



**Junket Due Diligence and Persons of Interest Process
Review**

Crown Resorts Limited
XX July 2020

Our Methodology

A customised four-phase approach to assessing Crown’s decision making processes relating to junket operators and persons of interest (POIs).

Background

Deloitte were engaged to conduct a review of Crown’s decision-making processes related to junket operators and persons of interest (POIs). The purpose of the review is to identify opportunities for Crown to enhance its junket operator and persons of interest due diligence frameworks to ensure that Crown is well-placed to make appropriate, informed decisions in accordance with Crown’s risk appetite.

Approach

Our approach involved conducting a review of relevant policies and procedures, internal communications and other documentation as deemed relevant. We also undertook interviews with the key Crown staff and leadership team involved in the processes. We have consolidated our findings through end-to-end mapping of the current decision-making processes relating to new and existing operators and POIs.



Executive Summary (1/2)

Murray

3. Matters to be reviewed

3.1 The Review is intended to make recommendations in relation to:

- a) Crown's **decision-making frameworks in respect of junket operators**, and the Crown policy settings which inform the decisions Crown makes in respect of junket operators;
- b) Crown's **decision-making frameworks in respect of persons of interest**, and the Crown policy settings which inform the decisions Crown makes in respect of those individuals;
- c) **how these frameworks and processes might be improved** to assist in the making of decisions reflecting Crown's risk appetite; and
- d) **the reporting to, and involvement of, Crown's board and board sub-committees** in relation to these matters.

Add terms of reference as an appendix

Executive Summary (2/2)

Murray – can we discuss on Monday what action required here?

DRAFT

Add terms of reference as an appendix

03 | New Junket Operators

DRAFT

New Junket Operators

Introduction and areas of focus

Murray – for
review

The processes for assessing and approving prospective junket operators at Crown Melbourne (Crown) are primarily managed by Crown's Credit Team, who are responsible for conducting due diligence and open source research to produce a recommendation for the decision maker as to whether or not Crown should enter into business with the junket operator.

The process has been subject to a number of enhancements over the last few years, however our review has focussed on the current state, with further information on the enhancements included within Appendix D.

We have made a number of recommendations for Crown to strengthen its processes, which have developed organically. Notably these include defining probity and Crown's risk appetite in this space, along with increasing the role and involvement of other key parts of the business to support the Credit Team in their initial assessments.

Our review examined three areas in relation to Crown's processes regarding prospective junket operators: information inputs; the process for assessing an application and the role for different aspects of the business.

A – Information Inputs

- Information obtained from prospective junket operators
- Due diligence searches
- Internal information
- Staff training

B – the Process for Assessing an Application

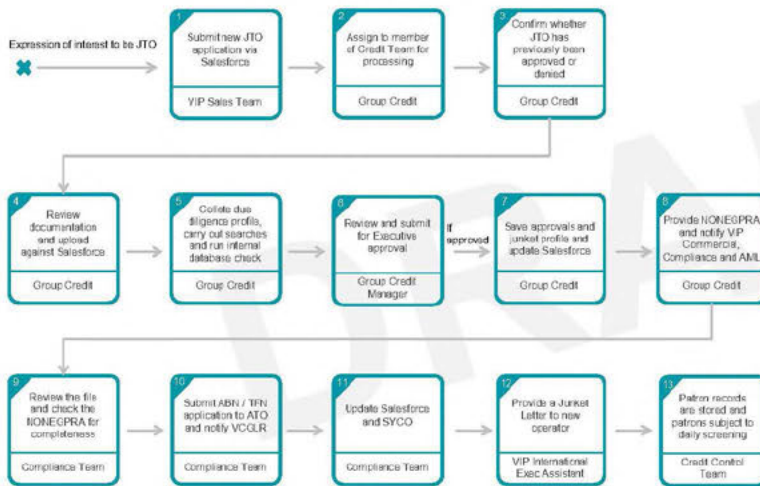
- Definition of probity and risk appetite
- Scope of Crown's Due Diligence Assessment
- Policies and procedures
- Information management and documentation
- Characterisation of risk associated with Junket Operators
- Reliance on DICJ Licensing Process
- Decision making process

C – the Role for Different Aspects of the Business

- The role of the Credit Team
- The assessment of red flags
- Three lines of defence model
- Policies and procedures

New Junket Operators

Process map: the junket operator approval process and documentation



© 2020 Deloitte Risk Advisory Deloitte Touche Tohmatsu

JTO APPLICATION INCLUDES:

- JTO's personal details
- Joint NONEGPRAs (Melbourne & Perth)
- Passport
- ID card or driver's license
- Proof of address
- Business card
- Personal cheque
- Police check
- DICJ license
- ABN / TFN or application
- Credit or cheque cashing facility request
- Application for deposit account, cheque cashing, credit facility/funds advance facility

+ ADDITIONAL DOCUMENTATION

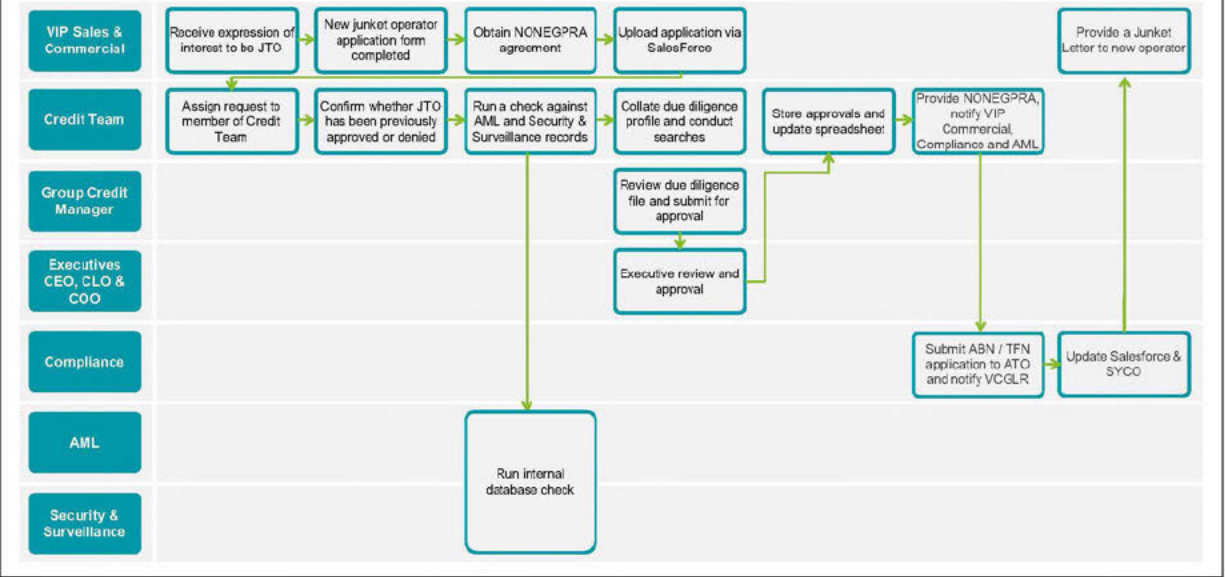
- Evidence of other junket operations
- Source of wealth
- Comments/other information

DUE DILIGENCE FILE INCLUDES:

- Crown history
- Other casino activity
- ID details
- Police check from every country of residency
- Police check via Fi2Work (Hong Kong & Singapore)
- DICJ link
- VEVO check
- DOW Jones
- Global Data
- Wealth X
- Factiva
- Searches: personal, company, property
- Recommendation

New Junket Operators

Process map: roles in the junket approval process



A – Information Inputs (New Junkets) (1/3)

All prospective junket operators are required to submit an application and supporting documentation. Crown's Credit Team then conduct due diligence, including through use of external providers and open source searching. To strengthen the process, Crown could request more information up front to allow for further verification and interrogation through the due diligence checks, and ensure that these are sufficiently tailored towards the international nature of the junket sector.

Information obtained from prospective junket operators

Prospective junket operators are required to complete an application form and provide supporting documentation. Mandatory supporting documents include a police check, identification documents including and credit related applications. The form also includes a space to provide additional documentation such as source of wealth and evidence of other junket activity.

Declarations are not sought regarding litigation history, financial situation or other business operations. Other gaming companies require operators to make specific declarations in relation to these issues. The advantage of such declarations is to strengthen the due diligence approach by collecting information from the operator which can be checked throughout the process. Requiring declarations can also deter potential dishonesty or corruption in the application process.

Due diligence searches

Crown currently makes use of a number of external providers whilst carrying out searches into prospective junket operators as part of the due diligence process, including:

- Factiva: searches on name and date of birth.
- WealthX and Global Data: aggregators of information, which focus heavily on wealth.
- Acuris C6: provides reporting on compliance and reputational issues.
- Google searches.

Of the searches undertaken, Acuris C6 provides the highest quality reporting for matters of compliance and reputation risk, however is used infrequently by Crown due to cost, primarily at the start of a new relationship. We have provided further insights into the providers used in Appendix E.

The current providers are generally limited when searching in Chinese. Recognising the international nature of the junket sector, additional providers such as Wisers and Baidu may supplement the information obtained through the current process.

© 2020 Deloitte Risk Advisory, Deloitte Touche Tohmatsu

Internet searches are currently run through Google. Best practice in this area is to use multiple search engines as well as metasearch engines to provide a more comprehensive findings.

Our review of these sample due diligence files indicated that online searches do not include additional investigation of companies that the operator is affiliated with or known associates. In one of the due diligence files we reviewed, we found that potential adverse information had been identified regarding potential business associates and affiliated company. This information was listed in the due diligence summary, however additional searches did not appear to have been conducted by Crown to verify the information.

Recommendations

We recommend that Crown considers seeking declarations from prospective junket operators as part of the application process, including on litigation history, financial situation and other business operations. This will strengthen the due diligence approach through providing the Credit team with additional information to cross-reference through their searches.

Our review identified that there are opportunities to strengthen the junket due diligence through ensuring it is sufficiently tailored to the international nature of the program, including through:

- Ensuring Crown's operational preferences for all current external due diligence providers are set to include searches in the relevant languages used by the prospective operator.
- Conducting searches on junket operator and agent aliases.
- Considering using international providers as part of the due diligence process, such as Wisers and Baidu.

Label completed for review

A – Information Inputs (New Junkets) (2/3)

The due diligence research for prospective junket operators is currently conducted by Crown's Credit Team and can be strengthened through additional training in opensource research and improved access to internal information and intelligence held by Crown. Recent introduction of an internal check with the AML and Security and Surveillance teams is a positive step in increasing the robustness of the due diligence process, however this is not yet documented within training or policy documentation to ensure consistent application.

Internal information

Currently, different departments within Crown maintain independent databases and intelligence records. This reflects the differing roles the departments play in Crown's overall integrity program; with the Security and Surveillance and Compliance departments responsible for liaising with law enforcement, and AML overseeing suspicious matter reports and the transaction monitoring program. Whilst it is necessary to restrict access to sensitive information, the lack of a holistic view of internal intelligence could result in Crown entering into a relationship with an operator about whom adverse information is held internally.

To mitigate this risk, the Credit Team has recently introduced an additional check into its junket operator due diligence process, which involves cross referencing the operator details against internal databases held by the Security and Surveillance and AML teams. This check provides a positive measure towards ensuring Crown's systems are effectively aligned, however at present is not formalised within policy or training documents therefore may not be consistently being applied.

The presence of a trace on Crown's internal databases however is an important consideration for the decision maker, which may signal adverse information being held regarding the prospective operator from any previous dealings with Crown or intelligence received from external agencies or other casinos.

Crown's policies should formalise this check within their processes, and include guidance on how any identified traces are investigated and communicated to the decision maker, to ensure they are effectively reflected and considered within the approval process.

Staff training

The due diligence process is currently conducted by staff in the Credit Team who have not received formal open-source research training.

Furthermore, the internal training guide outlining the process does not include details of different risks, AML typologies or red flags that should be considered whilst carrying out the searches and checks.

Recommendations

We recommend that Crown formalises internal checks as part of the junket approval process. These should be included within policy and training documents to ensure consistent application.

Deloitte recommends that those staff members in the Credit Team who are responsible for conducting due diligence are provided with formal training in open-source research and information collection. We also recommend that the internal training documents are supplemented to include guidance on carrying out searches and due diligence checks, including risks, red flags and typologies, along with better defined escalation points and triggers for further investigation.

Recommendations: We recommend conducting training to enhance in-house research capabilities by the following:
Developing and finalizing the Research Manual be further for utilisation by staff undertaking the due diligence checks and online research.

Developing a categorization of reputational risks such as 'Financial Crimes', 'Money Laundering' and 'Criminal Associations' in the Research Manual in order to better communicate or escalate potential risks to other teams.

Conducting staff training in advanced open-source information collection and research methodologies to increase the likelihood of adverse information being detected.

A – Information Inputs (New Junkets) (3/3)

XXX

Murray

Use of external investigations support

At the current time Crown does not engage third party investigation support to undertake due diligence in relation to junket operators. Across the industry it is common for companies to utilise appropriately qualified investigation providers to undertake in depth due diligence into identified high-risk business partners, including junket operators.

The value of this approach is the ability to undertake research in the relevant local languages by professional investigators who are familiar with accessing the relevant corporate and other records available in a particular jurisdiction. For example, a number of Chinese legal records can only be accessed within China via a manual search of a particular database. Third-party information aggregators such as those utilised by Crown are often unable to access this information.

Typically, providers will also undertake standard compliance checks related to international sanctions, conduct local language media, corporate records and litigation searches and where required can conduct inquiries via in-country contacts to obtain information on the reputation and background of operators.

Organisations differ in how and when they utilise such services. Some casinos outsource the due diligence process to an external provider while others will only engage these services where initial red-flags have been noted in the course of their in-house research. Given the value of research being conducted in local language by staff trained and experienced conducting due diligence research in the relevant jurisdiction, including this capability can significantly enhance the robustness of the due diligence process.

Recommendations

Crown identify suitably qualified investigations professionals with the experience and capability to undertake more in-depth due diligence investigations in regions relevant to the junket program. Given Crown already undertakes its own due diligence research, it is recommended this support be engaged on an as needs basis when red-flags are noted during the course of research but are unable to be resolved.

© 2020 Deloitte Risk Advisory, Deloitte Touche Tohmatsu

11

Recommendations: We recommend conducting training to enhance in-house research capabilities by the following:
Developing and finalizing the Research Manual be further for utilisation by staff undertaking the due diligence checks and online research.

Developing a categorization of reputational risks such as 'Financial Crimes', 'Money Laundering' and 'Criminal Associations' in the Research Manual in order to better communicate or escalate potential risks to other teams.

Conducting staff training in advanced open-source information collection and research methodologies to increase the likelihood of adverse information being detected.

B – the Process for Assessing an Application

XXX

Definition of probity and risk appetite

There is no clearly articulated risk appetite statement regarding the junket program, nor is there a clear definition of the term 'probity' in the context of junket operations. Clearly articulating Crown's risk appetite and defining what is meant by probity in relation to junket operators guide decision-making and define the risk factors which are to be assessed through the due diligence and approval process.

Crown's 'Junkets & Premium Players Internal Control Statement' ("ICS") aims to identify and evaluate risks inherent in the conduct of Junkets and Player Programs. According to the ICS Risk Assessment Matrix, the possible occurrence of criminal influence and exploitation may have moderate reputational, operational and financial risks to Crown. Overall, the risk presented by Junket Operators is deemed as significant.

We note the current version of the ICS was approved by the VCGLR in December 2015.

The ICS outlines the various Minimum Standards and Controls underpinning the Risk Assessment of Operators and Players. In section 2.5 of the ICS, Crown states that "Crown will ensure that it has robust processes in place to consider the ongoing probity of its registered Junket Operators, Junket Players and Premium Players". The ICS does not explicitly define Crown's definition of probity in relation to the junket program. Similarly, no explicit definition of probity is included in the Junket SOPs document.

Probity in relation to junket operators is instead operationalised throughout the document guiding the junket due diligence process. Current and previous versions of documents relating to Crown's program note one component of the assessment of probity as "the absence of a criminal record which is verified by Crown obtaining either a current police clearance or evidence of registration with the Macau JICJ".

We noted also Crown's discussions with the VCGLR in 2003 during which the regulator accepted that if a junket operator or agent was able to obtain a visa and to travel to Australia, this constituted tacit probity approval. This is reflected in the Crown Junket Processes requiring that Operators physically visit an Australian Crown property prior to the maiden junket visit and at least every two years thereafter.

The most recent review of junket processes completed in March 2019 notes Crown's brand and reputation may be compromised should junket program activity be linked to unethical or criminal conduct and states program activity must ensure integrity and transparency. This recent definition is indicative of the growing recognition and understanding of the risks associated with the program and this is reflected in the ongoing enhancements of the due diligence process. However, there is a lack of explicit definition of these risks in related policies and procedures. It also remains unclear whether the consideration of probity includes, or is in addition to, the assessment of the creditworthiness of the Operator.

Recommendation

Deloitte recommends the Junket Program ICS and related policies and procedures regarding junket onboarding and due diligence be updated to include a specific statement of the legal and reputational risks which are to be considered during the process. At a minimum, we recommend this definition include consideration of criminal history, potential money laundering and other forms of financial crime (e.g. fraud and corruption), financial and trade sanctions, and unethical business practices (e.g. forced labour etc.).

B – the Process for Assessing an Application

XXX

Murray

Scope of Crown's Due Diligence Assessment

Crown's current due diligence process applies to Junket Operators and Premium Players, and both groups undergo the same due diligence procedures and assessment of credit worthiness. Our discussions with Crown staff highlighted the awareness that the process should also include the Agents appointed by Operators.

From our understanding, Agents act as the representative for the Operator, often being present to manage the group during the visit to Crown. We were informed that Agents often have financial delegations on behalf of the Operator, including arranging cash outs and transfers as required. Given their position, Agents present a potential risk of legal and reputational issues for Crown.

While we note the additional ECDD applied under the AML Framework to Agents who visit Crown, their important role in junket operations warrants further due diligence being conducted. We note that while Crown keeps records of Agents attending the casino, no electronic records are kept regarding which Agents attended various visits or when they were added or removed by the Operators.

Crown's approach differs from that of other companies who obtain an approved list of agents at the outset of the relationship and record and track their visits to the casino over time. Including Agents as part of the due diligence process will assist in strengthening Crown's approach and improve the opportunity to identify individuals with known adverse histories.

Recommendation

Crown obtain details of authorised Agents as part of the initial information provided for new Operators and that these Agents be subject to risk-based due diligence procedures along with the Operator. We recommend also that Crown consider recording information about when Agents are added and removed by Operators and formally documenting their visits to Crown.

Information management and documentation

The records for Crown's current junket program are maintained via a series of excel workbooks which maintain records of the operators approval and revalidation details. These spreadsheets are then cross-referenced and updated from the other relevant internal systems via manual updating of the junket operator register.

Information collected during the due diligence process along with the due diligence summary sheet are contained on a secured shared drive with each operator being allocated a separate folder. We were informed the information contained within the folders has historically been updated by adding only the most current findings into the folder and replacing any previously held documents. Crown has identified the difficulty this creates in locating previously obtained information and in being able to recreate the exact information put before decision-makers when reviewing past decisions. Under the current processes, the executive decision-maker receives a hard copy of the due diligence summary and file for review which are not then retained as a record.

This approach to collecting and storing information is not optimal in creating an auditable trail of the due diligence process and documenting the discovery of information throughout the due diligence process. Crown is currently considering what enhancements can be made to this approach to improve record keeping within the due diligence and approval processes.

Recommendation

Crown should create a digital, point in time record of all information collected during the due diligence process along with the due diligence summary and the recorded outcome and rationale of the decision for the purpose of establishing a clear audit trail.

B – the Process for Assessing an Application

XXX

Murray

Characterisation of risk associated with Junket Operators

We note the due diligence process has evolved organically alongside the assessment of creditworthiness. The information collected at the outset of the onboarding process, as outlined in Section XX, is limited to basic identification, ABN registration and signed agreements. The first phase of review conducted by the Credit Team is focussed on establishing identification and creditworthiness. It is during the subsequent due diligence phase, that efforts are undertaken to obtain information relating to the reputation, track record and probity of the Operator.

As part of this initial review, the Credit Team allocate a Category Number based on the reliability information provided by the applicant and the weight attached to the KYC information as outlined below.

| Code | Description |
|------|---|
| 1 | DICJ Individual License Holder / Director of Corporate License Holder |
| 2 | DICJ Collaborator License Holder (per CGD list only) |
| 3 | Shareholder of Company who holds DICJ license |
| 4 | Director / Shareholder of Parent Company who holds DICJ license |
| 5 | Expired DICJ Principal License Holder |
| 6 | Director / Shareholder of Company who holds Expired DICJ license |
| 7 | Certificate of Criminal Record / RIZWork |
| 8 | Junket in another jurisdiction (non DICJ) |
| 9 | Other (e.g. unverified sub-agents, guarantors) |
| 10 | No link to DICJ or other jurisdiction |
| 11 | Ceased relationship with Crown |
| 12 | In progress |

© 2020 Deloitte Risk Advisory, Deloitte Touche Tohmatsu

From our discussions with Crown representatives, we understand this scoring system was developed as part of the review of Operators conducted in 2017. While we recognise the score is only finalised following approval, we observe it acts as a form of risk score during the due diligence process.

We note that applications that have a Category Number of 1-4 are assigned a green marker whereas applicants who have Category Numbers of 5-8 are assigned an amber marker. Unverified sub-agents and guarantors are designated in red, inferring that they are of higher risk. During the assessment process, the applicant is given a Category Number of "12" which indicates that the application is 'In Progress'. As more information is obtained throughout the process, the score is varied to reflect the increased information and understanding gained about the operator.

Recent changes to make obtaining a police clearance mandatory for all operators and obtaining clearance from multiple jurisdictions where an operator is identified as resident in different countries is a welcome enhancement. However this is yet to be updated in the approach to allocating a category number.

The allocation of the Category Number to Operators is not consistent with the scoring regime utilised under the AML program. The current credit scoring approach focuses predominantly on whether the JO is registered with DICJ or has provided some means to check criminal history. It does not appear to consider other potential reputational risks that may be associated with the operator or agents.

Recommendation

Crown should consider aligning the risk assessment processes for junket operators with other risk assessments, such as the AML rating, and create a single risk assessment of each operator. This rating should be established at the outset and updated to reflect the outcomes of the due diligence process. For example, the risk assessment should also reflect any potentially adverse reputational issues noted in connection with the operator.

It is also recommended Crown consider the appropriateness of separating the assessment of potential risks from the process for assessing creditworthiness. As noted in the approach taken by the Star, commercial and credit decisions are made after due diligence into potential risk has been completed.

B – the Process for Assessing an Application

XXX

Murray

Reliance on DICJ Licensing Process

It is also clear from our discussions that the Crown Credit Team have conducted independent research to understand the DICJ process for licensing Operators. The Credit Team Management has undertaken research using the available documents from the Macau Department of Justice ("DOJ"), to understand what information is collected by the DICJ.

We observed that Crown has historically placed a high level of trust in the DICJ Licensing Process. Emphasis is placed on DICJ registration, or a valid police clearance, as a mandatory requirement before progressing in the process. Whilst we understand that DICJ conducts some verification and research on applicants, we note that the central criteria for obtaining a license is that the individual does not have a criminal record.

Recent changes to Crown's approach has strengthened this process by making mandatory that Crown obtain a police check from the country of origin irrespective of whether the operator holds a DICJ licence.

Where an operator is not registered in Macau, Crown's current process has historically relied on the police check a police check obtained from the home jurisdiction to satisfy the requirements. The most recent update to the program now requires that, in the event an operator is identified as being resident in multiple jurisdictions, that a police check from each relevant jurisdiction is obtained.

Observation

Recent changes to the junket operator requirements have sought to reduce reliance on the DICJ licence as a proxy for police clearance and has introduced a mandatory requirement for clearances from multiple jurisdictions where relevant. Over time, this is will improve the quality and reliability of the information obtained in relation to the probity of the operators.

© 2020 Deloitte Risk Advisory, Deloitte Touche Tohmatsu

Decision making process

Crown's current approval process for new junket operators adequately reflect the risks associated with the program. Following completion of the due diligence and internal review by the credit leadership team, the Due Diligence Summary Sheet and all underlying information collected during the due diligence process is provided to the executive approval team consisting of the CEO, CLO and the COO. After reviewing the information, this committee is responsible for approving the new junket operator application.

Through our consultations with Crown staff, it was evident this process does involved genuine critical review of the information and we were informed decision makers can and do refer questions for additional research back the credit team in instances where they consider further information is required to inform their decision.

We did, however, note several areas for improvement related to the documentation and communication of executive decisions in relation to junket operators. During interviews with Crown staff, we noted that staff often have limited visibility of decisions made, particularly when a decision is made to continue business with an operator that has been subject of adverse reporting during the due diligence process.

During our engagement, we reviewed three examples of completed due diligence files that had been prepared as part of the annual review process for existing junket operators. In one of these files, we noted the individual was listed as a former shareholder of a company with which Crown had ceased to business some years prior. While the summary included reference to this shareholding under the bullet points for both the GlobalData and Acuris Risk Intelligence findings, the summary sheet provided no further analysis and did not make reference to Crown's having ceased its business relationship with the company. Such information is relevant to the decision and should be explicitly highlighted for the attention of the decision maker.

Recommendation

The junket due diligence summary should include the rationale for the decision made and held on the junket due diligence file. Creating a contemporaneous record of both the decision and the rationale would strengthen Crown's ability to review previous decisions and help to ensure all relevant issues have been considered.

B – the Process for Assessing an Application

XXX

Murray

Communicating risk categories in the due diligence summary sheet

We have reviewed the current due diligence summary sheet which has been enhanced recently by creating an excel based summary of all due diligence information collected throughout the course of the credit team's work. This document replaces the earlier Microsoft Word-based template.

In reviewing a worked example of this new format for one existing junket operator. An example related to a new junket application was not available given the recent introduction of the new format and the shut-down of Crown's activities due to COVID-19 meant it had not yet been used for a new application.

We note that the sheet adequately summarises the outcomes of all searches undertaken and includes a section for the Credit team to make recommendation to the decision-maker. In reviewing this document, we noted it has been improved to include the historical information collected through the course of the relationship with the particular operator.

Within the summary reviewed, we not key information derived from the external data sources largely related to wealth information rather than other risk categories. Our discussion with the team noted no adverse information had been noted in relation to this particular operator.

The summary sheet does not include specific consideration of the risk categories which were investigated throughout the due diligence process. For the purpose of informing the decision made by the executive, the due diligence sheet could be improved to explicitly document the risk issues to be considered and highlight whether any information was or was not found in relation to these issues. The specific categories should align to those outlined in defining probity and Crown's risk appetite in relation to junkets as outlined in section XXX.

The current version of the due diligence summary sheet should also incorporate an area for the recording of both the decision made and a short statement from the executive explaining the rationale for the decision. Once recorded a contemporaneous record of the document and the underlying information should be created and stored securely.

Recommendation

We recommend the due diligence summary template be updated to include:

1. Documentation of the risk categories considered in the due diligence research and the findings or otherwise against each of the categories; and
2. A section for the decision-maker to record to record the outcome and the rationale for their decision.

C – the Role for Different Aspects of the Business

XXXX

Murray –
Review

The role of the Security & Surveillance in the due diligence process.

Under Crown's current process, responsibility for the junket operator due diligence rests with the Credit Team. We note that historically this process has involved limited input from other risk owners in the business such as the AML team or the Security & Surveillance teams. While the Compliance team has had an ongoing role since at least 2017, until recently this has largely focussed on ensuring compliance with the requirement to notify regulators of junket relationships and ensure records are up to date.

Under recent enhancements, we note an increasing role for other teams within the process. Additional internal checks have been introduced earlier this year to ensure the Credit team undertakes checks with the security and surveillance team and include these results within the due diligence process. We note this takes the form of an email to the security and surveillance team who respond with whether there are suspicious matter reports (SMRs) or other information held in relation to the operator, including law enforcement referrals.

In the due diligence files reviewed in this engagement we noted examples of these checks that highlighted the existence of suspicious matter reports related to the named operator without providing details of these reports. While such reports are sensitive in nature and they should be managed appropriately, Crown's current Junket Operator procedures do not outline how these traces are resolved and who is responsible for obtaining further information on the content of these traces to be put before the decision-maker.

Recommendation

Crown update relevant junket policies to document the process for obtain trace checks from security and surveillance and outlined the procedures for resolving these traces within the decision making process. The results of the trace checking should be highlighted within the due diligence summary for consideration by decision makers and executive decision makers should outline what steps have been taken to review and consider this information.

The role of the AML team

Historically the AML team has had a limited role in the oversight of Crown's junket program. We were informed a key reason was the limited resourcing of the AML and the historical nature of the program. We are aware Crown is currently making investments into the AML team to support their work and that internally Crown is assessing options for strengthening the role of the AML team in the program.

This work is encouraging and should be prioritised. Given the significant risk of financial crime within junket operations globally, the AML team should have a central role in overseeing all aspects of the new junket registration program. Crown recognises these risk by considering junket operators as high risk under the AML program, however this prioritisation is not adequately reflected throughout the due diligence process as it currently stands. It is critical Crown's processes support it gaining a holistic view of the risk associated with a junket operator from the outset of the process. Including AML team members at the commencement of the due diligence process and throughout is required to ensure all potential red flags are considered and identified appropriately.

We note the Credit team has undertaken independent work to uplift their knowledge of AML/CTF risks and that this is ongoing. Their role should be supported by staff appropriately trained in AML/CTF and conducting enhanced due diligence who review the research and provide input on each case before a decision is made about the relationship. The outcome of AML review should be explicitly documented within the due diligence summary.

Recommendation

Crown strengthen the role of the AML team within the due diligence process to ensure a holistic view of risk is established at the outset of the due diligence process and establish a rating system that creates a holistic view of the potential risks and outlines the appropriate red flags to be investigated throughout the due diligence process. The due diligence research should be fully reviewed by an appropriately trained and experienced AML analyst during the research and prior to being forwarded to the decision maker. The outcomes of this review should be recorded on the due diligence summary sheet.

C – the Role for Different Aspects of the Business

XXXX

Murray –
Review

Three lines of defence model

As the customer facing team, VIP international are the first line of defence in the junket approve process. This is not articulated, and their role in contributing to the integrity process is not defined within the process and policy documentation. This includes a documented list of potential red flags they may encounter. We note the team do receive in person training from Compliance however, which will assist with clarifying their roles and responsibilities regarding the probity of the process.

During our consultations we were informed Crown is currently assessing how a three lines of defence model may be applied to the junket program. Establishing clear roles and risk accountabilities via a three lines of defence model would significantly enhance the identification and management of risk throughout the junket program.

Within this model, VIP international should be considered as the first line with both Credit and AML acting as second line functions to manage in the in-depth due diligence and approvals program and providing specialist input to the VIP international teams. At the current time, the most detailed outline of Crown's process for new junket applications is in the form of a training document for the Credit Team. This does not include consideration of the role of the VIP Sales Team as the first line of defence, or the additional step of engaging with Security and Surveillance and AML as part of the information gathering.

The three lines of defence model should also establish the relevant audit function across the program to selectively review the approvals and due diligence process and ensure the appropriate policies and procedures are adhered to.

Recommendation

Crown continue with its work to establish a three lines of defence model across the junket program which clearly articulates the roles and responsibilities of relevant parties and provides clear guidance on the risk issues to be considered during the consideration of new junket applications.

Prospective Junket Operators

Key Findings

- c) *the role for different aspects of the business, including the AML department, the compliance department, the credit department, the VIP International department, and other aspects of the business, in the assessment process; and*
- Credit Team
 - DD process managed by the credit team – historically a limited role for AML and Compliance and little to no oversight
 - Lack of holistic view of risks across the relationship
 - Assessment of the right red-flags
 - AML and Sec & Surv need a greater role
 - AML should review before the decision maker stage
 - Already considered high risk under AML program
 - Policies & Procedures
 - Need to articulate roles and responsibilities clearly
 - Three lines of defence model
 - VIP international are the first line but probably don't see it that way
- d) *the governance framework and responsibility for approving a new junket operator, including whether the framework and processes are well designed to make decisions reflecting Crown's risk appetite.*
- Executive level decision-making
 - CEO, Chief Legal and COO – appropriate level
 - Clarity required around the risk appetite and the risk focus of the decision-maker

Sid comments:

Operating model perspective

Be clear about what we're doing – it is not an operating model design – this is a specific piece on how they might build an op model.

04 | Existing Junket Operators

DRAFT

Existing Junket Operators

Introduction and areas of focus

Following the initial approval process, Crown has a number of measures in place to review its existing relationships with junket operators and monitor the probity and integrity of the program.

The central control involves an annual review, again led by Crown's Credit Team. This involves re-verification of the documentation held by the junket operator, and conducting repeat checks using a number of the same inputs as mined during the initial due diligence process.

Alongside the review, there are a number of different measures in place that contribute to the ongoing probity of the junket program, including daily Dow Jones screening of patrons, spot checks into junket activity and an inactivity threshold.

As with the process for approving new junkets, Crown has recently introduced a number of control enhancements to strengthen ongoing probity of operators. These include requesting updated criminal record checks, and instituting Executive approval as part of the annual review process. Our review has identified a number of additional areas where Crown may be able to strengthen the process, including through improved collaboration and use of internal information.

Our review examined the following areas in relation to Crown's processes regarding existing junket operators: the information inputs considered in the annual review, including in connection with existing operators' activity; the process for updating previous probity and background checks and role of different aspects of the business.

A - the information inputs to be considered and sources to be mined in connection with the annual review, including in connection with existing operators' activity over the prior year

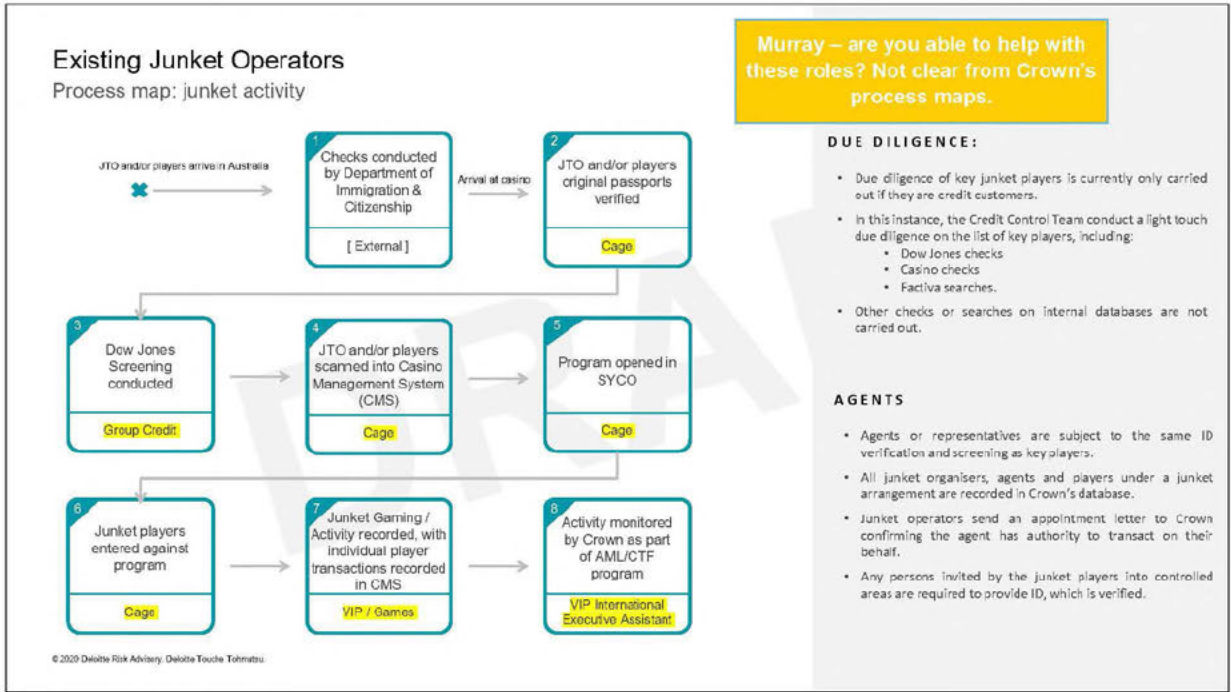
- Due diligence searches
- Internal information
- External information

B - the process for updating previous probity and background checks

- Annual review process
- Additional probity measures
- Junket agents

C - the composition of the committee reviewing existing operators and the role for different aspects of the business

- Composition of the committee reviewing existing operators
- Roles and responsibilities



Agents - play a huge role in game in the casino.

Believe that agents should be attributed same level of due diligence as the operators in advance of any visits. With same annual visits, same inactivity thresholds.

Players - do get EDD under AML program. Picks up PEPs etc. Players can be treated as anyone else who walks through the door.

Murray – for review

B - the process for updating previous probity and background checks

Diagram: ongoing probity measures for existing junket operators

- Our review has focussed on the annual review, which we recognise as the central process for updating the information held on file regarding existing junket operators, and reviewing this to ensure Crown still wishes to continue their relationship with them.
- We do recognise that there are a number of additional controls however which contribute to the ongoing probity of the junket program within Crown. These range from the daily screening of patrons, to the three year inactivity maker.
- Alongside controls around the junket operators themselves, junket players and activity are subject to Crown's transaction monitoring program, and subject to external reporting obligations. We have included further context around the regulatory environment in which junkets operate within Appendix B.

| | | |
|--------------------------|--|---|
| Daily | All junket operators and players are screened daily against Dow Jones. <small>Compliance</small> | Adverse hits on searches trigger a POI assessment form to be completed. <small>Manager, Compliance Reporting</small> |
| Monthly | Spot audits are carried out. <small>Gaming</small> | Meeting to cross reference junket records. <small>Group Credit Manager / Compliance</small> |
| Six-monthly | The junket register is reviewed to ensure compliance with processes. <small>Manager, Program Compliance</small> | The review includes: patron name, VCGLR notification, SVCO ID, ABN, minimum visit to Crown (every 2 years) |
| Annually | Due diligence is carried out on active junket operators. <small>Credit Team</small> | Annual due diligence refreshers are subject to Executive approval. <small>CEO, CLO, COO</small> |
| Every three years | After three years of inactivity, a JTO is marked inactive. <small>Credit Team</small> | After this time, a new application is required to resume activity. <small>Credit Team</small> |

© 2020 Deloitte Risk Advisory Deloitte Touche Tohmatsu 23

Annual review

Did security and surveillance pick up anything odd relating to that trip
 Were any SMRs raised during that trip / security and surveillance incidents / or other reporting that comes in/ Dow Jones
 Bit more thinking on what that needs to look like

Positive if Execs now having a role in annual review, Compliance should also review this first

Josh: We've got these large junkets, and a lot of small junkets. Instead of just relying on annual junket, we do need trigger points. If there's a ML request, we need to have trigger points which are embedded with people seeing them and recording them, understanding what's to be escalated to the committee. Instead of waiting for 12 monthly review process.

A - the information inputs to be considered and sources to be mined in connection with review, including in connection with existing operators' activity over the prior year

The annual review process of existing junket operators largely makes use of the same sources mined during the initial due diligence process, which can result in similar reports being received. To increase the robustness of this process, we recommend that Crown strengthens the processes to review information held both internally, and within its external network.

Due diligence searches

To ensure ongoing probity for the junket program, junket operators with an existing relationship with Crown are subject to an annual review process. This review comprises of a refresher of the due diligence checks, conducted by the Credit Team. As with the initial approval process, the team utilises Crown's external search providers to request reports on the junket operators, and conduct open source searches. Updated copies of required documentation are also obtained, including identification documents.

The same information sources are mined and external providers used for both the initial due diligence and annual review. During our consultation phase we were informed that this can result in very little to no change in the contents of the reports each time. As such, Crown tends to only obtain Acuris C6 reports every other year, due to the financial cost. As highlighted in the previous, we recognise Acuris as currently providing the highest quality reporting for matters of compliance and reputation risk. Through excluding its use in the annual review process, the information obtained in this process may therefore be less comprehensive than during the original due diligence process.

Internal information

Our review found that the mining of internal data sources for the annual review process is currently limited, as with the original junket approval process. The internal check with Security and Surveillance, and AML databases has also been included for the annual review, although as with the original junket approval process this is a recent development that has not been formalised within policy and process documentation.

During our review of due diligence files we found evidence of this check occurring in all three occasions. In two out of the three files, SMRs were identified, and SEER intelligence of Suspicion Transaction Reports was identified in the third. There was no further details provided, and these were not recorded on the summary form, which only provides a space to indicate whether an exclusion or barring was identified.

© 2020 Deloitte Risk Advisory Deloitte Touche Tohmatsu

The presence of a trace on Crown's internal databases is an important consideration for the decision maker and should be explicitly referred to within the summary sheet. Crown's policies should also explain how such traces should be resolved and require the decision maker to review this information prior to approving the continuance of the relationship.

Alongside internal checks, the process for sharing internal information could be strengthened through introducing additional feedback loops to share relevant intelligence following junket visits, for example whether any issues were encountered by Security and Surveillance or if any flags were raised by the transaction monitoring program. At present this information is only requested during the annual review, or if it is sufficiently serious so as to trigger the Persons of Interest process. Strengthening internal feedback loops and sharing any relevant information as part of the close out of each junket program would assist in building up the internal picture and determining whether reviews are required outside of the annual review process.

Additional information inputs

There may be scope for Crown to strengthen the annual review process via increased attention on external sources of intelligence, such as a holistic review across Crown's holdings, or through contacting other casinos. The review currently collates details of other casino activity of the junket operator, therefore there may be scope to verify this and obtain references to provide Crown with a higher level of confidence about junket operators it chooses to go into business with.

Recommendations

Deloitte recommends that Crown formalises its internal feedback and information sharing as part of the ongoing probity measures for junket operators. This should include considering more regular feedback loops to build up a more holistic picture of junket activity, and ensure that any concerns are responded to promptly ahead of the annual review.

We also recommend that any records relating to junket operators flagged by internal departments during the annual review are included on the summary form, along with further details on the results of these checks and their resolution.

Law enforcement requests? Or picked up in POI section?

Verify

B - the process for updating previous probity and background checks

The process for updating the probity and background checks of existing operators has been enhanced over the last few years to include additional checks around reconfirming the operator's criminal record and Australian visa status, however it still centres around updating the currency of information rather than establishing whether Crown still wishes to hold the relationship with the patron. As with new junket operators, the process focusses on the operator and does not consider their agents.

Annual review process

The process for updating previous probity and background checks on existing junket operators centres around the annual review. This is conducted by the Credit Team, and as outlined in Section A: *Information Inputs (Existing Junkets)*, for the most part involves conducting a repeat of searches and requesting updated documentation.

We were informed during our consultation that the process has evolved to include additional scrutiny of some of the documents provided, such as checking the ABN, DICJ license and conducting searches on licence holders in Maceau, including to verify the directors.

Additional enhancements introduced over the last couple of years include introducing the requirement to provide an updated police clearance, and conducting a VEVO check on junket operators. This allows Crown to understand the junket operator's current Australian visa status and conditions. Whilst these are positive steps, the review process remains focussed on updating the currency of information. Further strengthening of the program should reframe the process as a review of whether or not the relationship should continue and be based on all information available to Crown at that point as outlined in Section XX.

Additional probity measures

Alongside the annual review process, all junket operators are subject to daily screening via Dow Jones to ensure Crown is aware of any significant adverse information that enters into the public domain on a real-time basis.

To ensure the junket operator register remains current, Crown marks junket operators as inactive after three years without junket activity. Should an inactive junket wish to resume operations, they are required to re-apply and are treated as a new junket operator. The training document outlines that urgent re-approvals are considered, with the minimum threshold of due diligence checks being an ABN check, Executive approval, Non EGPA on file and a Dow Jones search, the rest may be completed as soon as practicable. In such instances the junket operator must accompany players.

© 2020 Deloitte Risk Advisory, Deloitte Touche Tohmatsu

Further details of ongoing probity measures are included in the diagram on page 23.

Junket agents

As with the initial junket approval process, the review of existing junkets does not involve due diligence being conducted on agents and representatives. Due to the higher risks posed by these groups, they should be considered as part of the process.

The annual review also provides an additional opportunity for Crown to conduct due diligence into those agents who have been most active with the junket over the previous year, without relying upon the operator to provide those details.

Recommendations

We recommend that the annual review process should seek to reconsider and test the decision as to whether Crown wishes to continue the relationship the patron, and be based on a more detailed summary of both the updated checks completed and a review of the internal information collected by Crown relating to the operator, rather than focussing on updating the currency of information held.

We further recommend the scope of the review incorporate junket agents and that they be subject to the same levels of repeat due diligence as the junket operators.

25

6 & 7 – decision recorded on summary and approved by Exec – documenting decision taken if Crown takes the risk – if adverse info received do they document why they still went ahead
Compliance and AML should be reviewing – before goes to Execs

Josh: We've got these large junkets, and a lot of small junkets. Instead of just relying on annual junket, we do need trigger points. If there's a ML request, we need to have trigger points which are embedded with people seeing them and recording them, understanding what's to be escalated to the committee. Instead of waiting for 12 monthly review process.

Basic recording that needs to be put in a front of a decision maker – decision maker will be reading that cover sheet – got to summarise up front what risks were looked for and what the outcome is – strengthening SOPs to include process maps, aligning definition to risk, aligning the way risk is assessed
Credit team are coming up with a risk assessment – risk rating in relation to junket operators, no where is it articulated what that risk rating is about – credit vs reputational risk
Bringing in risk buckets for POI – risk category areas to add consistency

Can't be looked at from a credit perspective

Start in the right direction – copying in AML and S&S as initial process – engaged in the process from the get go – shouldn't be a process where they're bought in at the end throughout application and due diligence

Intel network from S&S

Compliance are engaged – but we want them more engaged

Probity - codifying risks we worry about with junket operators and what we're assessing them against

Elevate role of credit – doesn't talk about adverse information – sanctions, PEP etc – even if not a hit demonstrate that they've done – add a finding is this person a PEP

Basic recording that needs to be put in a front of a decision maker – decision maker will be reading that cover sheet – got to summarise up front what risks were looked for and what the outcome is – strengthening SOPs to include process maps, aligning definition to risk, aligning the way risk is assessed

Credit team are coming up with a risk assessment – risk rating in relation to junket operators, no where is it articulated what that risk rating is about – credit vs reputational risk

Bringing in risk buckets for POI – risk category areas to add consistency

All JTOs are high risk from AML perspective, how do ratings of other forms of risk inter-relate to each other – these are all risk categories we should be rating as junket operator – they need to be separate findings from buckets of risk. Recommendation around re-structuring form around risk buckets.

All junket operators, junket players, premium players, as well as customers of Gold Tier and above are screened daily against Dow Jones Risk and Compliance and remain on the screening list, with any change to the customer's status alerted to Crown for assessment

DD profiles on active JTOs are reviewed annually

CDD on active JTOs who have not had a program but have had activity in the property

There is a further section highlighted yellow with a minimum threshold of docs required for 'urgent re-approvals' of inactive junkets, including ABN check, Exec approval, operator must accompany players, Non EGPA on file and Dow Jones search, the rest may be completed as soon as practicable.

Re-approval must be sought for cash junkets requesting credit.

> "Please note: The Junket Operator cannot commence operations or continue operations until the documents are received. Escalate requests to Manager if any documents are not received in a timely manner."

Copies of all searches are saved on the patron's file

Mary: Every year, we look at all documents, some expire some don't. Check ABN now as well, to see if that's still valid. Also look after Nonexclusive gaming agreement. Check DICJ license each year, also do searches as well on the licence holders in Macau. See who the directors are.

For trips, credit facility is looked at trip by trip. We look at documents required on a trip by trip basis, Dow Jones, personal checks. Review these at other intervals based on arrival.

We have refreshed all the C6, the rationale for that was the expense. When we tested that year to year, there was really no change between the first report and second. Between the first report and three or four years down the track. We've found in some changes there have been changes to these reports. So we may not do them annually, but maybe every second year

If moved to inactive (not had activity for 3 years), they must start the DD process again

Where concerns raised through law enforcement, Dow Jones, internal control programs, may be table through POI committee

Junket transaction monitoring program

C - the composition of the committee reviewing existing operators and the role for different aspects of the business

Murray – for review

At present, the review of existing junket operators is conducted by the Credit Team as part of their annual due diligence refresh. As with prospective junket operators, the AML and Compliance teams are not engaged throughout the process to inform decision making or the content of the summary file that is issued to the Executives for approval.

Composition of the committee reviewing existing operators

The Credit Team is responsible for compiling the file as part of the annual review of junket operators, which is then shared with VIP International, with Compliance and AML in copy, before being submitted to the Executive approval team made up of the CEO, CLO and COO.

This introduction of Executive approval is a positive step that will assist with elevating the exercise from reconfirming the accuracy of information towards re-evaluating the information held on file and deciding whether or not to continue the relationship based on the information presented.

At present however there is no articulation of what factors the committee should weigh in the decision to continue business, but primarily seems based on whether they have successfully updated their information and held visits to Crown premises as required.

The due diligence file should summarise up front what risks what risks were considered during the searches, and what the outcome was. We have provided details regarding our findings around Crown's definition of probity and risk appetite with relation to the junket program in the previous section of this report. These findings are also relevant to the program regarding existing junket operators.

Roles and responsibilities

The annual review process is currently managed by the Credit Team. As with the initial due diligence process, this results in the process being framed from a credit perspective, with the output not going into sufficient detail regarding potential adverse information, or AML red flags and typologies identified.

The process does not currently include engagement with AML, Security and Surveillance and Compliance on an ongoing basis to inform decision making within the annual review process. For approvals, it is initially shared with the VIP International General Manager and **Roland (Job Title)**, with AML and Compliance copied in.

We would suggest that the process could be strengthened through instituting a review to ensure that the file is scrutinised and the Credit recommendations are reviewed by a staff member with relevant training and expertise in AML and Compliance risks.

Recommendations

We would recommend that the AML and Compliance teams should hold a more central role in the due diligence program and review of existing junket operators, including through conducting a review prior to the file being escalated for approval. Any findings around potential red flags from an AML perspective should be included within the junket annual review summary document.

We have outlined our recommendations regarding risk appetite and defining probity within the previous section. These are also relevant for review of existing junket operators.

6 & 7 – decision recorded on summary and approved by Exec – documenting decision taken if Crown takes the risk – if adverse info received do they document why they still went ahead
Compliance and AML should be reviewing – before goes to Execs

Josh: We've got these large junkets, and a lot of small junkets. Instead of just relying on annual junket, we do need trigger points. If there's a ML request, we need to have trigger points which are embedded with people seeing them and recording them, understanding what's to be escalated to the committee. Instead of waiting for 12 monthly review process.

Basic recording that needs to be put in a front of a decision maker – decision maker will be reading that cover sheet – got to summarise up front what risks were looked for and what the outcome is – strengthening SOPs to include process maps, aligning definition to risk, aligning the way risk is assessed
Credit team are coming up with a risk assessment – risk rating in relation to junket operators, no where is it articulated what that risk rating is about – credit vs reputational risk
Bringing in risk buckets for POI – risk category areas to add consistency

Can't be looked at from a credit perspective

Start in the right direction – copying in AML and S&S as initial process – engaged in the process from the get go – shouldn't be a process where they're bought in at the end throughout application and due diligence

Intel network from S&S

Compliance are engaged – but we want them more engaged

Probity - codifying risks we worry about with junket operators and what we're assessing them against

Elevate role of credit – doesn't talk about adverse information – sanctions, PEP etc – even if not a hit demonstrate that they've done – add a finding is this person a PEP

Basic recording that needs to be put in a front of a decision maker – decision maker will be reading that cover sheet – got to summarise up front what risks were looked for and what the outcome is – strengthening SOPs to include process maps, aligning definition to risk, aligning the way risk is assessed

Credit team are coming up with a risk assessment – risk rating in relation to junket operators, no where is it articulated what that risk rating is about – credit vs reputational risk

Bringing in risk buckets for POI – risk category areas to add consistency

All JTOs are high risk from AML perspective, how do ratings of other forms of risk inter-relate to each other – these are all risk categories we should be rating as junket operator – they need to be separate findings from buckets of risk. Recommendation around re-structuring form around risk buckets.

Junket transaction monitoring program slide 29 190920

05 | Persons of Interest Process

DRAFT

Persons of Interest

Introduction and areas of focus

Murray – for
review

The Persons of Interest (POI) process has been developed to add more structure to the decision making process, having begun as a more informal review. The revised process involves the use of a Patron Decision Assessment (PDA) form, which provides structure through an in-built scoring system that supplies a risk rating of low, medium or high.

All assessments that receive the medium or high rating are recommended to be actioned through a POI Committee process, which either involves an email being sent to members of the committee, or a meeting being held in which the patron is discussed by all members present prior to a decision being made.

The process is a good example of Crown bringing differing perspectives and expertise together to ensure that the decisions are informed by a holistic review of risk. It is currently in its early stages, and we identified a number of areas where policy and process documentation could be strengthened to ensure consistent application.

An area highlighted as contentious during our review was around requests from law enforcement and how Crown can best manage reputational and other risk associated with continuing relationships where requests have been received. We have made recommendations for potential steps Crown can take to strengthen its process in this regard.

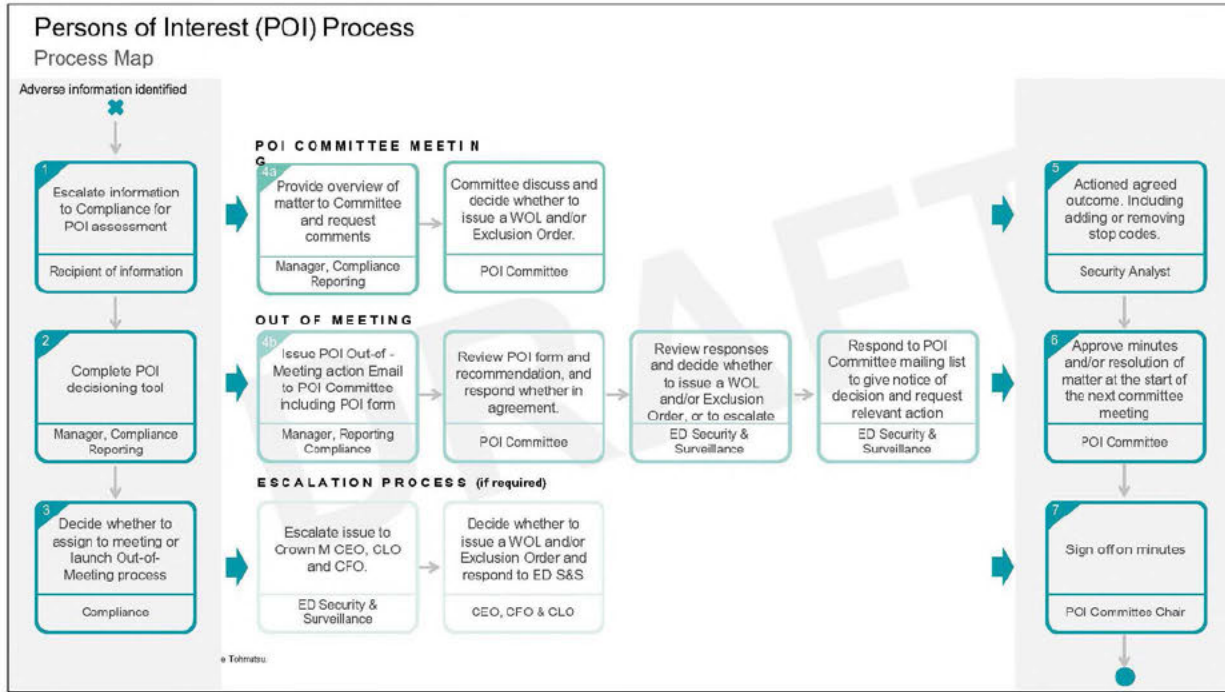
Our review examined the following areas in relation to Crown's processes regarding the Persons of Interest process: the information inputs considered in the POI process; and the process for reviewing and making decisions about persons of interest, including the role of different aspects of the business.

A – information inputs

- Information triggering the Person of Interest (POI) process
- Law enforcement requests
- Ongoing management of internal information

B – the process for reviewing and making decisions about persons of interest

- Information available to the persons of interest committee
- Process undertaken to weigh various factors in connection with a review of or decision about a person of interest
- Composition of the POI Committee
- Role for different aspects of the business



SMRs / hits on DOW Jones trigger POI process – what else triggers a POI process? Where is this documented? Should be articulated in the charter? What does this exist to do?

Risk scoring & tool – good step they may want to implement more broadly

POI – heading in right direction
Articulated direction from POI decisioning tool
Clear record of judgement of decision made

Key reasons for that decision should be documented

If they're making a decision – why
If they're making a decision to allow someone in the presence of adverse information

Positive it sits with compliance – holistic view – SMRs etc

Group participation –
Process for dealing with really sensitive stuff
Have it documented what is that process – how do those get dealt with with the community
Is it that if it's really senior it goes to a smaller level group – Exec Group will take decisions that others won't be privy to
Process can be communicated, but not details
Josh as CLO, Craig S&S, probably COO or CEO, Michelle – Compliance – smaller senior group who make that decision

Potentially someone like Anne could get reports without knowing detail

Flag on file – got to be entered into system to have that recorded – record created – somewhere they should have the rationale, but not held in open database – might be more central /close-hold

Look at make-up of committee – check it's balanced

Make sure it's adequately recorded around Craig having ownership

POI Tool

Would like to see assumptions that these are based on –

Crown weights conviction of offence as higher than someone who's never been charged
Decision making framework - this is how we come to those decisions, this is how they weight them
In our view, does this adequately represent the risks that Crown say they want to look at

Haven't articulated in any explicit fashion, what are the risks that Crown want to avoid with the POI process - what is this supposed to stop

Risk considerations - how is this articulated?

How well does this POI process reflect that decisioning list - and do we think that process is right?

They've weighted the different offences but not given assumptions as to why -

We will give appropriate regard as to the recency of allegations

Needs to be put in writing and entire executive need to be signed up to and agree on - does the committee sign up to this framework

Who's approved that framework

Is this something that group risk should be talking about - should it go to risk and audit committee - role for the risk committee - in at least determining the principles on which they are making these decisions

If you think about ARC's role in making sure risk is being managed appropriately

The principles that govern it, what they care about

Where's the shared agreement and articulation of this

What's the threshold for disagreement before it is escalated

A – Information Inputs (POI)

The information inputs that trigger the POI process are understood internally, however not yet captured within Crown's policy documentation which would assist in ensuring consistency and communicating the process externally. At present, the processes are not established to consistently manage law enforcement requests, which may pose significant reputational risk to Crown.

Murray – for review

Information triggering the Person of Interest (POI) process

According to Crown M's POI Charter, the role of the POI committee is to ensure that Crown M remains "free from criminal influence or exploitation, by reviewing persons of interest (POIs) who are brought to the attention of the Committee, for a variety of behaviours, be it at Crown or external to Crown, including but not limited to alleged matters relating to: drugs; money laundering; thefts; frauds; terrorism financing; assaults."

The charter does not document what different factors or sources of information may trigger the POI process however. During our consultation phase we were informed that this could include any of the following:

- A patron facing criminal charges;
- Law enforcement enquiries or requests;
- Adverse information in the media;
- Reports of untoward behaviour or barring from other casinos; or
- Red flags from transaction monitoring or criminal behaviour detected whilst at Crown.

Law enforcement requests

Responding to law enforcement requests poses a challenge for Crown, through striking a balance between the requirement to restrict information and protecting the organisation from reputational damage. This was discussed during our consultation phase, with staff explaining the particular challenges that arise due to Crown not being able to respond to media requests to confirm they are working with law enforcement when questioned regarding ongoing relationships with patrons.

Law enforcement requests either come through the Compliance department or Security and Surveillance. The Compliance Reporting Manager is responsible both for managing the POI process and for acting as the lead for law enforcement requests, therefore has a holistic overview of both processes. Requests that are made through Security and Surveillance are not always escalated through the POI process however, which may affect the completeness of Crown's records.

Ongoing management of internal information

Crown is taking initial steps to ensure the information inputs and outcomes of the POI process connect with its other internal systems. The AML customer risk rating, for example, includes the provision that any customer reviewed by the Crown M POI Committee becomes a 'high risk' on the risk rating scale.

Similarly, all patrons with whom Crown continues to do business following a POI Committee review become subject to increased scrutiny following the high risk rating. This increased monitoring may include daily screening via Dow Jones.

We asked staff responsible for the POI process whether it has the capability to take into account repeated flags being received for the same patron, such as multiple SMRs or law enforcement requests, however were informed that the data is not sufficiently sophisticated to do so at this stage. For example multiple law enforcement requests may be received regarding the same case, therefore would be inappropriate to trigger multiple POI processes. There may be little Crown can do to resolve this at this stage, depending on the nature of how these external requests are made.

Recommendations

Deloitte recommends that Crown documents the information sources and events that trigger the POI process, to ensure consistency of application and ensure the process for responding to such matters is documented.

We would also recommend that Crown look to streamline the POI process with law enforcement requests, to ensure that there is a complete record of information Crown holds regarding its patrons and ensure Crown's decisions to continuing a relationship with patrons remains defensible.

Moving forward as the process becomes more established, Crown may wish to explore how adverse information, such as SMRs or law enforcement requests are recorded to establish whether data driven solutions could assist with building up the intelligence picture and for consideration in the POI process.

the information inputs to be considered and sources to be mined in connection with reviewing and making decisions about persons of interest;

What triggers the POI process - this should be documented in the charter.

Michelle

We manage the POI committee which is quite an unusual process. Started as something off the cuff. It was never meant to be those things that people expect today.

That's largely where compliance intervenes.

It doesn't have to be a conviction; charge is enough for us to get that ball rolling. We do have some people who are charged and acquitted, committee considers removal of ban order.

If we see an article about someone in the paper. If it's associated with money laundering, drug trafficking, felony crime, we'll weigh in.

When we hear something's gone on untoward somewhere else, at another casino, we start doing checks internally. Check casino database.

Sometimes person involved in unacceptable behaviour is a front for someone else, they'll make those connections.

It's through the process of day to day business that adverse information comes up.

Staff members that do that - Sean Counihan - manages law enforcement and pulls POI together.

Anne

In the media, we can't go back and say we are working with law enforcement. We need to somewhere have something to say why did you stop working with those, because we were collaborating with law enforcement agencies.

Internally I'd say it would be up to Craig to say, whatever word we used, we don't need to say more. But at least we would know. I've put reason why on the form. At least we've documented it's something on our radar.

In that instance still go through POI process. If we have red flag that comes up, and tool tells us we need to think about, we shouldn't take exceptions out of that process. I think we need to take everyone to that committee - it's senior enough. If Craig says I'm overriding this, we need to know there's a good reason for it.

Nick wanted to say everything that's red we automatically exclude. I don't want people to jump through hoops, I want people to use that tool. Want everything to go through POI.

Law enforcement can ask us four times on the same case, and nothing comes up on it. Our data is not sophisticated - it's the same request over and over.

Same for SMRs. Not comfortable at this stage that reporting makes someone high risk, the kind of reporting is on threshold. In the past we would have reported a lot. Not a good source of data.

When you say keep an eye on it, what does that mean?

That increases the rating on our screening, so they are flagged up. When their name pings again, it increases the scrutiny. Junkets, VIP, PEPs have a timeline for run throughs, daily monitoring, in line with AML risk being higher level.

If something's been to a POI, allegation unconfirmed, say we'll monitor that more often. May mean daily DOW Jones.

AML customer risk rating: High - any customer reviewed by the Crown M POI committee (comprising representatives of Security, Legal & Regulatory, Gaming, Cage and Surveillance), any Foreign PEP or otherwise rated by AML team.

B – the process for reviewing and making decisions about persons of interest (1/2)

The POI process is a positive initiative to add a framework around decisions regarding persons of interest, which will increase consistency and ensure that Crown’s values and priorities are considered as part of the process. We recommend that the assumptions upon which the tool is designed are clearly articulated, and that the reliability of information sources are also considered. All decisions made through the POI process should be recorded with the rationale documented.

Information available to the persons of interest committee

The POI committee takes one of two forms: either through discussion during the meeting, or the out of meeting process in which the decision regarding the POI is made through email. The out of meeting process is used much more frequently, with meetings generally favoured for more controversial matters.

At POI meetings, the committee are provided with an overview of the matter and relevant information is provided including a Patron Decision Assessment (PDA) form. For the out-of-meeting process, the relevant information is shared via email, including the PDA form.

The PDA form includes the details of the person involved, the rationale for the request along with details of any allegations, including their status and source. The form also contains a risk assessment which factors in questions around the nature of the allegation, whether the individual has been charged, convicted or served their sentence, whether they may pose a threat to safety of Crown staff and patrons, as well as their relationship with and potential direct impact to Crown.

Once completed, the PDA provides an initial risk rating of low, medium or high. All patrons rated as medium or high risk go through the POI process. This is a positive measure in adding consistency, which allows the POI Committee to test out the scale and ratings from the PDA form with real life use cases as the process is in its infancy.

The exception to the rule with regards to information provided to the Committee is around law enforcement requests, as elaborated in the previous section: *Information inputs (POI)*. Further discussions are required within Crown to reach agreement on how POI Committee members are informed about sensitive cases that are exception to the POI process.

Process undertaken to weigh various factors in connection with a review of or decision about a person of interest

The purpose of the committee is to review information brought to it and decide whether the POI should be permitted to continue frequenting Crown, or whether they should have a withdrawal of licence (WOL) and/or Exclusion Order (EO).

To assist with the decision, the PDA tool provides an automatically generated numeric weighting to different responses provided, and their perceived risk level. The tool is therefore implicitly codifying Crown’s priorities and values. The assumptions upon which this is built however are not clearly stated, for example how we have not seen anywhere that the reasons which give rise to the various weightings are articulated. For consistency, the process would benefit from an articulation or guides around how this is reflected within the decision making process.

We were informed during our consultation that there does not tend to be much dialogue for out of office decisions, and rationales are not recorded. The meeting process involves an additional layer of discussion, and is therefore reserved for the more controversial matters. Considering the central role the tool therefore plays in determining Crown’s response, we would suggest the judgment around the weighting of different factors would benefit from approval at Audit and Risk Committee Level, given it is a fundamental decision around the level of risk that Crown is willing to accept.

Along with the completed tool and discussion, there should be a clear record of the judgement made, and the rationale should be documented. At present we were informed that the outcome is recorded, however providing a more substantive rationale and record of the discussion would assist with ensuring Crown’s decision is defensible.

Recommendations

Deloitte recommends that the assumptions upon which the Patron Decision Assessment tool is based are clearly articulated, including how the information is weighted.

We would further recommend that this include consideration of the reliability of information sources.

All decisions made through the POI process should be recorded, with the rationale behind each decision documented to ensure that Crown’s actions are defensible, particularly when Crown decides to continue a relationship with a patron about whom adverse information is held.

the information available to the persons of interest committee (and any other relevant body) in making decisions on particular persons of interest;

the process undertaken to weigh various factors in connection with a review of or decision about a person of interest, including review of:

- (A) any law enforcement requests in respect of the person of interest;
- (B) any suspicious matter reports issued in respect of activity connected to the person of interest;
- (C) any other information relevant to the person of interest available to Crown;

POI tool – would like to see the assumptions this is based on and weighting of decisions. Who should make this judgement? Potentially ARC given role in appropriately managing risk, with a shared agreement and articulation of this.

Records - there needs to be a clear record of the judgement made, and the reasons why should be documented.

Michelle

It’s far, far more out of meeting. The meetings get cancelled because by the time we get to meeting there’s nothing left. The reason we now go to meeting is if there’s some controversy.

History of adverse info, SYCO, findings from SIA, police records, sometimes ATO requests, child payment requests.

Best thing about it being by committee. S, 25 – one of things they love is that this is done by committee and not by a couple of senior managers. Everyone’s got a moral compass. The balance of everyone’s view. You won’t be surprised to find a few people have a louder voice. Normally advisors to business so voices carry extra weight, voice of lawyer would carry more weight than table games. Myself and Jan Williams are senior solicitors who attend these.

Craig Walsh is the ED of Security and Surveillance. He’s an ex-policeman, he’s on that plane. His experience and history give him a similar perspective.

With out of office ones, there’s not a great deal of dialogue with why people are making their decision, they just say supported – even if meetings, Sean will go through and we’ll just say supported and it’s recorded as outcome. For other ones, we debate for half an hour, and then tend to record just what the outcome was rather than rationale.

It seems that in recent times, with minutes being requested for regulators, people would say these minutes are insufficient. If people want us to put substantive information in, that’s something we could start doing, but this process was started to be with people, to be a good corporate citizen.

Interview with Josh:

decisioning tool for the POI process, one thing that’s really important is taking a risk-based approach to it. What is the reliability of information? Where did this come to us? You want to reflect that within decision making process and give some guides around how you rate that. Regulator will say you had all this info, what emphasis did you put on what. When we were looking at due diligence files, there were points when it said yeah there was this anonymous thing, but it doesn’t explain what process was followed, what weighting it was given etc. Need to include rationale around that so its defensible.

I've put reason why on the form. At least we've documented it's something on our radar.

In that instance still go through POI process. If we have red flag that comes up, and tool tells us we need to think about, we shouldn't take exceptions out of that process. I think we need to take everyone to that committee – it's senior enough. If Craig says I'm overriding this, we need to know there's a good reason for it.

Nick wanted to say everything that's red we automatically exclude. I don't want people to jump through hoops, I want people to use that tool. Want everything to go through POI.

Craig

Two levels of POI – POI stuff that happens on a daily basis.

We identify person who rented the room, they're blacklisted. We do that on regular basis, someone gets in a brawl, we see someone money lending, blacklisted. It's not practical to do that as we'd be meeting every day.

Wrong place to come if you don't want to be observed. [REDACTED] Bad call if you're coming here to get involved in criminal behaviour. Straight forward stuff comes to us. Got a matrix we use for consistency.

Can put hand on heart with section 25, I can say we have a process, we're consistent, this is the penalty that comes out of it. Gets a little bit tricky. Frankly our current POI Committee make-up is no way near senior enough. Uncomfortable sharing with all and sundry. Needs to be a tighter and more senior group. Over representation which can skew the voting. Gaming want everyone one. I take the opposite view; I want everyone out.

The trouble you've got with POI Committee, you don't have consistent representation in the committee. Pretty hard to get a consistent penalty basis. Underpinned by a matrix would be way to go. Think it needs to be reduced, made more senior and perhaps broader.

Anne

If nothing's done, no charges were ever laid, we can't be judge and jury.

Right now the tool says no decision at this stage and keep an eye on it.

In terms of decisioning tool, embedded within this scoring, is Crown's view on what matters:

I think so, which is why nature of conduct, stage they're at. First three or four questions multiply outcome, last question you add outcome.

What I've tried to do is mechanise what we were doing. This was a more bottom up approach. Filling in little box of risk categories and impact.

Out of meeting decisions are often straightforward agreements. Most of the time information is good enough we make a decision on it, but do exactly the same in a meeting.

Murray

Codifying assumptions and priorities into what we value, what we prioritise and structure to get into position.

It's a rational way of doing it – expressing these are Crown's priorities, these are things that matter.

B – the process for reviewing and making decisions about persons of interest (2/2)

Murray – for review

The membership of the POI Committee effectively brings in stakeholders from relevant internal departments to ensure that a holistic view of risk and internal perspectives is included within the decision making process. Crown may benefit from a more defined approach to Executive and Board escalation. It may also be appropriate to appoint a secondary committee that is restricted to senior leaders in the organisation for the management of particularly sensitive matters relating to law enforcement.

Composition of the POI Committee

The current composition of the POI Committee consists of one GM (or suitable delegate) from the following departments: Security & Surveillance, Table Games, Gaming Machines, Legal, Regulatory & Compliance, Responsible Gaming, Risk, Cage, AML. The Group General Manager of Regulatory and Compliance is the Chairperson, and the Manager of Compliance Reporting is the Executive Officer.

The POI Committee charter states that all members must have the skills and experience required to enable them to fulfil their duties and responsibilities as members of the committee.

We note it is a positive development to bring different aspects of the business together, which will provide a more holistic overview of the different risks associated with the decision and ensure that there is an aligned understanding around Crown's appetite in this regard. During our consultation however it was highlighted that the membership may not be sufficiently senior for those particularly sensitive matters, such as cases where Crown is liaising with law enforcement.

To ensure the information is sufficiently restricted in such cases, Crown could benefit from having a secondary group made up of smaller and more senior members, such as the Chief Legal Officer, Executive Director for Security and Surveillance, GM of Regulatory and Compliance and potentially the Chief Executive Officer and Chief Operating Officer. This would ensure that process was still being followed, and that decisions and rationale for such cases were still documented.

Role for different aspects of the business

It is positive that the responsibility for the day to day management and oversight of the group sits within Compliance, due to the oversight they hold of other related areas of business, including SMRs and law enforcement requests.

We were informed that the composition has evolved as the process grew, starting with Compliance and Gaming, before expanding to include other departments. The current list of departments represented is sufficient to introduce diverse perspectives to the discussion, and allow for a consideration of both the risk and commercial aspects associated with the decision. We were informed during our consultation that the voices that carry the most weight in discussion are those bringing expert perspectives, such as the legal view or that of Security and Surveillance.

The POI process includes the provision for escalation, with the CEO, COO and CLO being the next level for judgment on matters where the committee is in disagreement or cannot reach a decision. There is no clear or defined threshold however of the level of disagreement required to trigger escalation, which would ensure this was consistently applied.

In terms of the role of the Board, at present there is no standard POI report that is escalated. Matters would instead only be referred up on an ad-hoc basis, where there may be a significant risk posed for Crown.

Recommendations

We recommend that Crown considers establishing a secondary committee made up of senior stakeholders for management of sensitive cases involving law enforcement, to ensure that these are reviewed and documented appropriately whilst restricting knowledge to a need to know basis.

We also recommend that the policy documentation includes clear direction as to the threshold upon which decisions should be escalated for Executive Approval to ensure consistency. Crown may also wish to consider and document the principles around Board escalation thresholds.

the composition of the committee tasked with reviewing persons of interest;
the role for different aspects of the business, including the AML department, the compliance department, the credit department, the VIP International department, and other aspects of the business, in reviewing persons of interest; and

Escalation – where is the threshold for disagreement before it is escalated articulated?

Group participation – tension around current group membership for sensitive areas. Could have a smaller / more senior group for the really sensitive bits, who make decisions that others won't be privy to. CLO, S&S ED, COO/CEO and ED Compliance. Have the group mandate and process documented and somewhere secure to store decisions.

POI tool – step in the right direction. May wish to implement more broadly. Positive it sits with Compliance who have a holistic view.

Michelle

For 20 years, I've been Crown's evidence giver. That's something that me or someone in my team would go. I was in my 20s at the time, I've been doing it for about 20 years. I said to General Counsel at the time, I think we should look at some of these, I keep providing police this information, but unless they're arrested, they keep coming in.

Started with me and gaming department, purely because they dealt with these people. Then we called in Security and Surveillance as they deal with a lot of adverse information.

We now have a minimum base of departments that must be represented. What we did was put the information forward that we knew about this person. The bulk of them, if they're going to a meeting, they're probably not good for us, I'd say 90% of them get banned. Meeting was once a quarter back in early days, then once a month. We were getting some that were coming up and we needed to stop dealing with today. Started form, what we know about the person, what's adverse about them, what risk do they pose to the casino. Even if they don't present a risk to the casino per se we still don't want them. We fill that form out, email bombs to POI committee. We say respond with any feedback by X, but never get to that time. We will ban them pretty quickly in that space.

Matters that become a risk or could become a serious matter for Crown may go up. But isn't a POI report that goes to board.

POI tool – would like to see the assumptions this is based on and weighting of decisions. Who should make this judgement? Potentially ARC given role in appropriately managing risk, with a shared agreement and articulation of this.

06 | Board Involvement

DRAFT

Board Involvement

Detailed Findings

Murray

The Review is also to make recommendations for any improvements in governance or reporting frameworks for:

- (a) decision making in the process of assessing junket operator applications, the periodic junket operator review process, and the persons of interest committee process; and
- (b) reporting and referral to the Board and/or a Board subcommittee of decisions and/or any issues arising from such processes.

DRAFT

Board Involvement

Detailed Findings

Murray

Updating the current due diligence summary sheet

The Review is also to make recommendations for any improvements in governance or reporting

frameworks for:

- (a) decision making in the process of assessing junket operator applications, the periodic junket operator review process, and the persons of interest committee process; and
- (b) reporting and referral to the Board and/or a Board subcommittee of decisions and/or any issues arising from such processes.

Risk Management Strategy

Risk appetite and tolerances in relation relevant to the Junket program

| | | | |
|------------------------------|---|---|-----------------------------------|
| Regulatory/ legal | Maintain systematic compliance with regulatory, legal, statutory and contractual obligations | Significant breaches that may have a financial or reputational impact | Any event |
| | | Material legal action or class action | Any event |
| | Build and maintain professional and collaborative relationship with regulators and relevant government bodies | Significant breach or event that has the potential to damage the relationship | Any event |
| | Deliver gaming and alcohol services responsibly | Material RSG issues including adverse media | Any event |
| | | Integrity of liquor licences | Any loss of licence and/or points |

| | | | |
|-------------------------------|---|---|-----------|
| Brand / Reputation | Maintain shareholder confidence | Internal event creating a sustained share price loss | >5% |
| | Retain public confidence in the Crown brand | Sustained negative national or international media coverage | Any event |

Risk Management Strategy

Risk appetite and tolerances in relation relevant to the Junket program

| | | | | | |
|---|---|--------------------------|--|---|-----------|
| Brand / Reputation | Maintain shareholder confidence | Regulatory/ legal | Maintain systematic compliance with regulatory, legal, statutory and contractual obligations | Significant breaches that may have a financial or reputational impact | Any event |
| | | | Material legal action or class action | Any event | |
| | Build and maintain professional and collaborative relationship with regulators and relevant government bodies | | Significant breach or event that has the potential to damage the relationship | Any event | |
| | Deliver gaming and alcohol services responsibly | | Material RSG issues including adverse media | Any event | |
| | | | Integrity of liquor licences | Any loss of licence and/or points | |
| Retain public confidence in the Crown brand | Sustained negative national or international media coverage | Any event | | | |

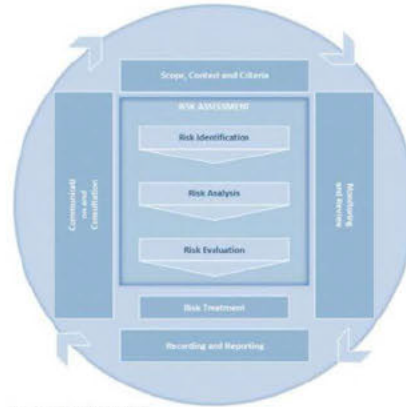
7.1. Risk Methodology

The risk management process is a systematic, recorded and regularly reviewed process. Crown follows the key principles and guidelines of *AS/NZS ISO 31000:2018 Risk Management – Principle and Guidelines* in identifying, assessing, evaluating, controlling and monitoring risk. This process is illustrated in the diagram below:

Overall junket programs is consistent with the requirements of ISO 31000:2018

Risk identification – they identify the higher risks associated with operators but not with the agents – needs to be corrected.

Risk analysis – need to include all relevant parties in the identification and evaluation of the risks associated with the particular operator relationship.



Source: AS/NZS ISO 31000:2018

These steps are the basis for any risk management activity at Crown and are outlined below.

07 | Appendix

DRAFT

Appendix A

Terms of Reference (1/2)

Matters to be reviewed

The Review is intended to make recommendations in relation to:

- a) Crown's **decision-making frameworks in respect of junket operators**, and the Crown policy settings which inform the decisions Crown makes in respect of junket operators;
- b) Crown's **decision-making frameworks in respect of persons of interest**, and the Crown policy settings which inform the decisions Crown makes in respect of those individuals;
- c) **how these frameworks and processes might be improved** to assist in the making of decisions reflecting Crown's risk appetite; and
- d) **the reporting to, and involvement of, Crown's board and board sub-committees** in relation to these matters.

New Junket Operators

- a) the **information inputs** to be considered and sources to be mined in connection with the assessment of a prospective operator;
- b) the **process for assessing an application made by a prospective operator**, including any consideration of any broader group of persons or entities with which the prospective operator might be associated;
- c) the **role for different aspects of the business**, including the AML department, the compliance department, the credit department, the VIP International department, and other aspects of the business, in the assessment process; and
- d) the **governance framework and responsibility for approving a new junket operator**, including whether the framework and processes are well designed to make decisions reflecting Crown's risk appetite.

Existing Junket Operators

- a) the **information inputs** to be considered and sources to be mined in connection with the annual review of existing operators;
- b) the **process for reviewing existing operators**, including, without limitation:
 - i. the **process for updating previous probity and background checks** on existing operators;
 - ii. the **process undertaken to weigh various factors** in connection with existing operators' activity over the prior year, including review, analysis, and consideration of:
 - A. any **law enforcement requests** in respect of the existing operator;
 - B. any **suspicious matter reports** in respect of activity connected to the existing operator;
 - C. any other information relevant to the existing operator available to Crown;
 - iii. the **composition of the committee reviewing existing operators**;
 - iv. the **role for different aspects of the business**, including the AML department, the compliance department, the credit department, the VIP International department, and other aspects of the business, in reviewing the background and probity of existing operators.
- c) the **governance framework and responsibility for the review of existing junket operators**, including whether the framework and processes are well designed to make decisions reflecting Crown's risk appetite.

Appendix A

Terms of Reference (2/2)

Persons of interest

- a) the **information inputs** to be considered and sources to be mined in connection with reviewing and making decisions about persons of interest;
- b) the **process for reviewing and making decisions about persons of interest**, including, without limitation:
 - the **information available** to the persons of interest committee (and any other relevant body) in making decisions on particular persons of interest;
 - the process undertaken to **weigh various factors** in connection with a review of or decision about a person of interest, including review of:
 - (A) any **law enforcement requests** in respect of the person of interest;
 - (B) any **suspicious matter reports** issued in respect of activity connected to the person of interest;
 - (C) any other information relevant to the person of interest available to Crown;
 - the **composition of the committee** tasked with reviewing persons of interest;
 - the role for **different aspects of the business**, including the AML department, the compliance department, the credit department, the VIP international department, and other aspects of the business, in reviewing persons of interest; and
- c) the governance framework and responsibility for reviewing and making decisions about persons of interest including whether the framework and processes are well designed to make decisions reflecting Crown's risk appetite (and whether it is desirable to more clearly articulate Crown's risk appetite).

Governance and reporting

The Review is also to make recommendations for any improvements in governance or reporting frameworks for:

- (a) **decision making** in the process of assessing junket operator applications, the periodic junket operator review process, and the persons of interest committee process; and
- (b) **reporting and referral to the Board** and/or a Board subcommittee of decisions and/or any issues arising from such processes.

Appendix B

Regulatory Landscape

Regulator expectations in Victoria, Western Australia and New South Wales

The respective regulatory bodies in Victoria, Western Australia and New South Wales do not provide specific guidance on what due diligence should be undertaken in relation to junket operators. Likewise current regulations do not proscribe any particular processes or procedures with respect to managing potential risks associated with junket operators, agents and players. However, they do specify that the Casino must establish an appropriate system of internal controls to appropriately mitigate the risks of operators and players.

Appropriate risk-based due diligence procedures are a key component of the internal controls that form part of Crown's compliance with regulatory requirements. As such, Crown's internal controls related to Junket Operations should be commensurate with the risks identified.

Queensland regulatory approach to Junket Operations

The *Queensland Casino Control Regulation (1999)* outlines the requirements for junket operations relating to casinos licenced in the state. Under the regulations, casinos enter into a junket agreement specific to each visit to the casino and strict requirements are outlined relating to reporting of all players and agents and provision of identifying information to the regulator.

Under the regulations, the casino must provide details of a new junket operator to the regulator prior to any activities occurring under the junket agreement for the purposes of allowing the regulator to 'assess the suitability' of the promoter.

At the current time Queensland is the only state in which the regulator takes on responsibility for approving junket operations.

Overseas regulator approaches to Junket Operator due diligence

The approach taken by the Casino Regulatory Authority (CRA) in Singapore represents the most conservative approach in the Asia-Pacific region. Applicants are required to provide comprehensive disclosures relating to ownership, financial position and reputation and track record. The CRA then engages a licenced investigations firm to verify all information including interviewing applicants and visiting the operations at other casinos outside of Singapore. As such responsibility for any due diligence is assumed by the regulator as part of the licencing process. At the time of writing, only two companies have been approved to operate junkets in Singapore.

Macau Gaming Inspection & Coordination Bureau

The Gaming Inspection & Coordination Bureau (DICJ) in Macau also requires detailed disclosure of information by the applicant, however we understand it has historically not undertaken steps to verify the information provided. Experienced gaming industry specialists in the Macau casino environment with knowledge of the DICJ have previously described the process as largely 'passive', with little investigation conducted by the DICJ to verify information supplied by applicants.

The DICJ have announced several planned changes to strengthen transparency and regulation of junket operators including higher capital requirements, publicising the details of shareholders senior employees and partners on the website of the DICJ and ensuring at least one shareholder that is a permanent resident of Macau. As of December 2019 the new legislation was yet to be introduced into the Macau legislative assembly.

The DICJ have continually increased scrutiny of junket licences as indicated by the reduction of licenced junket operators from a high of 235 in 2013 to just 95 licenced operators in 2020.

Appendix C

Industry Approaches

Industry approaches to Junket Operator due diligence

Our research identified information provided by Star Entertainment ("Star") as part of the 2016 review of its casino licence. The Star conducted a walk-through with the reviewer, J Horton, QC, who provided a summary of the process in his final report. While we have been unable to verify that the process operates as outlined in the course of normal business, several features of The Star's approach are worthy of note for later comparison with the procedures adopted by Crown.

While a detailed summary of the reported Star procedure is outlined in Annex 2, we note several features of their approach would support a robust due diligence process and aid in identifying a range of potential legal and reputational risks. First, the Star obtains a large amount of information from the Operator at the outset of the process. It collects identifying information for Operators, details of directors, shareholders and Agents. Operators are also required to provide disclosure of involvement in litigation, regulatory investigations, financial position and to provide consent for the Star to undertake and investigation into them. The benefit of this information is to provide a starting point for the due diligence process and aid the assessment of the transparency of the Operator.

Second, the Star conducts the risk assessment process independently of the assessment of creditworthiness. All Operators and their Agents undergo The Star's due diligence procedure prior to any commercial agreements being made. The Star applies the same level of due diligence to both the Agents who attend the casino and manage visits as it does to the Operators themselves.

Finally, The Star undertakes some basic research themselves but also utilises external consultants where required to undertake more complex due diligence investigations where required.

We are also aware of the approach taken by a large Macau-based Casino that undertakes very limited in-house research to determine basic identifying information for new Operators and then engages an external investigations company to conduct a due diligence investigation prior to any commercial discussions being undertaken. This approach is adopted across all Operator applications and is reviewed internally every 12 months and a new external investigator report conducted every two years.

<https://www.liquorandgaming.nsw.gov.au/documents/reports/casino/review-the-star-casino-licence-ilga-horton-qc-28-november-2016.pdf>

Appendix C

Industry Approaches

Industry approaches to Junket Operator due diligence

Our research identified information provided by Star Entertainment ("Star") as part of the 2016 review of its casino licence. The Star conducted a walk-through with the reviewer, J Horton, QC, who provided a summary of the process in his final report. While we have been unable to verify that the process operates as outlined in the course of normal business, several features of The Star's approach are worthy of note for later comparison with the procedures adopted by Crown.

While a detailed summary of the reported Star procedure is outlined in Annex 2, we note several features of their approach would support a robust due diligence process and aid in identifying a range of potential legal and reputational risks. First, the Star obtains a large amount of information from the Operator at the outset of the process. It collects identifying information for Operators, details of directors, shareholders and Agents. Operators are also required to provide disclosure of involvement in litigation, regulatory investigations, financial position and to provide consent for the Star to undertake and investigation into them. The benefit of this information is to provide a starting point for the due diligence process and aid the assessment of the transparency of the Operator.

Second, the Star conducts the risk assessment process independently of the assessment of creditworthiness. All Operators and their Agents undergo The Star's due diligence procedure prior to any commercial agreements being made. The Star applies the same level of due diligence to both the Agents who attend the casino and manage visits as it does to the Operators themselves.

Finally, The Star undertakes some basic research themselves but also utilises external consultants where required to undertake more complex due diligence investigations where required.

We are also aware of the approach taken by a large Macau-based Casino that undertakes very limited in-house research to determine basic identifying information for new Operators and then engages an external investigations company to conduct a due diligence investigation prior to any commercial discussions being undertaken. This approach is adopted across all Operator applications and is reviewed internally every 12 months and a new external investigator report conducted every two years.

<https://www.liquorandgaming.nsw.gov.au/documents/reports/casino/review-the-star-casino-licence-ilga-horton-qc-28-november-2016.pdf>

Appendix C

Industry Approaches

Star Entertainment's Junket Procedure

Our research identified information provided by Star Entertainment ("Star") as part of the 2016 review of its casino licence. Star provided the reviewer in this case with a 'walk-through' of its Junket onboarding process and the review provides some insight into the steps taken to conduct due diligence into Operators and Players prior to entering a relationship with them.

It is noted Star has no contractual involvement in the relationship between Operators and players, only signing an agreement with the Operator following completion of the due diligence process and following provisional authorisation being granted by the Gaming Manager.

The Star process for entering a new relationship and undertaking due diligence, as described in the report, is summarised below. At the outset, Star obtains several documents, disclosures and a 'consent to investigate' from the Operator. The value of this information is to provide a starting point for the due diligence investigation and a body of information to be verified against the available public records. In particular, information obtained from public record searches that had not been disclosed would serve as a clear red-flag for following up and may indicate dishonesty on the part of the Operator.

KYC Information collected at application:

1. Personal information including:
 - Police clearance certificate
 - Photo Identification
 - Certified copies of passport
2. Employment history
3. Business Associations
4. Junket operations with other casinos
5. Disclosure of involvement in litigation
6. Financial details
7. Character references
8. Notice of consent for The Star to conduct investigations into the Junket Operator
9. A release and indemnity

Appendix C

Industry Approaches

AML/CTF Checks and Internet Searches

The Star conducts AML/CTF Checks and undertakes additional internet searches in relation to the Operator to identify PEPs and other high-risk companies and individuals.

1. World-Check
2. Independent Internet Searches
3. Referral to external consultant

Information is reviewed by 'The Star's investigators' who may recommend further due diligence be undertaken, including by 'external consultants.'

Review and Provisional Approval

The Star holds a regular junket and player monitoring meeting to discuss information received in relation to proposed promoters, representatives or participants.

The Gaming Manager reviews all information collected and, if no information indicates the JO or their representatives are unsuitable, provides provisional approval. The operator then enters into discussions with the Star's international team to organise a junket and reach agreement with The Star in respect of the rebate, complimentary inclusions and the length of stay.

<https://www.liquorandgaming.nsw.gov.au/documents/reports/casino/review-the-star-casino-licence-ilga-horten-qc-28-november-2016.pdf>

Appendix D

Crown's Program and History of Enhancements

Have updated with table based on Josh's memo on s. 48. To delete this slide?

Development of the Due Diligence Process at Crown

Crown has undertaken an internal review of its policies and procedures designed to identify risks associated with Junket Operators with which it maintains relationships. We note that the policies and procedures underpinning the due diligence of Operators have evolved substantially since 2016, following an Audit conducted by the Victorian Commission for Gambling Regulation in 2011, and a Compliance Assessment by the Australian Transaction Reports and Analysis Centre ("AUSTRAC") dated 18 May 2018.

In 2003 Crown implemented *New Standard Operating Procedures* following the repeal of the Victorian Casino Control Act 1991 (CCA) and the Casino Control Regulations by the Victorian Government in consultation with the VCGLR. The key relevant provisions indicated that:

No approval or probity checking is required for a junket organiser or agent.

A Non-Exclusive Overseas Gaming Promotions Agreement must be signed by the junket organiser off shore before any junket activity can be undertaken at Crown

All junket organisers, agents and players under a junket arrangement are recorded in Crown's player database

All names in the Crown database are run against the WorldCheck database with a view to identifying any known terrorists as Crown is obligated not to knowingly deal with any recognised terrorists

The Crown player database is also run against the WorldCheck database for known criminals and Politically Exposed Persons to identify any potential risks

In December 2011 the Victorian Commission for Gambling and Liquor Regulation ("VCGLR") updated the Junkets & Premium Player Programs (Including Introduction of Players) Internal Control Statement (ICS). The key relevant provisions under the ICS indicated that:

ICS clause 2.2.1 (a) requires that a Junket Program Agreement be completed (and retained) prior to commencement of Junket Program Play documenting at a minimum Junket Operator (or Agent), Junket Program Type, Junket Program Player Names, Front Money, Commission payable to Junket Operator (where applicable), approval of terms and conditions by Junket Operator (or agent) and authorised Crown representatives and any subsequent changes to agreed terms and conditions.

Following this update, in June 2013 and October 2013, Crown undertook Internal Audits of internal processes and procedures for the initiation, monitoring and recording of Junket Program play which revealed that there were several discrepancies between Junket Program Agreements and Syco Records. Crown's management reinforced that all Junket Players named in the Junket Program Agreement are to be recorded in Syco in the form of full name, residential address and date of birth.

In 2016-2017 AUSTRAC undertook a casino junkets campaign to develop further understanding of how junkets work in Australia. AUSTRAC assessed Crown Melbourne's AML/CTF Program, ongoing -customer due diligence and reporting obligations.

AUSTRAC also separately conducted Compliance Assessment (in relation to Electronic Gaming Machine ("EGM") Operations between 1 July 2016 and 30 June 2017).

Appendix D

Crown's Program and History of Enhancements

AUSTRAC provided Crown Melbourne with ten (10) recommendations to assist it to strengthen its AML/CTF systems and controls. We note that AUSTRAC did not identify non-compliance by Crown Melbourne. AUSTRAC's recommendations broadly covered risk assessments and staff training relating to unusual or suspicious activity, the importance of automating transaction monitoring, and AML/CTF program policies and procedures.

Below we have outlined the relevant AUSTRAC recommendations that may impact the due diligence process of Operators and Premium Players below, noting that AUSTRAC's scope was limited to EGMs:

Recommendation 6 – Make records of investigations where no adverse findings were identified

Crown Melbourne currently records the findings of investigations of transaction monitoring alerts where suspicious customer activity is positively identified but does not make records of investigations where no adverse findings are identified. As such, Crown Melbourne may be unable to evidence whether an investigation took place or not. Making records of all investigation outcomes will enable Crown Melbourne to provide evidence of each investigation and its findings to auditors.

Recommendation 9 – Reference the requirement to verify customer's KYC information in the gaming payout procedures

Section 3032 - Processing an AUSTRAC Reportable Payout of the Gaming Machines Operations WPIs (Appendix B, Table 1, Item 43, page 149) states "the following information is required to be collected and retained: full name, date of birth, and residential address. The procedure does not instruct staff to verify the customer's full name and date of birth or residential address which is a requirement of the AML/CTF Act.

Beginning in November 2016 and until August 2017, Crown undertook an internal and ongoing review of all existing Operators and Premium Players. The following recommendations were identified in respect of Junket Program Activity, contained in a Risk & Assurance department memorandum dated 9 November 2016.

Internal Audit recommends a due diligence review of proposed Junket Operators to assess primarily, whether a Junket Operator is a valid Junket Operator. The review will also ensure that an appropriate audit trail in support of due diligence review be documented and retained in a central location and internal processes and procedures for the conduct of Junket Program activity updated to reflect checks undertaken.

Internal Audit recommends an additional column be included in the "Junket Operator and Agent" listing to indicate the date of VGCLR notification, and supporting documentation centrally retained.

Cash Transactions Reporting Manager (CTRM) advised that due to the significant amount of transactions reported in excess of \$50k, and following agreement with AUSTRAC, going forward Crown Melbourne is to review only patron losses in excess of \$50k and "report as required." Crown Melbourne will no longer report wins in excess of \$50k unless deemed to be a "reportable matter," at the discretion of the CTRM.

As part of the review, relevant Crown stakeholders formed a select committee to review five (5) junket profiles weekly in order to determine whether to proceed with the Junket relationship.

We understand that Crown applied three (3) key criteria when making a determination as to whether to proceed with the relationship.

Appendix D

Crown's Program and History of Enhancements

- The legitimacy of the Junket
- Whether the Junket Operator is a valid Junket Operator (versus a Premium Player)
- Whether the Junket Operator was involved in attracting Premium Players with which they had a business relationship (i.e. not personal associates)
- The Operator's domicile outside of Mainland China
- The probity of the Operator from a credit risk perspective

Following the review, Crown's executive management made the decision to terminate a large number of cash and credit Junket relationships.

In December 2017, the VCGLR took disciplinary action against Crown Melbourne. Crown was fined AUD 150,000 for failing, in thirteen (13) instances to adequately document junket arrangements. Following on from the disciplinary action, Crown has instructed its staff members to type out license numbers, and when not possible, to provide clear handwritten license numbers on Junket Agreements.

E – Overview of Junket Processes

C - M F14 ICS Junkets & Premium Player Programs Audit Report

G - Crown_2018_05_18_Compliance_Assessment_Report dated 18 May 2018.docx - A....pdf

C - M F15 Junket Processes - Audit Report - FINAL

Appendix D
Crown's Program and History of Enhancements

Updated – based on
Josh's memo

Development of the Due Diligence Process at Crown

| Control | Purpose | Enhancement |
|---|-------------------------------------|--|
| Police check obtained where operator does not have a DICJ license | Additional due diligence | Check was introduced in 2018, and carried out for all relevant jurisdictions from 2019 |
| Copies of other casino licenses requested if available | Additional due diligence | Control introduced in 2018 |
| VEVO check of Australian visa status | Currency | This control was introduced in 2020 |
| Junket profile | Summary document of key information | This document has evolved from 2018, with revisions also made in 2019 and 2020. |

Junket annual review process

| Control | Purpose | Enhancement |
|---|--|---|
| Copies of utility bill, bank statement or other proof of address | To determine residence for credit purposes | Exemptions could apply in 2017 / 18, however is required in all instances from 2019 |
| Copy of personal cheque | For credit purposes | Exemptions could apply in 2017 / 18, however is required in all instances from 2019 |
| Police check obtained where operator does not have a DICJ license | Additional due diligence | This check was required from 2019 for all relevant countries. |
| VEVO check of Australian visa status | Currency | This control was introduced in 2020 |
| Global Data check | Source of wealth | This was conducted on a case by case basis from 2018, becoming a requirement in 2020 |
| Wealth X & C6 checks | Source of wealth | This became a requirement in 2018, if a change was detected by Global Data or the online platform |
| Junket profile | Summary document of key information | This document has evolved from 2018, with revisions also made in 2019 and 2020 |
| Executive approval required | | Previously only where adverse or material changes were identified, in 2020 this was required in all cases |

Appendix E

Information Sources Used During the Junket Due Diligence Process

Murray – for
review

GlobalData

GlobalData is a data analytics and consulting company that delivers market and industry intelligence, servicing companies primarily across the consumer, retail, technology, healthcare and financial services sectors. GlobalData proprietary database is its Intelligence Center platform, which delivers its services through an online interface that combines search, browse and alert functionality.

Crown orders a GlobalData dossier on individual Operators which extracts information from the GlobalData Intelligence Center. The dossier outlines Operators' estimated net worth, employment history, wealth/asset ownership details, relationship groups and contact information.

Our experience with GlobalData is that the Intelligence Center consists of verified information which is ascertained from primary and secondary sources and is updated by analysts who both conduct research and make direct inquiries to confirm this information. Importantly, GlobalData does not offer what they call verticals into the gaming and casino's sector, therefore limiting insights into this industry.

Wealth X

Wealth-X specialises in data and insights on the world's wealthiest individuals to help organisations to effectively understand and engage them. Crown orders a Wealth-X dossier which outlines an Operator's biography, career history and wealth analysis.

Wealth-X does not capture all Operators, given that the database contains high net worth and ultra-high net worth individuals (over USD 30 million net worth). There are also inherent limitations in the platform due to the English-language capabilities.

Wealth-X among other third-party information platforms appear to simply scrape and collate data from information that is often made available/carefully curated by representatives of the individuals in question.

We recommend Crown continue using Wealth-X but supplement this information with open-source information such as Factiva, online research, property and litigation checks based on an Operator's footprint.

Acuris

C6 Data and Intelligence identifies risks associated with entities and individuals in the context of enhanced due diligence, adverse media, sanctions, PEPs and global ID verification. Acuris provides this offering by way of a customised report. Acuris also has a unique proprietary database called KYC6 which is claimed to contain over four million profiles collated over 15 years from public sources which are manually updated by its research team.

Crown obtains a C6 report into an Operator at the commencement of a new relationship. We understand that due to costs involved in requesting this report, it is not used for periodic re-validation. We also understand that C6 offer varying levels of reports covering basic or in-depth due diligence checks. The Express Report is a basic check which provides insufficient information around an Operator, particularly in identifying adverse media reporting and classifying reputational risks.

Previous experience of the reviewer with the platform noted the KYC6 product differs to other information providers because the research team is involved in collating and verifying the information displayed on the profiles, rather than relying on automated software that trawls public sources for information. Acuris claims that the database is manually updated with new adverse media records on a frequent basis.

We recommend that Crown order only the Executive level report from C6, while supplementing this report with in-house adverse media checks through Factiva and online research.



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 286,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People's Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam, in each of which operations are conducted by separate and independent legal entities.

Deloitte Australia

In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at <https://www2.deloitte.com/au/en.html>.

Liability limited by a scheme approved under Professional Standards Legislation.
Member of Deloitte Asia Pacific Limited and the Deloitte Network.

©2020 Deloitte Risk Advisory, Deloitte Touche Tohmatsu