and conditions.		Legal		
Areas for Improvement					
Ref	Description			Responsibility	Timeline
	Areas for improvement are typically identified as necessary to further strengthen controls.				

Sample Risk Assessment for Non-compliance with Established Laws, Regulations, and Code of Governance Risk

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R4	Non-compliance with established laws, regulations, Code of Governance risk	Category	Compliance	Risk Owner	Typically compliance / legal-related personnel / function
Risk Description					
(A) Failure to comply with legal, regulatory or contractual requirements, and significant breach of code of ethics and conduct or accepted industry practices; and/or (B) Unfavourable changes in regulatory guidelines and statutes that may have a high impact on business strategy, operations, funding and safety requirements etc.					
Risk Causes / Drivers			Risk Consequences		
<ul style="list-style-type: none"> Failure to understand and accept regulatory policies and standards Lack of strong management emphasis / focus 			<ul style="list-style-type: none"> Inquiry and investigation by authorities (e.g. Ministry of Health) Financial loss (if fines are imposed) Non-renewal of annual licensing Damage to reputation 		
Risk Assessment - Rating					
Typically, <u>low to moderate</u> likelihood and <u>high</u> impact risk, especially in Singapore's context. A Singapore registered Charity may lose its status as an Institution of a Public Character (IPC), hence the significantly higher magnitude of impact should this risk occur.			<div style="position: absolute; right: 0; top: 0;"> Risk typically rated in this zone </div>		
Existing Controls / Mitigating Measures					
Ref	Description		Responsible Party	Remarks	
R4.C1	Quarterly in-house trainings are conducted by Heads of Departments (HODs) or Training and Development team on external regulatory compliance matters for all general staff.		HR		
R4.C2	A staff disciplinary framework is in place to ensure adherence to external regulatory compliance matters. This is embedded within the staff performance review.		HR		
R4.C3	Annual internal audit and testing is conducted by an outsourced external party to ensure that any breach of external regulatory compliance issues are detected.		Finance		
Areas for Improvement					
Ref	Description		Responsibility	Timeline	
	Areas for improvement are typically identified as necessary to further strengthen controls.				

Sample Risk Assessment for Conflict of Interest Risk

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R1	Conflict of interest	Category	Compliance	Risk Owner	Typically Head of Compliance or Finance function
Risk Description					
Less favourable transactions entered into by management with related vendors (e.g. related party transactions not at arm's length).					
Risk Causes / Drivers		Risk Consequences			
<ul style="list-style-type: none"> Insufficient or Non-compliance to policies and procedures (e.g. procurement, vendor management SOPs etc.) Lack of communications or training on relevant SOPs 		<ul style="list-style-type: none"> Financial loss / Sub-optimal use of resources Negative media publicity and loss of stakeholder confidence should transactions be in breach of regulations (e.g. fraud and corruption) Operational disruptions due to investigations 			
Risk Assessment - Rating					
Typically, <u>low to medium</u> likelihood and <u>medium</u> impact risk.					
Typically, Charities have controls in place to manage this risk including SOPs, conflict of interest declarations etc. However, enforcement and effectiveness of controls may be a challenge in this area. Should the risk happen, impact may include adverse media publicity and wastage / loss of resources.		<p style="color: red; font-weight: bold;">Risk typically rated in this zone</p>			
Existing Controls / Mitigating Measures					
Ref	Description		Responsible Party	Remarks	
R1.C1	Procurement and Vendor Management policies and procedures in place including: <ul style="list-style-type: none"> Three quotes for procurements above a pre-defined value threshold Approval matrix in place for procurement and key transactions Due diligence process to be conducted on potential and approved vendors Reporting of potential related party transactions with follow up actions Disciplinary actions for non-compliance to policies and procedures.		Finance		
R1.C2	All parties involved in evaluation of quotations and tenders to sign Conflict of Interest declarations on a transaction basis.		Finance		
Areas for Improvement					
Ref	Description		Responsibility	Timeline	
	Areas for improvement are typically identified as necessary to further strengthen controls.				

Sample Risk Assessment for Employee Risk

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R5	Employee risk e.g. retention, disgruntled employees	Category	Operational	Risk Owner	Typically a Human Resource personnel / function																																			
Risk Description																																								
Inability to attract and retain the right talent with the required skill-set and competencies to takeover key positions which may result in disruption to operations, loss of institutional knowledge and inability to achieve long term strategic thrusts.																																								
Risk Causes / Drivers			Risk Consequences																																					
<ul style="list-style-type: none"> • Lack of strong 'corporate culture' and 'brand' • Lack of long term career development plans / roadmap 			<ul style="list-style-type: none"> • Operational inefficiency / disruption • Poor employee morale (E.g. heavier workload) 																																					
Risk Assessment - Rating																																								
<p>Typically moderate to high likelihood and moderate impact risk, especially in Singapore's context.</p> <p>Most Charities in Singapore have difficulty in competing with private-sector companies in terms of average compensation and benefits due to financial constraints, hence the higher likelihood.</p>			<table border="1"> <thead> <tr> <th colspan="5">Likelihood of Occurrence</th> </tr> <tr> <th>Almost Certain (5)</th> <th>Likely (4)</th> <th>Possible (3)</th> <th>Unlikely (2)</th> <th>Rare (1)</th> </tr> </thead> <tbody> <tr> <th>Insigificant (1)</th> <td>Yellow</td> <td>Yellow</td> <td>Red</td> <td>Red</td> </tr> <tr> <th>Minor (2)</th> <td>Blue</td> <td>Yellow</td> <td>Yellow</td> <td>Red</td> </tr> <tr> <th>Moderate (3)</th> <td>Green</td> <td>Light Blue</td> <td>Yellow</td> <td>Red</td> </tr> <tr> <th>Major (4)</th> <td>Green</td> <td>Light Blue</td> <td>Blue</td> <td>Yellow</td> </tr> <tr> <th>Severe (5)</th> <td>Green</td> <td>Light Blue</td> <td>Blue</td> <td>Orange</td> </tr> </tbody> </table> <p style="color: red; font-weight: bold;">Risk typically rated in this zone</p>			Likelihood of Occurrence					Almost Certain (5)	Likely (4)	Possible (3)	Unlikely (2)	Rare (1)	Insigificant (1)	Yellow	Yellow	Red	Red	Minor (2)	Blue	Yellow	Yellow	Red	Moderate (3)	Green	Light Blue	Yellow	Red	Major (4)	Green	Light Blue	Blue	Yellow	Severe (5)	Green	Light Blue	Blue	Orange
Likelihood of Occurrence																																								
Almost Certain (5)	Likely (4)	Possible (3)	Unlikely (2)	Rare (1)																																				
Insigificant (1)	Yellow	Yellow	Red	Red																																				
Minor (2)	Blue	Yellow	Yellow	Red																																				
Moderate (3)	Green	Light Blue	Yellow	Red																																				
Major (4)	Green	Light Blue	Blue	Yellow																																				
Severe (5)	Green	Light Blue	Blue	Orange																																				
Existing Controls / Mitigating Measures																																								
Ref	Description		Responsible Party	Remarks																																				
R5.C1	Credentials and background checks are performed on all staffs where possible referrals are required (including written referrals).		HR																																					
R5.C2	Comprehensive talent development programme aligned to Performance Management framework to develop talent from within, reviewed on an annual basis.		HR																																					
R5.C3	Salary benchmarking is undertaken on an annual basis to assess the competitiveness of the charity's salary and compensation packages against its peers.		HR																																					
Areas for Improvement																																								
Ref	Description		Responsibility	Timeline																																				
	<i>Areas for improvement are typically identified as necessary to further strengthen controls.</i>																																							

Sample Risk Assessment for Adverse Events Risk

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R2	Adverse events risk	Category	Operational	Risk Owner	Typically personnel / function in charge of Business Continuity																									
Risk Description																														
Failure to effectively manage and/or respond to force majeure crisis (e.g. haze, serious pandemic, typhoons, floods) or man-made events (e.g. terrorist attack) resulting in interruption to business.																														
Risk Causes / Drivers		Risk Consequences																												
<ul style="list-style-type: none"> Acts of God (external environment) 		<ul style="list-style-type: none"> Operational disruptions Injury or death of staff Damage to assets Loss of key data Financial loss (e.g. asset replacement costs) 																												
Risk Assessment - Rating																														
<p>Typically <u>low</u> likelihood and <u>high</u> impact risk, especially in Singapore's context.</p> <p>Singapore is not in a natural disaster prone region, but should such events happen, impact in terms of operational disruption could be prolonged and severe.</p>		<table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Almost Certain (5)</td><td>Yellow</td><td>Red</td><td>Red</td><td>Red</td></tr> <tr><td>Likely (4)</td><td>Blue</td><td>Yellow</td><td>Red</td><td>Red</td></tr> <tr><td>Possible (3)</td><td>Green</td><td>Blue</td><td>Yellow</td><td>Red</td></tr> <tr><td>Unlikely (2)</td><td>Green</td><td>Green</td><td>Light Blue</td><td>Yellow</td></tr> <tr><td>Rare (1)</td><td>Green</td><td>Green</td><td>Light Blue</td><td>Red</td></tr> </table>				Almost Certain (5)	Yellow	Red	Red	Red	Likely (4)	Blue	Yellow	Red	Red	Possible (3)	Green	Blue	Yellow	Red	Unlikely (2)	Green	Green	Light Blue	Yellow	Rare (1)	Green	Green	Light Blue	Red
Almost Certain (5)	Yellow	Red	Red	Red																										
Likely (4)	Blue	Yellow	Red	Red																										
Possible (3)	Green	Blue	Yellow	Red																										
Unlikely (2)	Green	Green	Light Blue	Yellow																										
Rare (1)	Green	Green	Light Blue	Red																										
Existing Controls / Mitigating Measures																														
Ref	Description		Responsible Party	Remarks																										
R2.C1	<p>A Business Continuity Plan (BCP) is in place covering key operations and processes to address key adverse events / scenarios including:</p> <ul style="list-style-type: none"> Loss of access to building premises Loss of computing services, power, utilities, etc. <p>Mass staff quarantine in the event of pandemics.</p>		Administration																											
R2.C2	<p>Critical systems and data are backed up daily. Backup data is kept on off-site servers with documented SOPs to restore critical systems using backup.</p>		IT																											
R2.C3	<p>Communications backups are in place in the event of failure of email system, including direct phone and fax lines.</p>		IT																											
R2.C4	<p>Fire drills are conducted periodically in line with SCDF guidelines, with findings and attendance documented.</p>		Administration																											
Areas for Improvement																														
Ref	Description		Responsiblity	Timeline																										
	<i>Areas for improvement are typically identified as necessary to further strengthen controls.</i>																													

Appendix E: Sample operational risk registers by sector

Note: The content outlined below are suggestions based on KPMG's experience with risk assessments completed for similar risks in Charities. The information presented is not meant to be exhaustive. Risk registers should be tailored to individual Charities to ensure relevance and value of risk assessment exercises conducted.

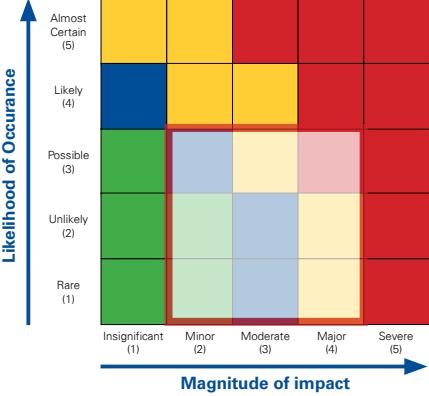
Sample Risk Register for Arts

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R1	Project Management Risk	Category	Operational	Risk Owner	Typically Project team and/or Director of Productions
Risk Description					
A lack of sufficient planning and management of arts events, resulting in an uncertain event or condition that, if it occurs, has a positive or negative effect on the charity.					
Risk Causes / Drivers			Risk Consequences		
<ul style="list-style-type: none"> Underperformance of vendors / partners Poor project planning and budgeting Lack of appropriate skill sets and experience to manage projects Partnership with parties who lack integrity, professionalism, capabilities or commitment to follow through on objectives 			<ul style="list-style-type: none"> Cost overruns in events Adverse publicity from negative media reports Complaints from event attendees Loss of stakeholders' confidence due to unsatisfactory delivery 		
Risk Assessment - Rating					
<p>Typically <u>medium</u> likelihood and <u>high</u> impact risk, especially in Singapore's context.</p> <p>Art scene in Singapore is growing and frequency of events is largely cyclical. Impact, however, is typically in the high zone due to the potential reputational impacts of such incidents to the charity due to the large number of attendees at events.</p>			<p style="color: red; font-weight: bold;">Risk typically rated in this zone</p>		
Existing Controls / Mitigating Measures					
Ref	Description		Responsible Party	Remarks	
R1.C1	Pre-assessment by staff on potential companies for partnerships - staff will discuss with companies to define and set parameters and expectations for the partner.		Development		
R1.C2	Identification of key Director of Productions with necessary experience to lead the productions / events.		Artistic		
R1.C3	Ongoing monitoring and updates on events are held to identify key areas for follow up.		Production		
R1.C4	Post mortem review of production / events to identify areas for improvement for following productions / events.		Production		
R1.C5	Production / event budget established prior to event and monitored throughout the event.		Finance		
Areas for Improvement					
Ref	Description		Responsibility	Timeline	
	<i>Areas for improvement are typically identified as necessary to further strengthen controls.</i>				

Sample Risk Register for Social and Welfare

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R1	Programme / outcome management	Category	Operational	Risk Owner	Typically personnel / function in charge of the programme / activity
Risk Description					
Lack of monitoring and reporting of programme outcomes resulting in inability to achieve programme objectives.					
Risk Causes / Drivers		Risk Consequences			
<ul style="list-style-type: none"> Key Performance Indicators (KPIs) are not clearly established Periodic reporting mechanisms are not in place Programme objectives are not clearly communicated 		<ul style="list-style-type: none"> Programme objectives not achieved Insufficient programme funding Forfeit of grants received Loss of reputation 			
Risk Assessment - Rating					
<p>Typically <u>low</u> likelihood and <u>moderate</u> impact risk, especially in Singapore's context.</p> <p>Due to the regulatory environment in Singapore, the likelihood is low. Impact is also typically in the moderate zone due to the potential reputational impacts and affect the ability to get grants and funding.</p>		 <p>Risk typically rated in this zone</p>			
Existing Controls / Mitigating Measures					
Ref	Description		Responsible Party	Remarks	
R1.C1	Establish clear KPIs and objectives for each programme.		Programme Management		
R1.C2	Regularly review the outcome against KPIs and budget to be reported to senior management / Board / Management committee.		Programme Management		
R1.C3	Any variances and deviations are investigated and justified.		Programme Management		
R1.C4	Strategic planning is performed every 3 to 5 years to review the mission and the programmes of the Charity.		Executive Director		
Areas for Improvement					
Ref	Description		Responsibility	Timeline	
	Areas for improvement are typically identified as necessary to further strengthen controls.				

Sample Risk Register for Education

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R1	Awarding of scholarships / grants to ineligible or unintended applicants	Category	Operational	Risk Owner	Typically personnel / function in charge scholarships																									
Risk Description																														
Proper due diligence is not carried out prior to approving the awarding of scholarships / financial assistance to applicants, resulting in grants given to ineligible or unintended applicants.																														
Risk Causes / Drivers		Risk Consequences																												
<ul style="list-style-type: none"> Clear criteria not established in the assessment of applicants Lack of independent checks and conflict of interest management No process of document authentication and verification 		<ul style="list-style-type: none"> Waste / abuse of Charities' funds Negative publicity thereby affecting the Charities' reputation Intended beneficiaries not reached Charities' objects not achieved 																												
Risk Assessment - Rating																														
<p>Typically <u>medium</u> likelihood and <u>medium</u> impact risk, especially in Singapore's context.</p> <p>Inherently, due to relatively high volumes of applicants requiring financial assistance and other support, likelihood of the risk occurring is typically 'medium'. However, the quantum of each case of financial aid is typically not very high; hence the impact is moderate.</p>		<table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>																												
Risk typically rated in this zone																														
Existing Controls / Mitigating Measures																														
Ref	Description		Responsible Party	Remarks																										
R1.C1	Establish a clear and measurable criteria in the evaluation.		Finance																											
R1.C2	Provide training to all staff involved in the award process to communicate clear guidelines and criteria.		HR																											
R1.C3	Establish process to manage conflict of interest.		HR																											
R1.C4	Establish clear procedures to carry out due diligence, which includes proper authentication of supporting documents and having independent checks.		Finance																											
Areas for Improvement																														
Ref	Description		Responsibility	Timeline																										
	<i>Areas for improvement are typically identified as necessary to further strengthen controls.</i>																													

Sample Risk Register for Health

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R1	Risk of sub-standard Clinical care	Category	Operational	Risk Owner	Typically personnel / function in charge of medical / clinical services
Risk Description					
Sub-standard clinical care, professional negligence by act or omission by a healthcare professional in which the treatment provided falls below the accepted standard of practice in the medical community and threatens patients' physical and/or mental well-being.					
Risk Causes / Drivers			Risk Consequences		
<ul style="list-style-type: none"> • Human error / fatigue • Poor understanding of clinical SOPs / work instructions • Lack of regular competency checks on healthcare professional • Insufficient / ineffective safety checks on staff, nurses or volunteers • Lack of incident reporting channels / near misses 			<ul style="list-style-type: none"> • Families / Patients complaints • Patient pre-mature deaths and/or injuries • Liability claims and costs, investigations • Adverse publicity from negative media reports 		
Risk Assessment - Rating					
<p>Typically <u>low</u> likelihood and <u>high</u> impact risk, especially in Singapore's context.</p> <p>Healthcare in Singapore is a relatively regulated sector, likelihood and frequency of such medical incidents tend to be low. Impact, however, is typically in the high or extreme zone due to the potential reputational impacts of such incidents to the Charity.</p>			<p style="color: red; font-weight: bold;">Risk typically rated in this zone</p>		
Existing Controls / Mitigating Measures					
Ref	Description		Responsible Party	Remarks	
R1.C1	Background and reference checks are performed on potential new hires to assess suitability of the candidate to the charity and role.		HR		
R1.C2	Ongoing monitoring and tracking to ensure all clinical staff involved in delivery of patient care services have the required valid licenses and certifications to carry out their respective work responsibilities.		Clinical Services		
R1.C3	All new staff are required to go through a mandatory orientation and on-the-job training programme to familiarise with scope of work, clinical processes / SOPs, and roles and responsibilities.		HR		
R1.C4	Formal incident reporting process in place for staff to report clinical and patient care related incidents, including reporting channels, escalation protocols, investigative procedure etc.		Clinical Services		
R1.C5	Periodic spot checks or audits are conducted on key clinical processes and services to ensure standard of care is maintained.		Clinical Services		
Areas for Improvement					
Ref	Description		Responsiblity	Timeline	
	Areas for improvement are typically identified as necessary to further strengthen controls.				

Sample Risk Register for Religious

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R1	Money laundering and terrorist financing	Category	Operational	Risk Owner	Chief Financial Officer / Chief Executive Officer
Risk Description					
Inability to detect and report suspicious activities that may relate to money laundering and terrorism financing.					
Risk Causes / Drivers			Risk Consequences		
<ul style="list-style-type: none"> • Lack of awareness of the risk and implications of money laundering • No established procedures to perform due diligence on donors • Lack of staff training 			<ul style="list-style-type: none"> • Non-compliance with regulations, resulting to potential penalties • Loss of reputation • Activities are not in line with the Charity's objectives 		
Risk Assessment - Rating					
<p>Typically <u>possible</u> likelihood and <u>high</u> impact risk, especially in Singapore's context.</p> <p>Due to the nature of activities, including overseas missions and tie ups with foreign institutions, the likelihood is possible. Impact is also typically in the high or extreme zone due to the potential reputational impacts of being involved in money laundering activities.</p>			<p>Risk typically rated in this zone</p>		
Existing Controls / Mitigating Measures					
Ref	Description		Responsible Party	Remarks	
R1.C1	Establish procedures to conduct due diligence checks for major donors, especially those from overseas.		Finance / Fundraising		
R1.C2	Establish a framework for the identification and reporting of suspicious transactions.		Finance / Fundraising		
R1.C3	Conduct training to increase staff awareness of money laundering.		HR		
R1.C4	Establish approval limits to ensure expenditure are in line with the charity's objectives.		Finance		
R1.C5	Establish procedures for overseas financial transactions to go through licensed financial channels.		Finance		
Areas for Improvement					
Ref	Description		Responsibility	Timeline	
	Areas for improvement are typically identified as necessary to further strengthen controls.				

Sample Risk Register for Sports

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R1	Sports infrastructure and facilities risk	Category	Operational	Risk Owner	Typically personnel / function in charge of planning / scheduling of events
Risk Description					
Inability to secure suitable / adequate sports facilities to meet the charity's needs (e.g. for events, competitions, trainings etc.).					
Risk Causes / Drivers		Risk Consequences			
<ul style="list-style-type: none"> Lack of suitable infrastructure or facilities available in Singapore Insufficient budget to acquire / develop facilities Inability to secure facilities on a long-term lease 		<ul style="list-style-type: none"> Disruption to competition and training schedules Loss of business or commercial opportunities Negative impact to crowd experience during competitions and events Negative impact to development and performance of athletes 			
Risk Assessment - Rating					
<p>Typically <u>medium</u> likelihood and <u>medium</u> impact risk.</p> <p>In a land-scarce country like Singapore, competing uses of land and facilities means that Charities may not always be able to secure suitable facilities for their uses. When such situations arise, potential impacts may include loss of opportunities or re-scheduling of events, but is typically unlikely to severely threaten the reputation or ongoing operations of the Charity.</p>			<p>Risk typically rated in this zone</p>		
Existing Controls / Mitigating Measures					
Ref	Description	Responsible Party		Remarks	
R1.C1	Channels in place to provide regular feedback to authorities on expected future needs in terms of sports infrastructure development.	Programme Management			
R1.C2	Events, competitions and trainings are planned in advance, with regular communications with partners / organisers / sponsors on schedule and facilities.	Programme Management			
R1.C3	Information of availability of facilities are available to relevant parties (e.g. schools, the public other sports charities etc.).	Programme Management			
R1.C4	Regular communications to venue owners to explore and discuss options for longer term leases where appropriate.	Marketing and Communications			
R1.C5	Documented guidelines and criteria in place to prioritise reservations of sports facilities.	Administration			
Areas for Improvement					
Ref	Description	Responsibility		Timeline	
	<i>Areas for improvement are typically identified as necessary to further strengthen controls.</i>				

Sample Risk Register for Community

The sample risk register provides a guideline of how a risk register on this risk may be completed.

R1	Grants or funds awarded not used in line with approved objective	Category	Operational	Risk Owner	Typically personnel / function in charge of the programme / activity																														
Risk Description																																			
Lack of monitoring over use of grants / funds by recipients to ensure that the funds disbursed are used in line with the initial approved objectives.																																			
Risk Causes / Drivers		Risk Consequences																																	
<ul style="list-style-type: none"> Periodic reporting mechanisms from grant / fund recipients are not in place Process for following up with late or delayed submissions is not in place Periodic evaluation and review of grants / funds usage is not performed 		<ul style="list-style-type: none"> Unauthorised use of grant/funds by recipient may not be identified in a timely manner Waste of charity funds Programme objectives not achieved Forfeit of grants received Loss of reputation 																																	
Risk Assessment - Rating																																			
<p>Typically <u>medium</u> likelihood and <u>medium</u> impact risk, especially in Singapore's context.</p> <p>Inherently, due to number of applicants requiring financial assistance and other support, likelihood of the risk occurring is typically 'medium'. However, the quantum of each case of financial aid is typically not very high; hence the impact is moderate.</p>		<table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Almost Certain (5)</td><td>Yellow</td><td>Yellow</td><td>Red</td><td>Red</td><td>Red</td></tr> <tr><td>Likely (4)</td><td>Blue</td><td>Orange</td><td>Light Yellow</td><td>Pink</td><td>Red</td></tr> <tr><td>Possible (3)</td><td>Green</td><td>Light Blue</td><td>Yellow</td><td>Pink</td><td>Red</td></tr> <tr><td>Unlikely (2)</td><td>Green</td><td>Light Green</td><td>Light Blue</td><td>Yellow</td><td>Red</td></tr> <tr><td>Rare (1)</td><td>Green</td><td>Green</td><td>Blue</td><td>Yellow</td><td>Red</td></tr> </table> <p style="color: red; font-weight: bold;">Risk typically rated in this zone</p>				Almost Certain (5)	Yellow	Yellow	Red	Red	Red	Likely (4)	Blue	Orange	Light Yellow	Pink	Red	Possible (3)	Green	Light Blue	Yellow	Pink	Red	Unlikely (2)	Green	Light Green	Light Blue	Yellow	Red	Rare (1)	Green	Green	Blue	Yellow	Red
Almost Certain (5)	Yellow	Yellow	Red	Red	Red																														
Likely (4)	Blue	Orange	Light Yellow	Pink	Red																														
Possible (3)	Green	Light Blue	Yellow	Pink	Red																														
Unlikely (2)	Green	Light Green	Light Blue	Yellow	Red																														
Rare (1)	Green	Green	Blue	Yellow	Red																														
Existing Controls / Mitigating Measures																																			
Ref	Description		Responsible Party	Remarks																															
R1.C1	Establish reporting timeline for each recipient.		Finance																																
R1.C2	Periodic review of the submissions for each recipient to ascertain that the use of the funds is in line with the initial approved objective.		Finance																																
R1.C3	Any variances and deviations are justified and revisions approved.		Finance																																
Areas for Improvement																																			
Ref	Description		Responsibility	Timeline																															
	Areas for improvement are typically identified as necessary to further strengthen controls.																																		

About Us

Charity Council

The Charity Council aims to promote and encourage the adoption of good governance and best practices, to help enhance public confidence and promote self-regulation in the charity sector. It also aims to help build capabilities of Charities and IPCs to enable them to comply with regulatory requirements and enhance public accountability. In addition, the Council advises the Commissioner of Charities (COC) on key regulatory issues such as proposals on new regulations, where there may be broad-ranging impact on charities and IPCs.

The Charity Council comprises 15 members, including the Chairman. 10 members are from the people sector, chosen for their expertise in accountancy, corporate governance, entrepreneurship and law. They are also involved in volunteer and charity work in varied fields such as arts and heritage, community, education, health and social services.

KPMG

KPMG in Singapore is part of a global network of professional services firms providing Audit, Tax and Advisory services. The KPMG network operates in 152 countries, with more than 189,000 people working in member firms around the world. In the ASEAN region, member firms operate across all 10 countries of this regional grouping providing professional services supporting the growth, compliance and performance objectives of their clients.

KPMG's experience and investment in the Charities/ IPCs sector translates to specialised knowledge that can help meet the sector's specific needs. Its dedicated team of professionals in Risk Consulting has assisted the Sector Administrators from the various ministries in reviewing more than 100 Charities/IPCs since the enactment of the Charity's rules and regulations, and has made recommendations to improve the governance, risk and compliance framework in these Charities and IPCs.

NUS Business School

The National University of Singapore (NUS) Business School is known for providing management thought leadership from an Asian perspective, enabling its students and corporate partners to leverage global knowledge and Asian insights.

The school has consistently received top rankings in the Asia-Pacific region by independent publications and agencies, such as The Financial Times, Economist Intelligence Unit, and Quacquarelli Symonds (QS) Top MBA, in recognition of the quality of its programmes, faculty research and graduates. In the Financial Times Global Rankings, the NUS MBA was ranked 26th in 2017, while the NUS-UCLA Executive MBA and Asia-Pacific Executive MBA were ranked 6th and 17th respectively in 2016.

In the biannual Forbes rankings for two-year MBA programmes, NUS Business School was ranked 7th among business schools outside the United States in 2015. QS has also ranked the school 12th in the world for accounting and finance.

The school is accredited by AACSB International (Association to Advance Collegiate Schools of Business) and EQUIS (European Quality Improvement System), endorsements that the school has met the highest standards for business education. The school is also a member of the GMAC Council, Executive MBA Council, Partnership in Management (PIM) and CEMS (Community of European Management Schools).

Notes

Contact us

Charity Council

Charity Council Secretariat

E : Charity_council_sec@mccy.gov.sg

www.charitycouncil.org.sg

KPMG in Singapore

Irving Low

Partner, Head of Risk Consulting

E : irvinglow@kpmg.com.sg

Tea Wei Li

Director, Risk Consulting

E : wtea@kpmg.com.sg

www.kpmg.com.sg

National University of Singapore Business School

Richard Tan

Adjunct Associate Professor

Department of Accounting, NUS Business School

E : biztclr@nus.edu.sg

Susan See Tho

Senior Lecturer

Department of Accounting, NUS Business School

E : susan.seetho@nus.edu.sg

<http://bschool.nus.edu.sg/>

Singapore Institute of Technology

Ho Yew Kee

Professor of Accounting

Associate Provost (SkillsFuture & Staff Development)

E : yewkee.ho@SingaporeTech.edu.sg

This publication was issued in June 2017.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 Charity Council, KPMG Services Pte. Ltd. and the National University of Singapore Business School. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without prior written permission from Charity Council, KPMG and NUS Business School.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.