www.pwc.com.au

Internal Audit and Enterprise Risk Management

October 2015

pwc

Agenda

A. Risk Management – A Quick Overview:

- What does a comprehensive RM approach involve and what can you expect from an effective framework?

B. Alignment of IA and RM

- The importance of aligning IA with other assurance activities and how Risk Assurance Mapping can help

C. A Simplified RM Model

- A practical example of how the RM strategy can be used to increase the value of the RM process to management, ensure alignment with IA and increase the value of the RM function

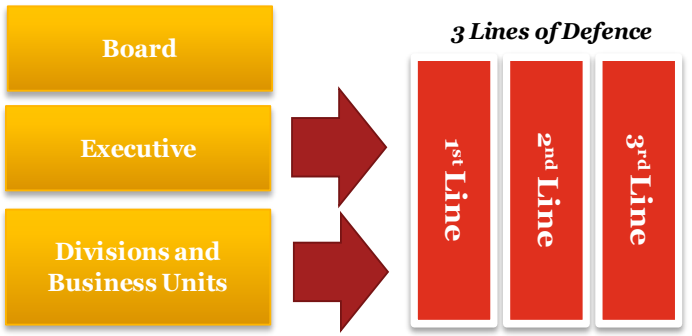
A. Risk Management – A Quick Overview

Four Aspects of Risk Management

Risk Management Framework

- Strategy, financial planning and risk appetite are integrally connected
- The Board set Risk Appetite, the Executive manage the organisation within Appetite
- Monitoring performance against Appetite is the essence of management
- Understanding and addressing variances is the difference between success and failure

The Operational Model



The Cultural Dimension

Tone from the top, Walking the talk

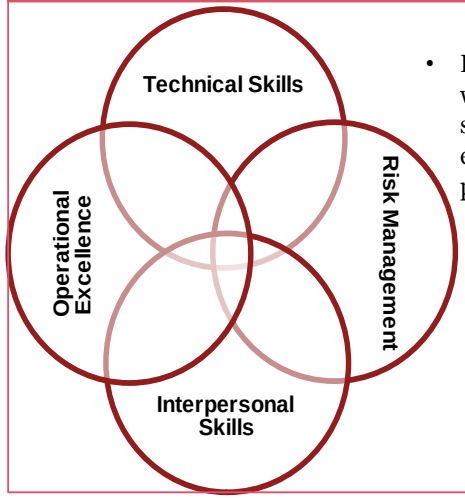
The ERM framework – rules and accountabilities

Strong Risk Management Culture

Education and awareness – the major enabler

Established norms and behaviours of individuals and the group

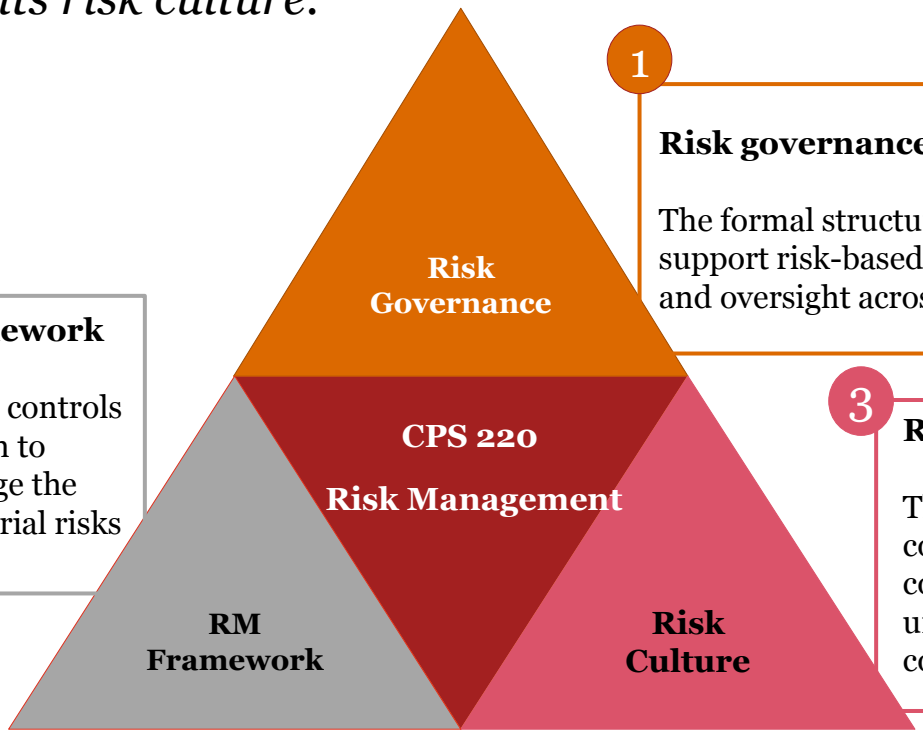
Capacity and Capability



- Right number of people with right balance of skills and experience employed in the right places

Financial Services – Regulatory Perspective on RM

Conglomerate Prudential Standard 220 articulates APRA's heightened expectations of the quality of an institution's risk governance, risk management framework and its risk culture.



1

Risk governance

The formal structures used to support risk-based decision-making and oversight across all operations

2

Risk management framework

The systems, resources and controls that enable the organisation to identify, analyse and manage the current and emerging material risks within the business

3

Risk culture

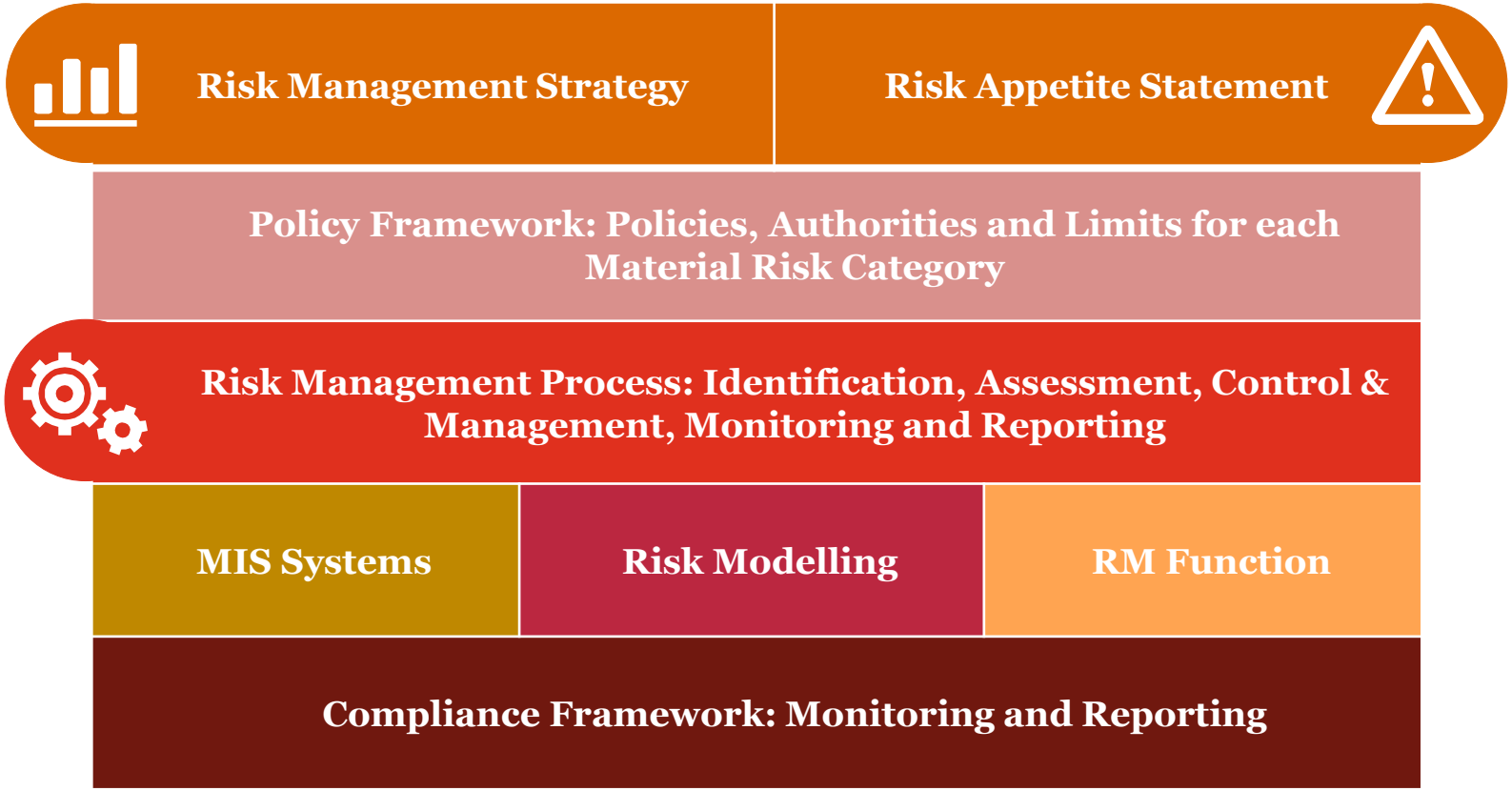
The combined set of individual and corporate values, attitudes, competencies and behaviours that underpin the organisations commitment to risk management

Material Risks

- Strategic Risks
- Market and Interest Rate Risks
- Credit Risks
- Liquidity Risks
- Operational Risks

Components of the RM Framework

A RM Framework can be divided into a number of components:*



**CPS220*

Risk Management Strategy

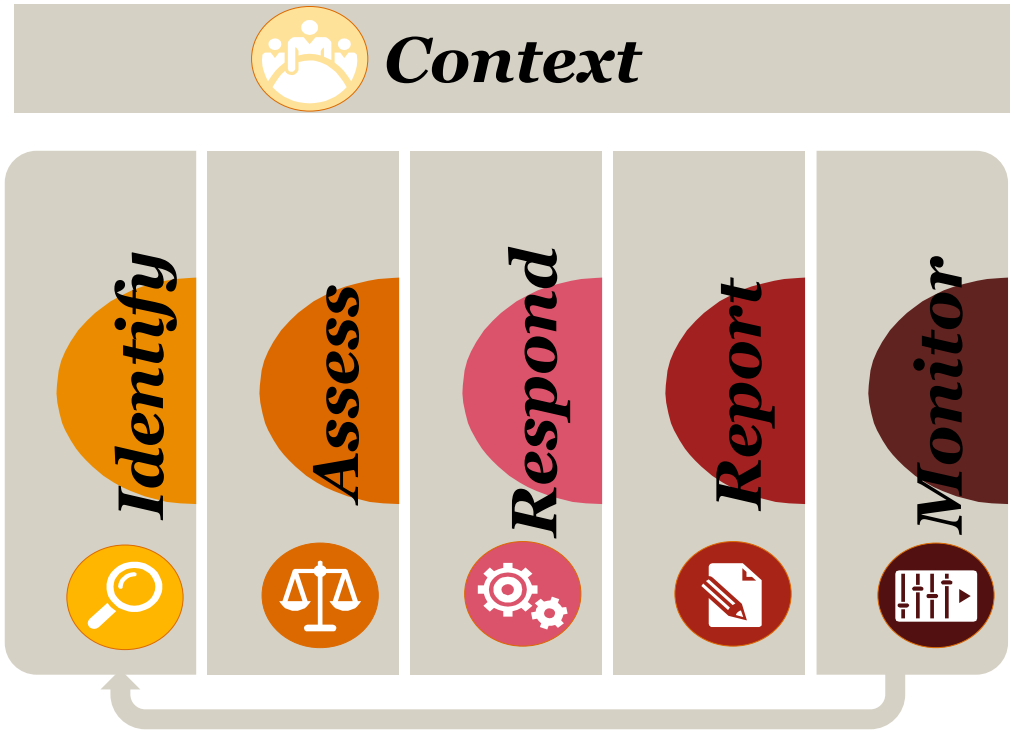
A Risk Management Strategy is defined as a document that contains the following minimum components:*

- A description of each material risk identified, and the institution's approach to managing these risks
- A list of the policies and procedures dealing with risk management matters
- The role and responsibilities of the risk management function
- A description of the risk governance relationship between the Board, board committees and senior management with respect to the risk management framework
- An outline of the approach to ensuring all persons have awareness of the risk management framework and for instilling an appropriate risk culture across the institution

**CPS220*

The Risk Management Process

The core Risk Management process can be summarised as below:



Context: Refers to the general environment, culture and business requirements within which the risk management process operates

Identify: The process and approach applied to the identification of risks and opportunities facing the organisation

Assess: The process and approach applied to the assessment of the potential level of threat to the organisation associated with risk events

Respond: The process and approach applied to determining whether the current risk level is appropriate or whether some form of action needs to be taken to reduce either likelihood or impact

Report: The format and content of the risk register that is the formal output of the risk management process

Monitor: The process and approach applied to the ongoing review of the risk profile including progress in implementing remedial actions where necessary

Focusing questions…….

What are we worried about? → What 'asset' is at risk → Are we doing enough? → Can we evidence our thinking? → Has anything changed since we last checked?

What to Expect From an Effective RM Program

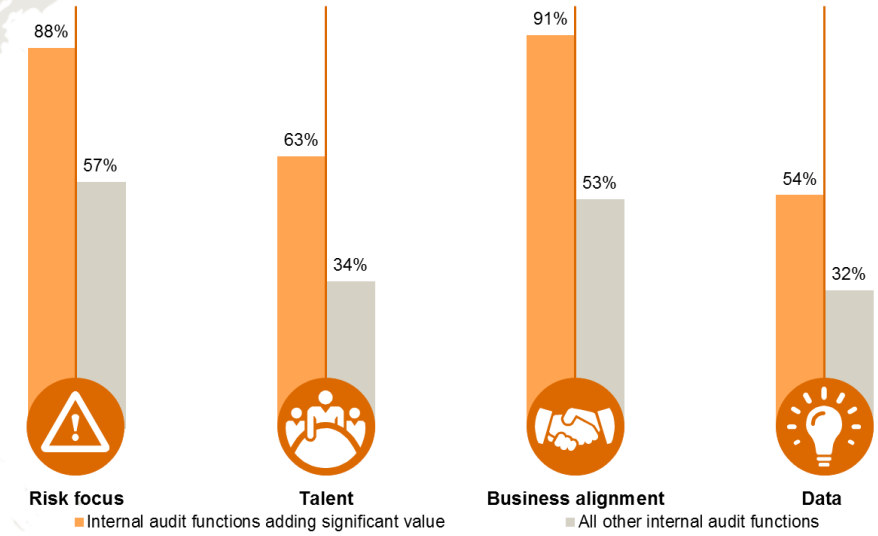
B. Alignment of IA and RM

The importance of aligning activities

Risk focus, alignment across the lines of defense, talent and data analytics are seen by CAE's and stakeholders alike as significant factors enabling internal audit to contribute to strategic initiatives*.

Significant factors enabling internal audit to contribute to strategic initiatives

- **A focus on the right risks at the optimal time in the process**
- **The talent and business acumen to be relevant and offer valuable insights**
- **Stronger alignment with ERM and other line of defense**
- **Proficient use of data analytics to provide powerful insights into the business**



State of the Profession Survey 2015

Risk and business alignment

Aligning assurance activities to business strategy and priorities has positive benefits for an organisation:

Organisations in which internal audit contributes significant value report their functions are better aligned with the company's risk management program: **87% are well aligned versus only 21% of lesser valued organisations***

Strong alignment results in:

- Better visibility to the information produced by other lines of defence
- Less risk management fatigue among participants
- Better risk management for the enterprise
- Greater efficiency

**State of the Profession Survey 2015*

Three lines of defence – a typical overview

The model provides a framework for segregating and aligning responsibilities for control and assurance activities:

First line of defence	Second line of defence	Third Line of Defence
Key attributes	**Key attributes**	**Key attributes**
• Implementation, ongoing maintenance and enhancement of the risk management framework, including: • Identification and effective management/mitigation of risks; and • Issues identification, recording, escalation and management. • Likely to include executive and management committees, forums and delegated authority.	• "Centre of excellence" in risk management to be leveraged to benefit the whole organisation • Scope includes all risk types; strategic, financial, operational, regulatory, compliance, etc. • Understand aggregated risk positions and support in developing and advising on risk strategies	• Independent assurance that the risk management framework has been complied with and is operating effectively. • A periodic comprehensive review of the appropriateness, effectiveness and adequacy of the risk management framework.
Execute Controls	**Monitor Controls**	**Assess Controls**

Control Activity | **Assurance Activity**

Reasonable Assurance

To have an effective assurance outcome you need to optimise both control and assurance activities and they must address **Risk**

Risk Assurance Mapping

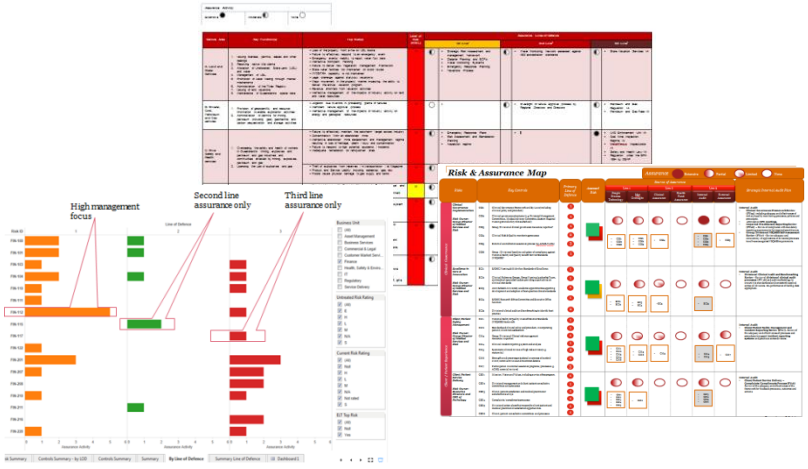
A RAM can be used to ensure assurance activities are aligned:

A RAM can be constructed for a variety of purposes including:

- **To identify the level of assurance activity and any gaps in coverage / over-assurance against strategic risks (risks to strategic plans)**
- **To provide a view on the cost of controls if assurance is mapped against key controls**

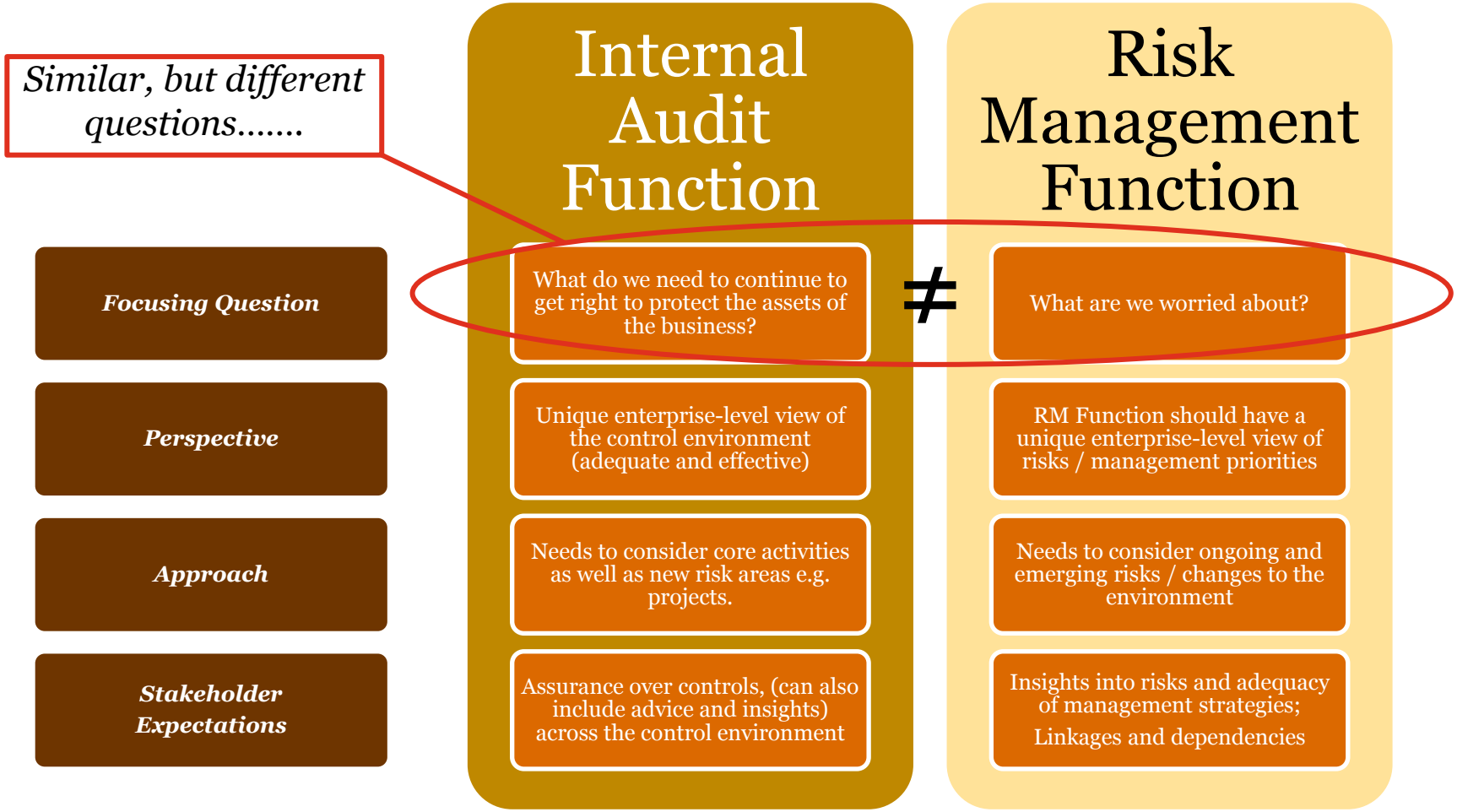
Challenges include:

- **Making sure that the mapping is conducted at the most appropriate level (risk category / risks / individual control)**
- **Strategic Risks don't always get captured in risk registers**
- **Judgment is often required on what constitutes and the adequacy of the assurance activity**



Comparison between IA and RM Functions

There are some clear parallels between the role of the IA and RM functions:



Risk Categories

The use of Risk Categories provides a link between the business strategy and risk management.

Risk Categories should reflect the nature of business activities

The RAS should provide guidance on what is acceptable / not-acceptable against each Risk (sub) Category

The Risk Categories should be used to aggregate specific risks for reporting purposes

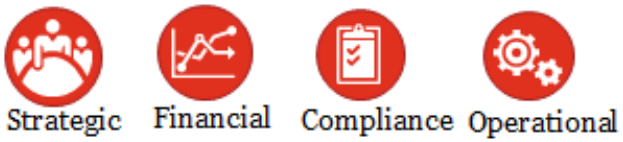
- Risk Categories are not the same as Risk Impacts, but the RAS should be used to calibrate the risk assessment criteria (impact definitions) as a key way of operationalising the RAS.
- Other ways include:

Delegated Authorities	Board Reserved Matters	Treasury Policy	Standard Operating Procedures	Codes of Conduct

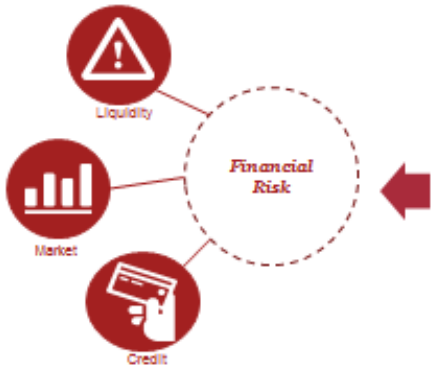
Aligning Risk Appetite and Risk Categories

The use of Risk Categories provides a link between the business strategy and risk management. Ideally, risk appetite statements should be developed for each risk category / sub-category:

Agree Risk Categories to be used for Assessment and Reporting Purposes



Identify any Sub-Categories against which an appetite statement needs to be developed



Agree definitions to be applied against each sub-category

Very Low	Low	Moderate	High
Avoid	Limit	Selectively seek	Actively seek

Develop detailed risk appetite statements and tolerance levels for each sub-category

Strategic Risk		
RA Statement	**Appetite**	**Risk Tolerance**
Reputation: xxxxx	Low	Residual operational risks assessed as critical are to be escalated to the Board.
Growth: xxxxxx	Moderate	xxxxxxx

Operationalise the RAS including aligning to the Risk Impact tables

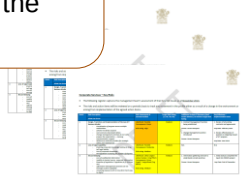
C. Risk Management – A Simplified Practical Implementation

A Sample Methodology

BAU RISKS

BU Risk Registers

The RM team will commission updates of the BU Risk Registers

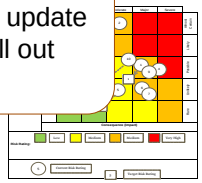


Consolidation

The RM team will then aggregate the registers against the Risk Categories

Analysis & Trends

The RM team will then update the EMT report and call out any trends or issues



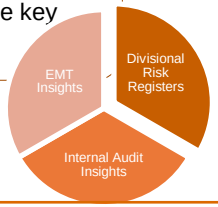
Focusing Questions:

- Are we comfortable with the Target Risk Rating against each of the Risk Categories?
- Are we comfortable that the BU's have adequate response plans in place to reduce the overall risk rating where necessary?
- Are there any anomalies in ratings between / across the different Divisions?
- Are we comfortable that our regular management and assurance processes adequately address these risks?

EMERGING RISKS

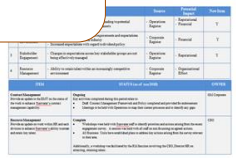
Initial Scan

The RM team will gather together views from three key sources



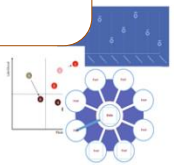
Emerging Priorities List

The RM team will produce a consolidated list for discussion



Items for Discussion / Review

Further information can be gathered and presented for discussion



Focusing Questions:

- Are we comfortable that the list of Emerging Priorities includes any and all issues of significance that may adversely impact on the organisation's risk profile?
- As a management team, do we have enough transparency over the status of the issues identified?
- Are we comfortable that we have appropriate monitoring and response plans in place or is there something else we need to be doing?

Sample Business Unit Register

Target rating is below Current rating – requires an Action Item

XXX – Key Risks (as at June 2015)

Risk #	Risk Description What Can Occur	Risk Assessment of Current Position	Target Risk Rating (L / M / H/ VH)	Additional Actions if Necessary (and Action Owners) to Achieve Target Risk Rating	Key Milestone / Implementation Date	Mapping to Enterprise Report
1	**Budget Expenditure Oversight – Monitoring of Service Delivery** Inability to accurately predict expenditure or to identify, prevent or respond to material unplanned expenditure variation. - *Reported financial position does not align with the 'true' position* - *Implications of programs and activities not fully costed or understood* - *Assumptions are wrong and/or not applied to budgets* - *Change in strategic priorities* - *Difficulties in differentiating, tracking and reporting on core and discretionary funding requirements*	High (Moderate to Major Fiscal and Reputational Impact – Possible Likelihood)	Medium	Being addressed through the business process improvement activities across the xxx areas including implementation of the XXX Review recommendations	January 2016	1 Budget and Estimates
2	**Budget Process** Material errors in budget or actuals reporting or incorrect advice to xxx or other stakeholders on expenditure proposals. - *Errors in consolidation process: system or manual* - *Quality of information captured does not support analysis and understanding of past, current and future position* - *Data is incomplete and / or not current (poor version control)* - *Deadlines missed*	Low (Minor Fiscal, Minor Reputational – Unlikely Likelihood)	Low	N/A		1 Budget and Estimates
3	**Governance / Ethics / Reputation** Ineffective processes and policies for core business strategy, managerial governance such as performance monitoring, decision-making, delegations, risk management, allocation of roles and responsibilities, ethics and misconduct. - *Expectations are not clearly defined and/or communicated to staff*	Low (Minor Regulatory / Legal, Reputation – Possible)	Low	N/A		6 Governance / Ethics / Integrity
4	**Knowledge Management / Systems** Lack of integrity or confidentiality of information. Loss of availability of key people, systems, intellectual property, etc. - *Poor security over sensitive / confidential data* - *Over-reliance on individuals for specific subject / agency knowledge* - *Historical context / knowledge is not retained or handed on* - *Failure to securely handle commercially sensitive and/or confidential data*	Medium (Moderate Regulatory / Legal – Possible Likelihood)	Medium	N/A		7 Knowledge / Systems Management
5	**People and Culture** Inability to achieve desired cultural and workplace reform, productivity targets, or to attract, retain, utilise and develop people and culture or failure to maintain a safe working environment for people. - *Roles and responsibilities are not clearly defined* - *Overly stable / overly dynamic workforce* - *Limited progression and development opportunities* - *Cultural environment impacts engagement and productivity* - *Skills and capability gaps across xxx arising from changing business model*	Medium (Moderate Reputation – Possible Likelihood)	Medium	N/A		8 People and Culture

Risks are aligned to the relevant Material Risk Category

Only <u>additional</u> action items are captured

Target rating is determined by the Board (or equivalent)

Sample Enterprise Aggregated Risk Report

Reporting using Risk Categories enables a view of risk across the organisation and provides a mechanism for aggregation:

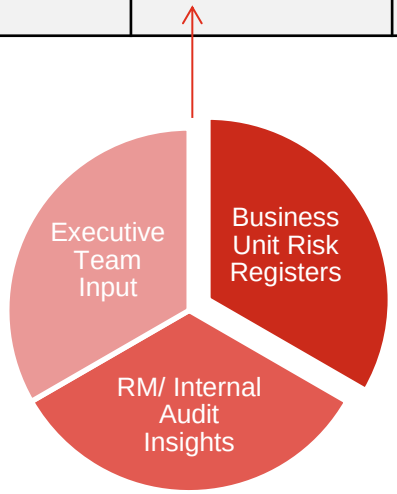
	Risk Category	Context/Causes/Concerns	Current residual rating by area						Current rating	Target rating
			Unit A	Unit B	Unit C	Unit D	Unit E	Unit F		
Service Delivery	**1. Budget and Forecasts**	• Failure to accurately predict expenditure and/or revenue or to identify, prevent or respond to material unplanned expenditure variation • Incorrect advice to Board or other stakeholders on expenditure proposals	H		H				H	M
	2. Revenue Collection	• Failure to collect revenue - ineffective enforcement regime • System, and business process failures					M		M	M
	3. xxx	• Failure to xxxxxx			H				H	M
	4. xxx	• Ineffective execution of service delivery xxxxxx			M	M			M	M
Enabling Activities	**5. Stakeholder Engagement**	• Inability to build and maintain effective relationships with key stakeholders.	M		M	M	L	M	M	M
	6. Governance/ Ethics/ Integrity	• Fraud and misconduct risk - ineffective processes and policies for core business strategy, managerial governance such as performance monitoring, decision-making, delegations, risk management, allocation of roles and responsibilities.	L	M	L	M	L	M	M	L
	7. Knowledge /Systems Management	• Lack of integrity or confidentiality of information • Loss of availability of systems, intellectual property, etc.	M	H	M	M	H	M	H	M
	8. People/Culture	• Inability to achieve desired cultural and workplace reform, productivity targets, or to attract, retain (including key staff), utilise and develop people and culture or failure to maintain a safe working environment.	M	M	M	M	M	M	M	M
	9. Programs /Projects/ Contracts	• Material impact on budget or outputs due to failure to deliver organisational change through programs, projects and management of vendors or contracts.	M	H			H	M	H	M
	10. Resource Management	• Inability to manage resources to meet cost, quality and time expectations (e.g. meeting budget)		M		M	H	M	H	M

Emerging Risks

The dynamic nature of risk can be captured very simply with the intention of focusing on the discussion rather than the process:

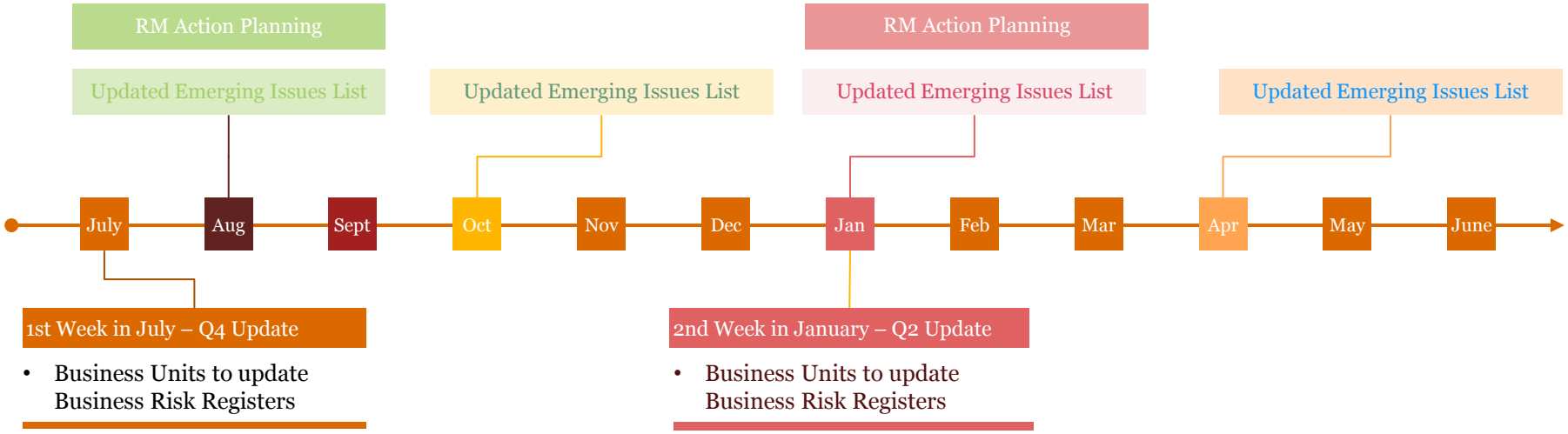
Ref	Issue	Brief Details	Source	Potential Impact
1	**New ICT Business Model**	- Impacts on business processes and operations resulting from the new ICT model that will have to be assessed and managed.	- Corp Group	- Service Delivery - Org Effort
2	**Project XXX including XXX Replacement**	- Divergence between current and future state technology - Opportunity to leverage replacement project to improve quality, integrity and timeliness of financial and non-financial data	- Business Unit A	- Financial - Service Delivery - Reputational - Org Effort
3	**XXX Business Model Transformation**	- Unable to build capability under the new model - Business continuity impacts throughout the transition	- Business Unit B	- Financial - Reputational
4	**Portfolio Management**	- Limited capacity and capability to deliver the extensive program of work across the organisation - No mechanism in place for effective prioritisation of competing program resources - Impacts on corporate teams (other than IT) has not been assessed	- RM Team	- Service Delivery - Org Effort - Reputational

Issues escalated to the leadership team sourced through a number of routes including:



Risk Management Calendar

A structured program of activities helps to maintain the value of the RM process and the relevance of the RM Function to management:



Key Features:

- ***Bi-Annual bottom-up Risk Register refresh****:* minimises the effort required to maintain BAU risk registers
- ***Quarterly Emerging Issues List refresh****:* ensures that changes in the environment are considered in a timely fashion
- ***Alignment of IA and RM activities****:* IA function to engage in the quarterly discussions and ensure ongoing relevance of the IA Plan . This may potentially remove the need for IA to undertake a separate annual planning round.
- ***Bi-Annual Executive Action Planning session****:* Pro-active action planning to address any issues / themes / opportunities identified

Summary and Key Messages

- ***Alignment*** *means clarification of the roles and accountabilities of the two functions, but also ensuring that practices (e.g. risk assessment criteria) are consistent wherever possible – gives management confidence that the assurance functions are talking the same language*

- *The use of* ***Risk Categories*** *is central to making the link between strategy. Appetite and the risk assessment process*

- *Both IA and RM needs to be* ***dynamic and responsive*** *to the changing business environment*

- *Critical to think about the* ***value and relevance*** *that the functions offer and to formulate plans accordingly*

Contact details

Nick Potter
PwC | Senior Manager
Direct: +61 (7) 3257 5356
Mobile: 0420 277 282
Fax: +61 (7) 3023 0969
Email: nick.potter@au.pwc.com
PricewaterhouseCoopers
Riverside Centre 123 Eagle St Brisbane QLD 4000
http://www.pwc.com.au