

17 January 2022



**THE POWER OF BEING UNDERSTOOD**  
AUDIT | TAX | CONSULTING

# Contents

- Introduction 3
- Risk Management Pathfinder 4
- Road Map 9
- Appendices Index 10

# Risk Management Pathfinder

## Introduction

The aim of this risk management pathfinder exercise is to provide options as to how Cambridgeshire & Peterborough Combined Authority's (CPCA) approach to managing risk can be developed and strengthened. In some cases these will be "quick wins" as well as changes that may require a greater period of time or resources to achieve.

The risk management pathfinder is not an audit, instead it involves a high level assessment of key documents leading to the creation of an output that can be used for discussion with the CPCA Executive Team. The risk management pathfinder by its nature is not an all encompassing review of risk management. Management of course may decide that a more detailed review is required to achieve the outcome required following completion of the risk management pathfinder exercise.

This pathfinder contains three separate segments:

- Risk Framework Components
- Capability & Expertise
- Risk Management Hierarchy & Reporting

The options and suggestions arising from the pathfinder exercise are based purely on the RSM's risk management advisory knowledge and experience of managing risk from across all sectors. There on, any further action is for management to decide. These suggestions have been developed into a Road Map which can be found on page 9 of this document.

It should be noted that following the adoption of any of the suggestions from this pathfinder review, it will be important for the organisation to update its risk management strategy to ensure that it is reflective of any changes to the framework .

# Risk Management Pathfinder

## Risk Framework Components

Ref:	RSM Challenge:	RSM Comments:	RSM Slide Ref:
1.	<i>The risk register format is conducive to the effective recording of risks and associated information</i>	<p>The current risk register template is comprehensive, and provides scope for key information to be captured. The organisation uses 'cause and effect' analysis fields to help breakdown the risk narrative so that context can be provided to the end users. This area could be developed further with some small amendments to the template to ensure that there is a 'golden thread' for each risk. i.e. from risk description, inherent risk score, controls, residual risk score, improvement actions etc.</p> <p>It should be noted that the risk register document itself should be viewed as a data repository and the information contained within, used to inform risk reporting that is tailored to its audience.</p> <p><b>Suggested Action:</b> Revise the risk register template to ensure that the information for each risk flows in a logical manner and provides scope to capture any enhancements made regarding developments highlighted in this pathfinder, for example risk appetite and assurance mapping.</p>	Slide 13
2.	<i>There is an appropriate and effectively utilised risk scoring methodology</i>	<p>CPCA uses a multiplier scoring matrix which can lead to risk scores being unintentionally mis-leading. For example, one risk may have a score of impact 5, likelihood 1, equalling a score of 5, and another impact 1, likelihood 5, also equalling 5. These two risks have the same score, but would be managed very differently from a control, treatment plan and assurance perspective.</p> <p>By using a non multiplier scoring methodology, it ensures that risks are assessed appropriately with the emphasis on the level of impact for each risk. This model can allow for easier prioritisation, interpretation and avoid the example above occurring.</p> <p>There are limited descriptors for impact and likelihood within the scoring methodology. These could be enhanced to provide greater direction so that they assist in removing subjectivity around the scoring of the risks. For example, impacts for the following could be developed i.e. safety, quality, finance, regulatory, reputation.</p> <p><b>Suggested Action:</b> Amend the impact and likelihood matrix to a 'non-multiplier' and develop descriptors for the impact scale to help the assessment of risks and remove subjectivity.</p>	Slides 18, 19 and 20

# Risk Management Pathfinder

## Risk Framework Components

Ref:	RSM Challenge:	RSM Comments:	RSM Slide Ref:
3.	<i>There is a clearly defined and documented risk appetite statement</i>	<p>CPCA does not currently have a defined, Board agreed risk appetite in place. Putting a risk appetite approach in place, will assist management in understanding what level of risk is acceptable for different types of risk, meaning that management can more efficiently allocate and prioritise resources to mitigate risk to reach an acceptable risk score / exposure. For example, if a risk is deemed to be within its risk appetite, the challenge of whether or not further controls are required, should be made.</p> <p>This approach can then assist in driving a more dynamic risk reporting and monitoring approach, where risks which have lower appetites may receive greater visibility than those that the organisation is comfortable with.</p> <p><b>Suggested Action:</b> Develop a risk appetite statement and methodology that links to the impact and likelihood assessment. This will aid decision making, prioritisation of resources and targeted reporting.</p>	Slides 22, 23 and 24
4.	<i>Key controls are mitigating actions are clearly identified for each risk</i>	<p>The existing risk register template includes clear fields for current controls and future controls. There are however instances where the current control area includes actions that are being undertaken. It is therefore unclear what controls currently exist to manage the risks and what actions are required to address gaps in the control environment.</p> <p>All individual actions should be assigned to a named individual, with an expected implementation date, with action owners providing and recording regular updates on progress. This will assist with risk reporting because reports with just an action description provide no real update to Committees and Board on how that action is progressing month on month.</p> <p>It should also be noted the residual risk score and risk appetite should be used as a gauge for whether or not further action is required. There are currently examples within the risk registers where the residual risk scores are green and there are a number of actions identified.</p> <p><b>Suggested Action:</b> Review all actions or planned improvements to ensure that timescales are applied to encourage ownership and accountability. Ensure that these actions demonstrably mitigate the risk and are proportionate to the residual risk score and risk appetite applied.</p>	Slide 16

# Risk Management Pathfinder

## Risk Framework Components

Ref:	RSM Challenge:	RSM Comments:	RSM Slide Ref:
5.	<i>Assurances are mapped to the key control environment, providing visibility of control effectiveness.</i>	<p>Currently there is no formal assurance mechanism in place to capture the levels of confidence in the effectiveness of the control environment identified as part of the organisation’s corporate and directorate risk registers.</p> <p>A key development for CPCA as it moves forward will be to develop an ability to do this in a pragmatic and proportionate manner so that visibility of control effectiveness can be gained and reported on to the Audit and Governance Committee.</p> <p>By mapping assurances to the control environment for key risks, the organisation will be in a position to better inform its risk-based decision making and its allocation of resources moving forward. If proportionate to the risk exposure, assurance activity should be identified where assurances are not available / documented to ensure that a complete picture is obtained and weaknesses identified.</p> <p>One best practice method for capturing assurances is the adoption of the ‘three lines of defence’ model, where assurances are identified at different levels dependant up where the source has come from and the confidence it provides.</p> <p>This is not to say that assurances will be required or available for all controls or for all three lines of defence, as a proportionate approach is required, based upon the risk exposure and risk appetite for that risk.</p> <p><b>Suggested Action:</b> Develop a proportionate assurance gathering mechanism for capturing and demonstrating the effectiveness of controls identified for the Corporate Risk Register risks. This should include not just the assurance source but also the effectiveness rating.</p>	Slides 14, 15 and 17

# Risk Management Pathfinder

## Capability & Expertise

Ref:	RSM Challenge:	RSM Comments:	RSM Slide Ref:
6.	<i>There is sufficient dedicated risk management expertise and resource to enable the risk framework to be effectively facilitated.</i>	<p>The CPCA currently has limited risk management expertise within the organisation. The risk management framework is currently administrated by three non-specialist individuals with no risk management experience. In order for the organisation to have an effective risk management framework and process in place it should consider filling this gap in specialist skills and experience.</p> <p>There are a several options available to the organisation to ensure that the appropriate level of skills and expertise are in place. However it should be ensured that the individual responsible for risk, and who is effectively the 'risk manager' has sufficient gravitas and seniority within the management hierarchy to engage and challenge individuals.</p> <p>If recruitment is undertaken, the position should be considered in terms of seniority, as the equivalent to a 'Head of Internal Audit' and have a similar set of skills and experience in terms of communication, and understanding of risk, with an appropriate or relevant qualification. It will also be important to ensure that practical experience in terms of risk and the sector are present. Our experience however has been that individuals soon become engrained within an organisation and fail to remain objective as they become part of the organisation. We have outlined an alternative option for management to consider on Slide 25 which would allow for risk management to remain independent of the organisation and provide an impartial view and scrutiny over the risk framework.</p> <p><b>Suggested Action:</b> Consideration to be given as to the most appropriate channel to acquire specialist risk management expertise for CPCA to facilitate the risk management framework.</p>	Slide 25
7.	<i>There is a programme of risk management training in place to build capability within the organisation</i>	<p>On completion of enhancements to the CPCA risk management framework and updating of the risk management strategy, it will be key to engage with stakeholders. This should be done through developing an on-going cycle of risk management awareness training that is tailored to the audience, i.e. Board, Performance &amp; Risk Committee to build risk management capability.</p> <p><b>Suggested Action:</b> A risk management training programme should be developed and delivered that is tailored to suit the targeted group of individuals. i.e. Board, Audit &amp; Governance Committee, staff.</p>	N/A

# Risk Management Pathfinder

## Risk Management Hierarchy & Reporting

Ref:	RSM Challenge:	RSM Comments:	RSM Slide Ref:
8.	<i>There is a clear and appropriate risk register structure that allows for risks to be considered at the appropriate levels. i.e. strategic vs operational</i>	<p>The CPCA has a Corporate Risk Register (CRR) in place that is supported by four 'Directorate' risk registers which are owned by each of the four Directors on the Executive Team. Based upon the organisational structure and a drive to ensure that the risk management approach is pragmatic and proportionate, this hierarchy of risk is considered appropriate.</p> <p>The current CRR contains 18 risks, of which 8 that are inherently amber and then, in turn residually green. Therefore challenge is required to assess whether or not these should remain on the CRR or be de-escalated to the appropriate directorate risk register or indeed closed if they are no-longer risks. A key focus for the CRR is that the risks contained within it are of top priority for the Executive Team and the Board, and are explicitly linked to the CPCA strategic objectives.</p> <p><b>Suggested Action:</b> Refresh the existing CRR to align the risks to the CPCA objectives and major Board concerns, and rationalise the volume of risk information. A similar exercise should be undertaken for the Directorate risk registers to ensure that they are focused and relevant.</p>	Slides 11 and 12
9.	<i>Risk reporting is dynamic, visual and provides the appropriate information</i>	<p>Although risk reporting currently takes place to various forums within the governance structure, the reporting is not considered dynamic and lacking visual presentation, as it consists of reporting the risk register document in its existing guise. To ensure that risk reporting is meaningful to the end user and easy to understand, it is important to analyse and interpret the information within the risk registers and use this to inform risk reports that are tailored and appropriate for the audience.</p> <p>The recently formed Performance &amp; Risk Committee has an agenda that lends itself to receiving the corporate risk and emerging directorate risk reporting. The Committee should be considered the 'engine room' to ensure that risk management is working effectively. This Committee could also facilitate a 'deep dive' programme, through which it can ensure that the control environment is in place for specific risks and that actions are being implemented in a timely manner and essentially being managed effectively.</p> <p><b>Suggested Action:</b> Introduce new reporting formats that are focused on visual risk reporting, exception based indicators, escalation of directorate risks, trends and risk appetite. i.e. heat map. This should also incorporate a 'Deep Dive' programme of work looking at specific risks.</p>	Slides 14 and 21



# Road Map



Indicated potential deadline for activity to be completed.

	Suggested Actions	Q1	Q2	Q3	Q4
1	Revise the risk register template, to ensure that the information for each risk flows in a logical manner and provides scope to capture any enhancements made regarding developments highlighted in this pathfinder, for example risk appetite and assurance mapping.				
2	Amend the impact and likelihood matrix to a 'non-multiplier' and develop descriptors for the impact scale to help the assessment of risks and remove subjectivity.				
3	Develop a risk appetite statement and methodology that links to the Impact and Probability assessment. This will aid decision making, prioritisation of resources and targeted reporting				
4	Review all actions or planned improvements to ensure that timescales are applied to encourage ownership and accountability. Ensure that these actions demonstrably mitigate the risk and are proportionate to the residual risk score and risk appetite applied.				
5	Develop a proportionate assurance gathering mechanism for capturing and demonstrating the effectiveness of controls identified for the Corporate Risk Register risks. This should include not just the assurance source but also the effectiveness rating.				
6	Consideration to be given as to the most appropriate channel to acquire specialist risk management expertise and input for CPCA to facilitate the risk framework				
7	A risk management training programme should be developed and delivered that is tailored to suit the targeted group of individuals. i.e. Board, Operational staff, Audit Committee.				
8	Refresh the existing CRR to align the risks to the CPCA objectives and major Board concerns, and rationalise the volume of risk information. When this refresh exercise has taken place, a similar exercise should be undertaken for the Directorate risk registers to ensure that they are focused and relevant.				
9	Introduce new reporting formats that are focused on visual risk reporting, exception based indicators, escalation of directorate risks, trends and risk appetite. i.e. heat map. This should also incorporate a 'Deep Dive' programme of work looking at specific risks.				

# Risk Management Pathfinder

Slide Index: We have included some further guidance on the following slides (and referenced above) around risk management and the benefits it brings to an organisation, explaining various ways of improving and embedding risk management across CPCA

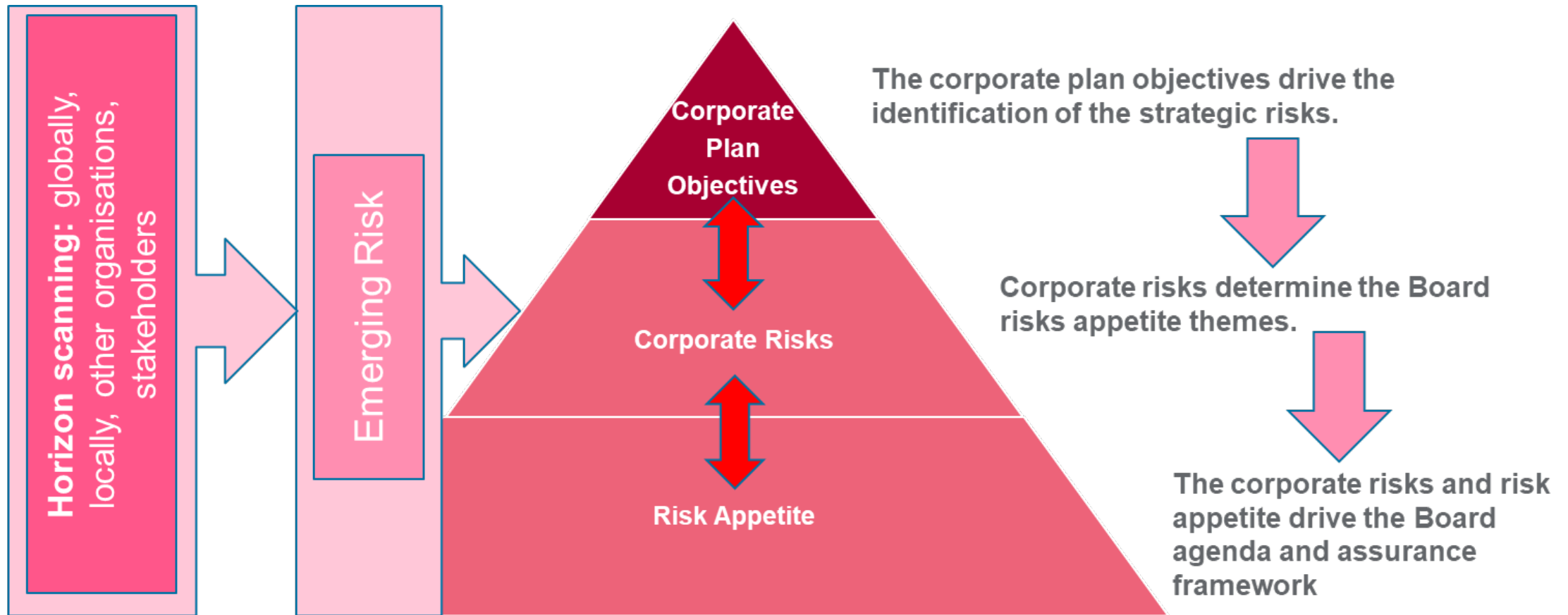
Slide Ref:	Explanation:
11	4 questions that can be asked what else might be drawn out in regards to identification of your strategic risks?
12	Demonstrating the relationship between strategic objectives, risk appetite and strategic risks.
13	Example of a standard risk register report (without assurances) that could be used for more operational areas to report their risks
14	Example of a Board Assurance Framework (BAF) report that includes the 3 lines of assurance that could be used for more detailed reporting to ET, Committees and Board
15	Example of an Assurance Report containing all references and assessments over the effectiveness of controls from 1 <sup>st</sup> , 2 <sup>nd</sup> and 3 <sup>rd</sup> lines of assurance
16	Example of an Actions Overdue report highlighting all actions associated to improving the management of a risk that are overdue and require updating
17	The 3 Lines of Assurance – explaining the process where you would seek to obtain evidence / assurance from Management, Oversight and Independent that the controls are working effectively.
18, 19, 20	Example of a 5x5 risk matrix including Impact and Likelihood descriptors that are used to ensure all risks are scored consistently using a set criteria
21	Example of a Heat Map that can be used to effectively position a key set of risks on a matrix to clearly show where each risk is positioned
22, 23 & 24	Risk Appetite – an introduction into how risk appetite can be developed using different levels, descriptions to report which risks sit within and outside of appetite.
25	Senior Independent Director – role outline

# Risk Management Pathfinder

If the 4 questions were asked what else might be drawn out? – worst case, challenge, opportunity, emerging. The 4 questions below can be used to extract from the board / executive what are the risk appetite themes / strategic or corporate risks. If these were asked what would the responses be and how would these compare with current corporate risk register entries.

Question:	
1	Given the CPCA vision, mission and priorities, what would be the worst thing that CPCA could experience tomorrow or in the next 12 months? i.e. activities or events that you would want to potentially avoid e.g. a significant health and safety breach etc.
2	Given the CPCA vision, mission and priorities, what are the greatest challenges that CPCA faces in the next 12 to 24 months? i.e. activities or events that may occur with which you would want to engage or tackle in some way e.g. achieving digital transformation of services for users etc.
3	Given the CPCA vision, mission and priorities, what are the greatest opportunities that CPCA has in the next 12 to 36 months? i.e. activities or events that you would want to capitalize on or seek out e.g. Commercial growth through partnering and collaboration etc.
4	Given the CPCA vision, mission and priorities, what do you see as the emerging events or threats that could impact on CPCA either negatively or positively and that you believe should be watched i.e. those items still morphing or on the horizon e.g. climate change / environmental, Cov-Sars 21 etc.

# Risk Management Pathfinder



**Emerging risks** will need to be monitored and kept in check.

**Corporate risks** enable the key controls to be identified and assurances mapped, creating a Board Assurance Framework.

**Risk appetite themes** will drive operational risk reporting – type of risk, volume, what is “in” and “outside” risk appetite.

# Risk Management Pathfinder

## Example: Standard Risk Report (No Assurances) using Risk R3

Strategic Risk Management Plan								
Risk Ref	Risk Title	Cause & Effect	Inherent Risk Score	Risk Control	Residual Risk Score	Action Required	Progress Notes	Target Risk Score
SRMP 1	College is unable to progress systems development and integration. <b>Risk Owner:</b> Craig Duff <b>Risk Lead:</b> <b>Last Updated:</b> 03 Nov 2021 <b>Latest Review Date:</b> 03 Nov 2021 <b>Latest Review By:</b> Craig Duff <b>Last Review Comments:</b> Risk discussed at Audit Committee and score reduced from 16 to 12 due to new controls added	<b>Cause</b> <ul style="list-style-type: none"> <li>- Poor training and awareness</li> <li>- Lack of a Digital Strategy</li> <li>- IT Department - lack of skills and experience</li> <li>- Insufficient funding and investment</li> </ul> <b>Effect</b> <ul style="list-style-type: none"> <li>- Inefficient work practices</li> <li>- Opportunities for efficiency missed;</li> <li>- Resources wasted/unable to reallocate to growth areas</li> <li>- Increased costs</li> <li>- Seen as "old fashioned" by stakeholders.</li> </ul>	I = 4 L = 4 16	2018/19 Digital Leadership Programme raising awareness of the importance of digital culture across the college <b>Control Owner:</b> Matt Humphrey	I = 4 L = 3 12	Update the 2018/19 Digital Leadership Programme for 2022/23 to ensure the College continues to raise awareness of the importance of its digital culture <b>Person Responsible:</b> Craig Duff <b>To be implemented by:</b> 31 Jan 2022	<b>03 Nov 2021</b> <b>Craig Duff</b> 1st Draft will be discussed at SLT during December 2021	I = 4 L = 2 8
				2019/20 - Launch of the Digital Strategy <b>Control Owner:</b> Craig Duff				
				Systems & Reporting improvement identified as a key component of revised Strategic Plan. Working Group established & continued additional investment for specialist resource with clear continuing priorities for data / reporting <b>Control Owner:</b> Duncan Short				
				Tribal Edge Learner journey and engagement app and software implemented from September 2019 onwards (SDConnect, online enrolments, ILP) <b>Control Owner:</b> Will Hollis				

# Risk Management Pathfinder

## Example: Board Assurance Framework Report

9b. Board Assurance Framework Acad / Staff											
Risk Ref	Risk Title	Cause & Effect	Inherent Risk Score	Risk Control	Control Assurance (Department)	Control Assurance (Management)	Control Assurance (Independent)	Overall Assurance Strength of Control	Residual Risk Score	Action Required	Progress Notes
STAFF 1	Insufficient staff development and retention  <b>Risk Owner:</b> Mrs H Jones <b>Risk Lead:</b> Mr C Smith <b>Last Updated:</b> 04 Nov 2021 <b>Latest Review Date:</b> 02 Mar 2021 <b>Latest Review By:</b> Mr C Smith <b>Last Review Comments:</b> Risk reviewed at Team Meeting and no updates made	<b>Cause</b> - Appraisal and performance management arrangements are not consistent - Unable to provide appropriate training and development opportunities - Insufficient resources to deliver training - Can't get staff out of day job to deliver training  <b>Effect</b> - Low standards of teaching and education. - High staff turnover / Shortage of staff. - Reputational damage - Difficulties in recruiting	I = 5 L = 5 25	Action Plans in place for all staff to further develop career  <b>Control Owner:</b> Ms T Carter	All staff 1-1's carried out and reported into HR	HR report into Committee each meeting on progress	External Consultant used to support and review process	Adequate  Assurance Date: 12 Jan 2021  Assurance By: Mr N Brown	I = 5 L = 2 10	Bring in an external HR specialist to undertake an independent survey across all staff on their views around the support and training.  <b>Person Responsible:</b> Mr C Smith  <b>To be implemented by:</b> 31 Jul 2021	25 May 2021 <b>Ms T Carter</b> Shortlist down to 3 - decision to be made end June 21 02 Mar 2021 <b>Mr C Smith</b> Contact has been made with a number of organisations and will discuss at next working group meeting March 2021
				All staff provided with personal training and development plan  <b>Control Owner:</b> Mrs H Jones	Training and development plans reviewed termly with management and HR	Update report taken to Management Team termly	External staff survey results provided by ABC Ltd	Adequate  Assurance Date: 12 Jan 2021  Assurance By: Mr N Brown		Ensure all staff appraisals are carried out annually in line with policy  <b>Person Responsible:</b> Mr N Brown  <b>To be implemented by:</b> 02 Aug 2021	25 May 2021 <b>Ms T Carter</b> Action on target and will be completed on time 12 Jan 2021 <b>Mr N Brown</b> 1st review carried out to determine who has not had an appraisal – action on track
				Annual Appraisal Processes in place for each member of staff that will include staff development plan that will be monitored throughout each year  <b>Control Owner:</b> Mrs H Jones	All appraisals held centrally in HR and reviewed annually	Update report taken to Management Team termly	Internal Audit review of appraisals annually	Limited  Assurance Date: 12 Jan 2021  Assurance By: Mr N Brown			
				Experienced in-house training and development team in place to support all staff on their specific needs.  <b>Control Owner:</b> Mr C Smith	HR team includes mix of experienced and specialist staff to deliver the programme	Management team review the process ensuring we have the right skills mix in place	Internal Audit review carried out across the HR team including the effectiveness of the HR team to deliver the training	Substantial  Assurance Date: 12 Jan 2021  Assurance By: Mr N Brown			



# Risk Management Pathfinder

## Example: 3 Lines of Assurance Report using Risk R3

Strategic Risk Management Plan															
Risk Ref	Risk Title	Risk Appetite	Inherent Risk Score	Residual Risk Score	Risk Control	Control Assurance (Department)	Department Assurance Owner	Department Strength of Control	Control Assurance (Management)	Management Assurance Owner	Management Strength of Control	Control Assurance (Independent)	Independent Assurance Owner	Independent Strength of Control	Overall Assurance Strength of Control
SRM P 1	College is unable to progress systems development and integration.  <b>Risk Owner:</b> Craig Duff <b>Risk Lead:</b>  <b>Last Updated:</b> 03 Nov 2021 <b>Latest Review Date:</b> 03 Nov 2021 <b>Latest Review By:</b> Craig Duff  <b>Last Review Comments:</b> Risk discussed at Audit Committee and score reduced from 16 to 12 due to new controls added	IT Investment - Open 12+	I = 4 L = 4 16	I = 4 L = 3 12	2018/19 Digital Leadership Programme raising awareness of the importance of digital culture across the college  <b>Control Owner:</b> Matt Humphrey	All training and awareness sessions evidence held by IT team and reviewed annually	Craig Duff	Substantial  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	CLT review progress against IT Strategy at least once a year at annual planning seminar.	Matt Humphrey	Adequate  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	RSM Internal Audit review June 2021	Duncan Short	Limited  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	Limited  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff
					2019/20 - Launch of the Digital Strategy  <b>Control Owner:</b> Craig Duff	Head of IT reviews Digital Strategy annually with team	Craig Duff	Substantial  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	Digital Strategy taken to Senior Leadership Team annually for update and approval Report presented at September 2020 Audit Committee	Will Hollis	Substantial  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	RSM internal audit of Digital Strategy complete	Matt Humphrey	Substantial  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	Substantial  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff
					Systems & Reporting improvement identified as a key component of revised Strategic Plan. Working Group established & continued additional investment for specialist resource with clear continuing priorities for data / reporting  <b>Control Owner:</b> Duncan Short	College dashboards launched in autumn term 2019 – well received with good user feedback	Duncan Short	Substantial  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	College dashboards reports discussed at IT working group and SLT monthly	Craig Duff	Adequate  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	Ofsted Inspection 2020 reviewed Strategic Plan	Matt Humphrey	Adequate  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	Adequate  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff
					Tribal Edge Learner journey and engagement app and software implemented from September 2019 onwards (SDConnect, online enrolments, ILP)  <b>Control Owner:</b> Will Hollis	IT Team ensure Cross-college engagement with Tribal EBS and Microsoft Office 365 products remains on-going	Craig Duff	Adequate  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	Quarterly updates to SLT on progress made	Matt Humphrey	Substantial  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	External consultants used ad-hoc throughout the year to advise on progress made and any further recommendations	Duncan Short	Adequate  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff	Adequate  Assurance Date: 03 Nov 2021  Assurance By: Craig Duff

# Risk Management Pathfinder

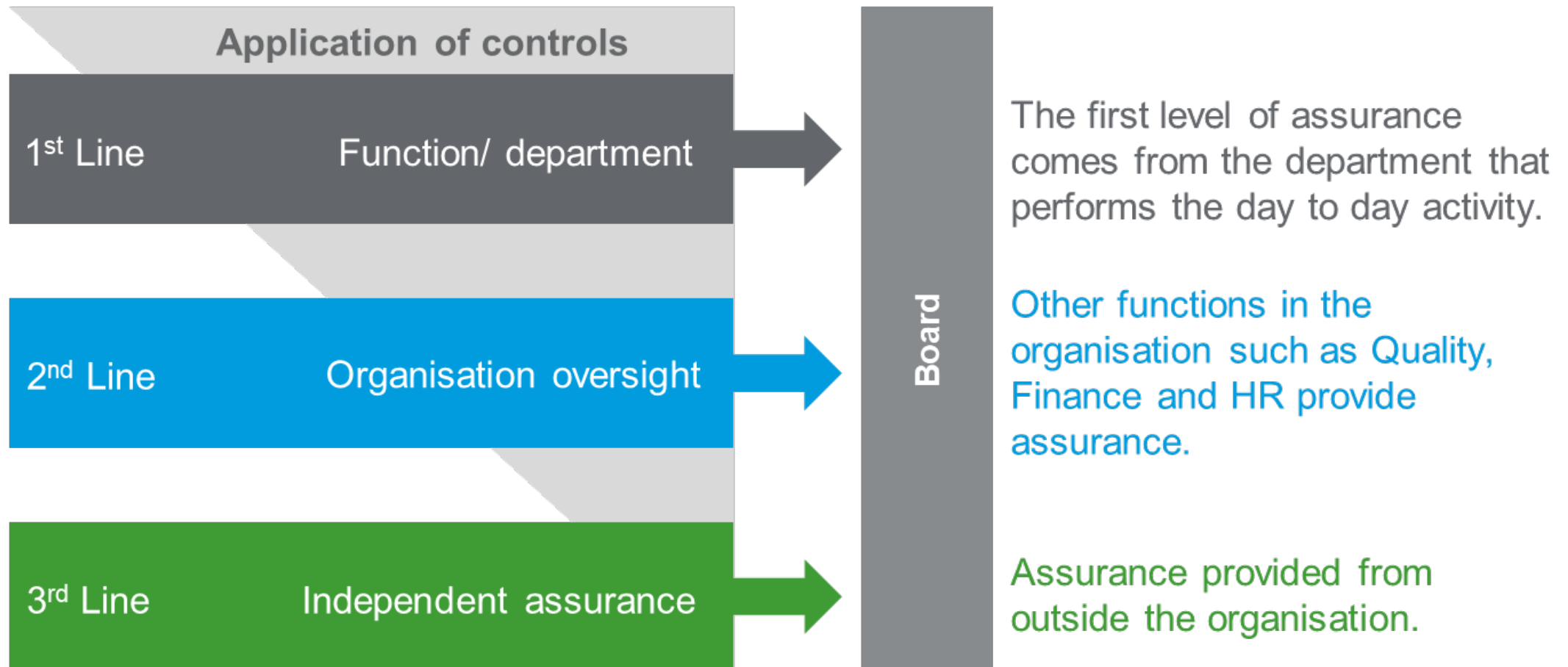
## Example: Actions Overdue Report:

Risk Ref	Risk Title	Inherent Risk Score	Residual Risk Score	Action Required	Person Responsible	To be implemented by	Progress Notes	Target Risk Score
STR 1	Governance: Fail to ensure governance arrangements are accountable, appropriate & effective. <b>Risk Owner:</b> Craig Duff <b>Risk Lead:</b> Duncan Short <b>Last Updated:</b> 20 Oct 2021	I = 4 L = 4 16	I = 4 L = 2 8	1. Review and redraft the Terms of Reference for the Board and each of its Sub-Committee(s).	Duncan Short	31 Jul 2021	<b>20 Oct 2021</b> <b>Insight4GRC Support</b> This is what is happening <b>21 Sep 2021</b> <b>Craig Duff</b> Action delayed at key member of staff has been on long-term sick.	I = 3 L = 1 3
STR 2	Failure to achieve growth, increase turnover and the diversity of the organisations services in order to keep working towards the mission statement. <b>Risk Owner:</b> Craig Duff <b>Risk Lead:</b> Duncan Short <b>Last Updated:</b> 22 Sep 2021	I = 5 L = 5 25	I = 5 L = 3 15	4. Following on from external review, Finance Team to ensure reports include month on month comparisons	Matt Humphrey	30 Sep 2021	<b>27 Jul 2020</b> <b>Craig Duff</b> Action date agreed by group to extend to end Sept 20	I = 4 L = 2 8
STR 2	Failure to achieve growth, increase turnover and the diversity of the organisations services in order to keep working towards the mission statement. <b>Risk Owner:</b> Craig Duff <b>Risk Lead:</b> Duncan Short <b>Last Updated:</b> 22 Sep 2021	I = 5 L = 5 25	I = 5 L = 3 15	1. To appoint a Development Partner to help support our growth plans	Craig Duff	15 Oct 2021	<b>28 Aug 2020</b> <b>Craig Duff</b> Action on target. Interviews to be held early September <b>02 Dec 2019</b> <b>Craig Duff</b> Date extended into end Jan 20 due to difficulties in trying to recruit	I = 4 L = 2 8



# Risk Management Pathfinder

Making use of the assurances available



# Risk Management Pathfinder

### Example: Risk Matrix (Non-Multiplier)

Impact	5 Major	15	19	22	24	25
	4 Significant	10	14	18	21	23
	3 Moderate	6	9	13	17	20
	2 Minor	3	5	8	12	16
	1 Negligible	1	2	4	7	11
		1	2	3	4	5
		Rare	Unlikely	Possible	Likely	Almost Certain
Likelihood						

# Risk Management Pathfinder

## Example: Risk Impact Criteria / Definitions

Impact:	Safety	Reputation	Media Attitude	Legal Action	Direct Loss
<b>5 - Critical</b>	Potential to cause one or a number of fatalities. H&S breach causing serious fine, investigation, legal fees and possible stop notice.	Stakeholders / Third parties suffer major loss or cost.	Governmental or comparable political repercussions. Loss of confidence by public.	Action brought against The Group for significant breach.	Over £300,000
<b>4 – Major</b>	Serious risk or injury possibly leading to loss of life. H&S investigation resulting in investigation and loss of revenue.	Significant disruption and or Cost to Stakeholders / third parties.	Story in multiple media outlets and/or national TV main news over more than one day.	Law suit against for major breach with limited opportunity for settlement out of court	Between £50,000 and £300,000
<b>3 – Moderate</b>	High risk of injury, possibly serious. H&S standards insufficient / poor training.	A number of Stakeholders are aware and impacted by problems.	Critical article in Press or TV. Public criticism from industry body.	Probable settlement out of court	Between £10,000 and £50,000
<b>2 - Minor</b>	Small risk of minor injury. H&S policy not regularly reviewed.	Some external Stakeholders aware of the problem, but impact on is minimal.	Negative general article of which The Group is mentioned	Legal action with limited potential for decision against	Between £1,000 and £10,000
<b>1 – Insignificant</b>	No risk of injury. H&S compliant	External Stakeholders not impacted or aware of problem	No adverse media or trade press reporting.	Unsupported threat of legal action	Between £0 and £1,000

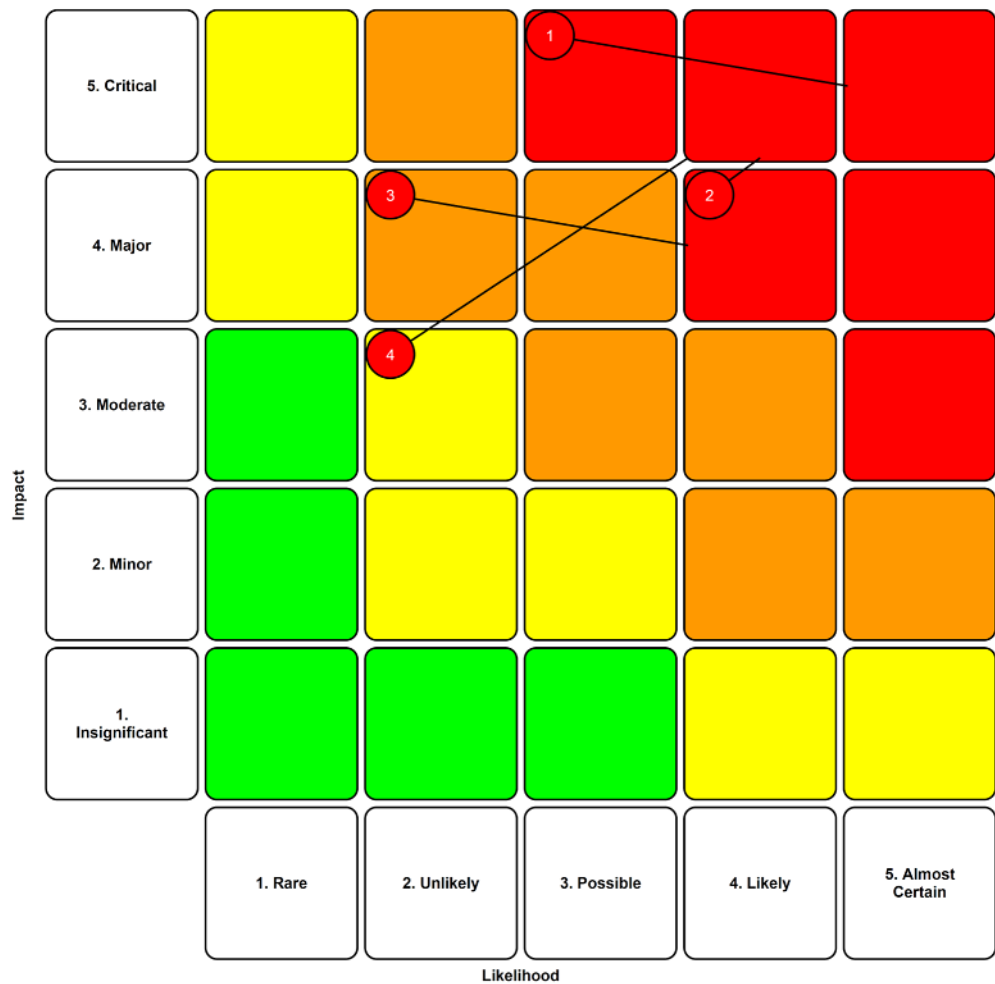
# Risk Management Pathfinder

## Example: Risk Likelihood Criteria / Definitions

Likelihood:	Description:
5. Almost Certain	<ul style="list-style-type: none"><li>• A history of it happening across the organisation</li><li>• The event is expected to occur</li><li>• 80% - 100% probability</li><li>• Could occur within 1 month.</li></ul>
4. Likely	<ul style="list-style-type: none"><li>• Has happened across the organisation in the recent past</li><li>• The event will probably occur in most circumstances</li><li>• 60% -80% probability</li><li>• Could occur within 6 months</li></ul>
3. Possible	<ul style="list-style-type: none"><li>• Has happened across the organisation in the past</li><li>• The event should occur at some time</li><li>• 40% - 60% probability</li><li>• Could occur within 1 year</li></ul>
2. Unlikely	<ul style="list-style-type: none"><li>• May have happened across the organisation in the past</li><li>• The event could occur at some time</li><li>• 20% - 40% probability</li><li>• Could occur within 1-3 years</li></ul>
1. Rare	<ul style="list-style-type: none"><li>• . No history of it happening across the organisation</li><li>• The event may occur only in exceptional circumstances</li><li>• &lt; 20% probability</li><li>• Could occur within 3 – 5 years</li></ul>

# Risk Management Pathfinder

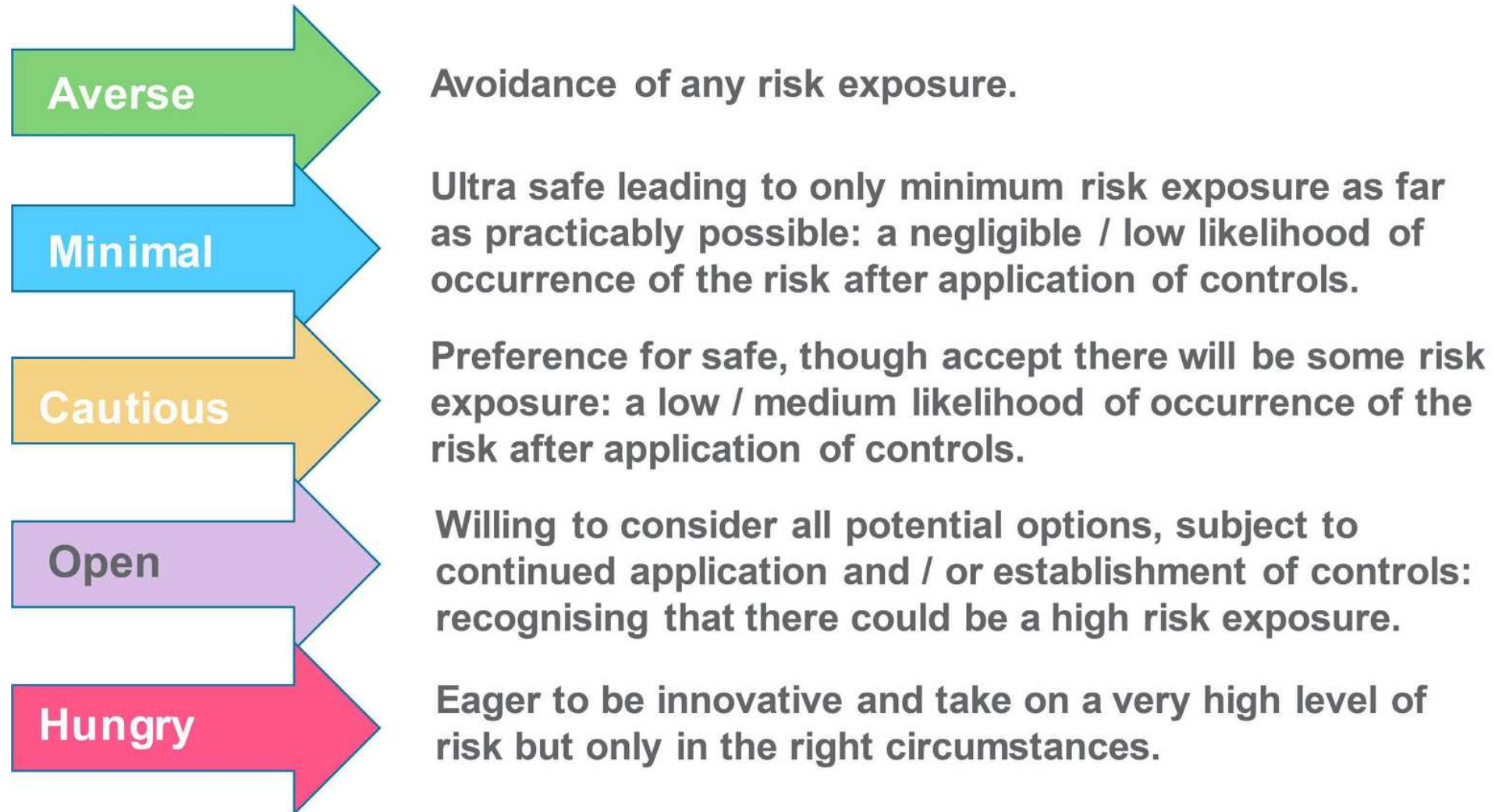
## Example: Heat Map and Risk Details



Grid #	Risk Ref	Risk Title	Inherent Risk Score	Residual Risk Score	Target Risk Score
1	STR 2	Failure to achieve growth, increase turnover and the diversity of the organisations services in order to keep working towards the mission statement.	I = 5 L = 5 25	I = 5 L = 3 15	I = 4 L = 2 8
2	HR 2	Fail to recruit and retain staff	I = 5 L = 4 20	I = 4 L = 4 16	I = 1 L = 1 1
3	STR 1	Governance: Fail to ensure governance arrangements are accountable, appropriate & effective.	I = 4 L = 4 16	I = 4 L = 2 8	I = 3 L = 1 3
4	HR 1	Failure to recruit and retain good quality skilled staff.	I = 5 L = 4 20	I = 3 L = 2 6	I = 2 L = 1 2

# Risk Management Pathfinder

## Example: Risk Appetite Levels and Descriptions



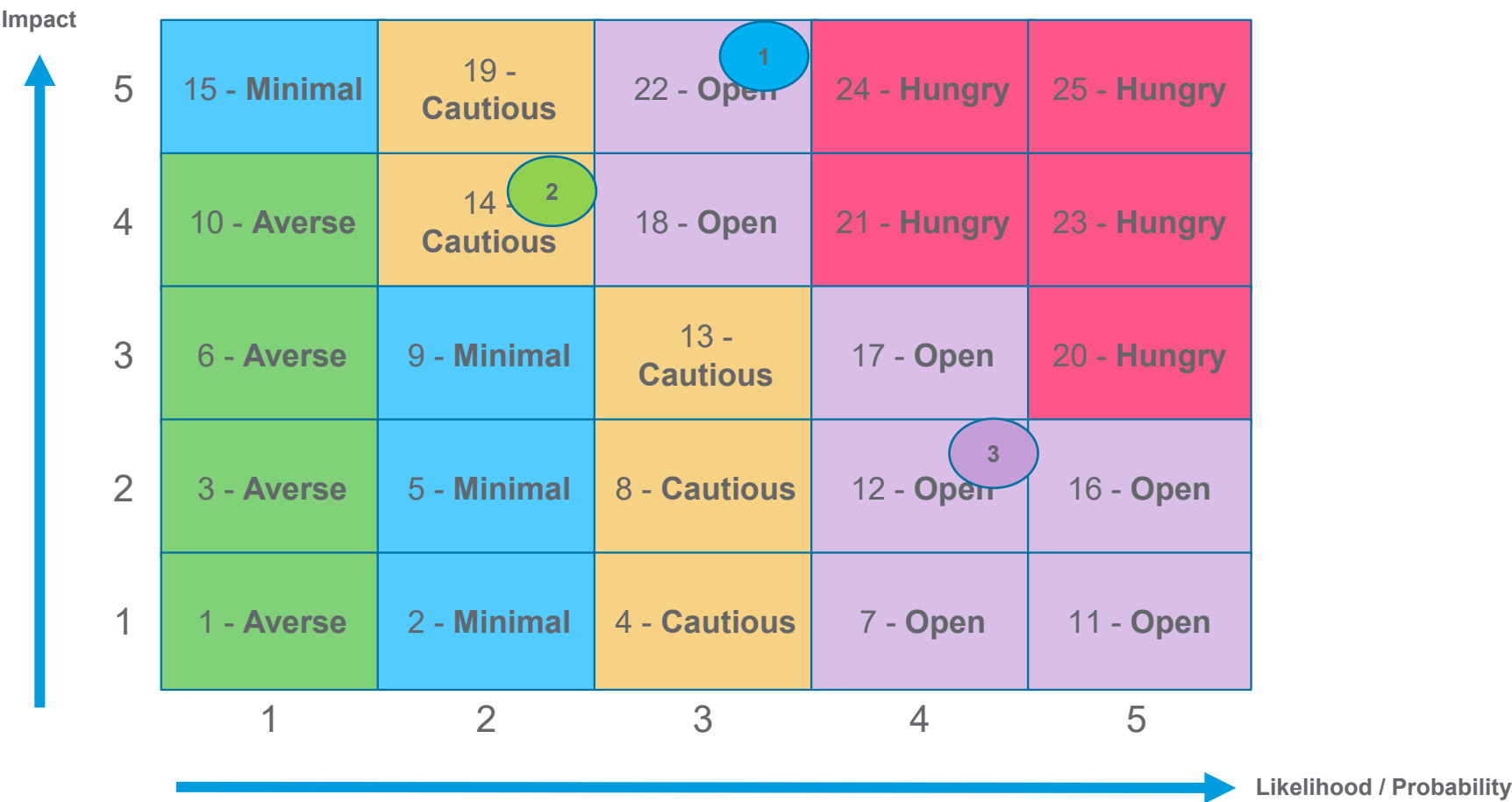
# Risk Management Pathfinder

Example: Risk Appetite Themes with applicable Risk Appetite level

Risk Appetite Theme	Averse	Minimal	Cautious	Open	Hungry
Maintaining financial resilience					
Protecting our students and staff					
Ensuring quality, resilience and continuity of services					
Successful service transformation					
Managing our reputation					
Managing Development and growth					
Managing environmental / climate impact					
Embracing the regulatory framework					
Providing quality curriculum and services					

# Risk Management Pathfinder

Example: Risks plotted by Appetite Theme V Risk Appetite Boundaries



**Risk 1**  
Appetite Theme – Minimal  
Outside of Appetite

**Risk 2**  
Appetite Theme – Averse  
Outside of Appetite

**Risk 3**  
Appetite Theme – Open  
Within Appetite



## Senior Independent Director (or similar)

Considering how to resource and facilitate a risk management framework can be challenging for many organisations as finding the 'right' candidate with the appropriate skills, experience / sector knowledge and within budget is difficult.

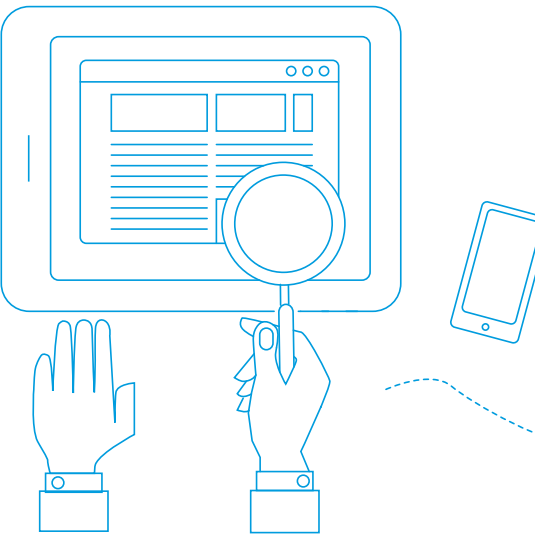
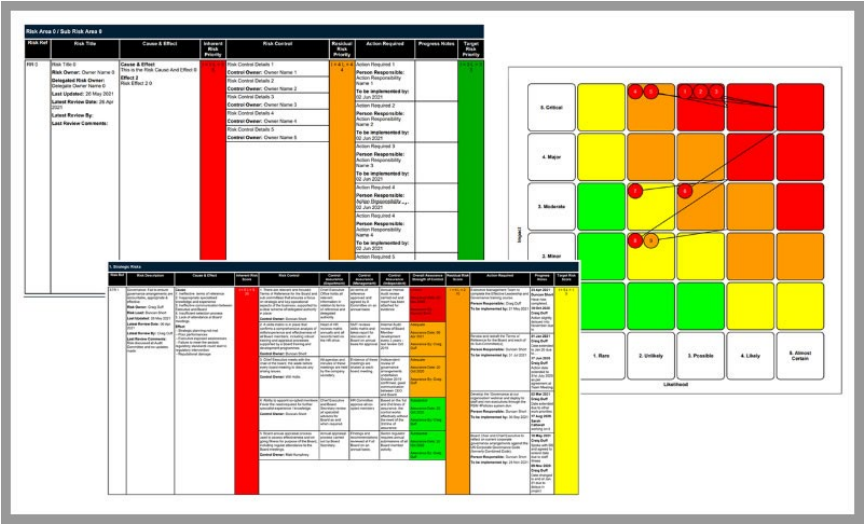
One solution to this is to develop a position similar to a Senior Independent Director within the public limited company arena. This role can often be cost effective for organisations and can be sourced with the appropriate skills and knowledge required to facilitate and challenge the risk management framework.

This role is a particularly effective element within a risk management framework as it is an independent role, i.e. free of any connections that may lead to a conflict of interest within the organisation, meaning that the ability to be objective and challenge remains strong.

It is suggested that this role could consist of the following for CPCA:

- Work closely with the Chief Executive and Mayor to provide risk advice and guidance on certain matters
- Providing risk insight and advice to the Executive Leadership Team as required
- Facilitate a quarterly check and challenge of the corporate risk register with Executive Leadership Team
- Attend the Performance & Risk Committee to provide advice and guidance and 'check and challenge'.
- Ensure that Directorate risk information is updated and to a suitable quality in terms of content
- Aid the interpretation of risk reports and advise on how these might be developed
- Guide and steer the risk management framework in conjunction with the Executive Leadership Team to ensure that it remains effective
- Develop, oversee and lead the risk deep dive programme.

# Visibility & Oversight



## Insight4GRC



A complete picture of your risk management in real-time

[www.insight4grc.com](http://www.insight4grc.com)

### STR 1 - Governance:

Fail to ensure governance arrangements are accountable, appropriate & effective.

Cause and Effect	Existing Controls	Action Required	Notes/Risk Events	Strength of Controls	History
Control Status: Existing					
Risk Control	Assurance Given	Assurance Date	Strength of Control	Assurance Line	
1. There are relevant and focused Terms of Reference for the Board and sub committees that ensures a focus on strategic and key operational aspects of the business, supported by a clear scheme of delegated authority in place	Yes	19/01/2021	Limited	Management	<a href="#">View Details</a>
2. A skills matrix is in place that confirms a comprehensive analysis of skills/experience and effectiveness of all Board members, including robust training and appraisal processes supported by a Board training and development programmes	Yes	06/04/2021	Adequate	Overall Assurance	<a href="#">View Details</a>
3. Chief Executive meets with the chair of the board, the week before every board meeting to discuss any arising issues.	Yes	20/10/2020	Adequate	Overall Assurance	<a href="#">View Details</a>
4. Ability to appoint co-opted members if ever the need required for further specialist experience / knowledge.	Yes	20/10/2020	Substantial	Overall Assurance	<a href="#">View Details</a>
5. Board annual appraisal process used to assess effectiveness and on going fitness for purpose of the Board, including regular attendance to the Board meetings.	Yes	20/10/2020	Substantial	Overall Assurance	<a href="#">View Details</a>

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction.

The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Northern Ireland (UK) Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are licensed by the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. RSM Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Before accepting an engagement, contact with the existing accountant will be made to request information on any matters of which, in the existing accountant's opinion, the firm needs to be aware before deciding whether to accept the engagement.

© 2021 RSM UK Group LLP, all rights reserved

