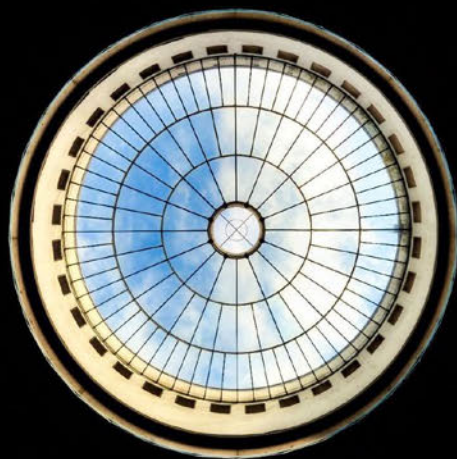


Deloitte.



Crown : Risk Management Framework Review
Discussion points

Ken McLay: Director, Risk Advisory (FSI)
February, 2019

Crown Resorts Risk Management Strategy

Within Scope of review

Outside scope but offered as suggestions to improve document

1. Governance: Has this been ratified by the Crown Melbourne Board – when ?
2. This is document sets out the Risk Management Framework – not Strategy. Consider changing title of Document to Crown Resorts Risk Management Framework Crown Resorts Risk Management Strategy and change RMS in doc to RMF
3. Perhaps reference this is the Group RMF to be adopted by all Group entities
4. Could reference risk culture in Exec Summary, As it is specifically referenced in the Principles
5. S3 Risk Management Principles. Could be strengthened with the additional comments that the RMF is also based on the principles of
 - Ensuring the safety and soundness of Crown
 - Supporting fair customer outcomes
 - Could reference forward looking and top and emerging risks
6. S3 Principles. Reference is made to risk culture. S5.5 also references 2LOD role in supporting Board's desired Risk Culture. Consider referencing risk culture elsewhere in Governance areas such as
 - 5.1 Role of Board - setting desired risk culture
 - 5.2 Role of RMC (or should it be ERCC for Crown Melb) – lead, oversight Ensuring the safety and soundness of Crown
 - 5.4 All staff have a role in embedding risk culture – not just CEO, Execs and Snr Mgt
7. S5: Risk Governance: Why is it that an effective risk governance framework applies to only material risks faced. Why not all risks. ? The reference to material risks in decision making is made a few times in the document
8. 3LOD table, The Business all staff responsibilities do not recognise the role of all staff. Note that s5.4 (b) bullet 3 does. So this is simply a matter of updating the graphic to support what is in the text (internal document consistency)
9. Re Governance table, It refers to a Risk Committee reporting to Board. That is Crown Resorts. Does this table need to be different for Crown Melbourne (ie ERCC not RC)
10. S5.4 opening statement refers to material business decisions, that is debateable as risk is part of all decisions. An accumulation of poor consideration of risk in small decisions could accumulate to a material risk event (reputational risk etc)
11. S5.5 Could argue that some Finance and HR roles are also 2LOD roles. But this is not a critical observation,
12. 6.2 Risk Appetite – refer separate page for discussion items

Risk Appetite

Within Scope of review

Outside scope but offered as suggestions to improve document

Risk Management Strategy Document,

1. The qualitative statement are not expressed in the form that is normally expected. While these are not wrong – they could be expressed more meaningfully
2. Weak definition/ give clarity on the terms material, significant etc or the period (e.g 5% point increase in staff turnover of rolling 12 months, fiscal period ?)
3. 6.3 Question . A trigger is a Breach of Risk Appetite ie Red , If so does that mean RMC will only be informed of “triggers” by exception. Good practice would also suggest that a “trigger” is the threshold that alerts management that there is a real risk that a breach of risk appetite may occur unless business activities are curtailed or risk appetite is changed. Best practice is that potential breaches are discussed at RMC – not just breaches
4. 6.4 What is the process when an event occurs leading to a potential breach or an actual breach of Risk Appetite, Current wording does not give enough clarity on accountabilities
 - Escalation to line manager, Exec, RMC, Board
 - How soon after identification, immediate, next reporting cycle
 - What it reported (What, When, How, Impact, Mitigation, Lessons learned)
5. Matrix: Could be clearer on what is in and outside of risk appetite with reference to thresholds. 6.4 What is the process when an event occurs leading to a potential breach or an actual breach of Risk Appetite;
6. S7, Is there clarity that the review of risk appetite should be aligned to and embedded in the strategic and business planning cycle

Other

1. Is it the intention to have Departmental Risk Appetite Statements , ie will departmental risk registers and risk profiles map to risk appetite
2. How does risk reporting show the aggregation of risks to inform Crown Melb risk appetite
3. How is risk appetite cascaded to the Departmental CEO and reflected in their plans and decision making
4. Does risk appetite form part of Exec role profiles, performance objective setting and performance assessment and remuneration

Risk Appetite: Discussion

Within Scope of review

Outside scope but offered as suggestions to improve document

1. Crown has identified 7 Risk Appetite Categories – in place since Dec? Lets call these Level 1 Risk Appetite
 - Each - has a qualitative statement and an qualitative metric
2. The Corporate Risk profile report (ie Nov 2018) has a comprehensive list of risks and definitions and an inherent and residual risk assessment, for example
 - Terrorism, disruption to demand for services, Third party risk, Aviation, Bad debts
 - For the sake of discussion lets call these Level 2 risks
3. These are mapped to the Corporate Risk Map (?)
4. Question/ Observation:
 - How do these “Level 2” risks map into the Level 1 Risk Appetite categories
 - If Level 2 risks are considered material risks, and reported and mapped into the matrix, should they have their own risk appetite statement?
5. General question as a illustrative point. Finance refers to shareholder value and measured by EBITDA and capital , equity injection. It would be expected that Crown has some firm policies around funding or liquidity (?). Are there risk appetite statements for these, if so should they form part of the risk appetite statements and a Level 2 risk ?
6. Are the Risk Appetite tolerance levels set relative to the size of Crown Resorts OR Crown Melbourne ? They look the same. Should they be?
7. Is it the intention to have Departmental Risk Appetite Statements , ie will departmental risk registers and risk profiles map to risk appetite?
8. How does risk reporting show the aggregation of risks to inform Crown Melb risk appetite?
9. How is risk appetite cascaded to the Departmental CEO and reflected in their plans and decision making?
10. Does risk appetite form part of Exec role profiles, performance objective setting and performance assessment and remuneration?

Governance

Within Scope of review

Outside scope but offered as suggestions to improve document

Clarifying questions

1. ERCC

- Why Chaired by Legal?
- Is this a subcommittee of the Crown Melb Board (as RC is for Crown Resorts)?
- What are the delegated authorities of the ERCC?
- ie Charter it says it is supported by – should it reference its sub committees " e.g is Fraud Committee?
- Should Charter reference managing risks within risk appetite, and oversight of risk culture and ownership review of risk management policies ?

2. Fraud Committee

- Where is reference to risk appetite, does it review it, propose it ?
- It refers to "Objectives" should this not be "Responsibilities and Duties"?
- Where does it get its delegated authority from and to whom does it report (ERCC)?
- Why is there noone from the Business on the Committee?

1. Crown Resorts Risk Management Policy

- Says there is a risk register – is there one for Crown Melb?

2. Can we see Crown Melb Board Charter?

3. Crown Melb Risk Mgt Update June 2018

- Reference to Departmental risk registers to be formalised – what is the progress on this ?
- What is status of departmental risk profile

Positive Observations

Outside scope but offered as suggestions to improve document

Within Scope of review

1. Commenced journey
2. A lot of progress over a short period of time
3. All the key elements exist – but recognising the short time frame there is still considerable effort for to be embedded and refined
4. Sound risk management principles
5. Recognition of the importance of risk culture
6. Board approved RAS (confirm date)
7. Recognition of a strong and independent 2LOD
8. There is recognition of the role of risk as aligned to strategy
9. Recognition of escalation of risk appetite breaches and accountability
10. Risk Matrix and Corporate Risk profile evidence considerable depth of understanding and scope of risks to Crown Melb
11. Good reporting / recognition of emerging risks (ERCC)
12. Evidence of 1LOD raising risk issues (ie CMO and Data) challenge of existing risk ratings (email Jan 14 and “industrial action” rating
13. Reference to cascading of risk framework via Risk Registers and Corporate Risk Profiles, **Can we discuss**

Deloitte.

Proposal only

This proposal is not intended to be a binding offer or to give rise to a binding contract with us. If you would like to accept our proposal please let us know and we will provide you with an engagement letter which will be the basis of the contract between us for the proposed services. This document and the information contained in it is confidential and should not be used or disclosed in any way without our prior consent.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of more than 200,000 professionals, all committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, Deloitte Global Services Limited, Deloitte Global Services Holdings Limited, the Deloitte Touche Tohmatsu Verein, any of their member firms, or any of the foregoing's affiliates (collectively the "Deloitte Network") are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

© 2018 Deloitte Australia Cyber Intelligence Centre