

FILE #: \_\_\_\_\_



### CONTROL SYSTEM SUBMISSION

This is Schedule "I" to the  
Kahnawá:ke Gaming Commission Regulations concerning Interactive Gaming

**Applicant Information:**

Name of Applicant (Company name as it would appear on CPA): \_\_\_\_\_

Name of Person making the Application: \_\_\_\_\_

Date of Application: \_\_\_\_\_

Address: \_\_\_\_\_

Contact Info:

Business Tel: \_\_\_\_\_

2<sup>nd</sup> Business Tel: \_\_\_\_\_

Cellular: \_\_\_\_\_

Fax: \_\_\_\_\_

Email: \_\_\_\_\_

2<sup>nd</sup> email: \_\_\_\_\_

**Additional Information:**

Applicant Status:     New Operator     Existing Operator

Name of Primary Software Provider: \_\_\_\_\_ Contact Person: \_\_\_\_\_

Address of Software Provider: \_\_\_\_\_

Type of Games to be offered:     Casino Games \_\_\_\_\_     Sports Book \_\_\_\_\_  
(With corresponding software     Poker \_\_\_\_\_     Horse Racing \_\_\_\_\_  
provider if different from above)     Bingo \_\_\_\_\_     Other (please specify) \_\_\_\_\_

Gaming Brand Name(s) - as they would appear on the gaming website(s):


List of gaming URL's:


Projected Start or "Go Live" Date: \_\_\_\_\_

**All information provided to the Commission will be held in the strictest confidence and will not be used by the Commission for any purpose other than matters pertaining to this application nor will the information be provided, in whole or in part, to any other party without the Applicant's express written permission.**

## 1. Authority

This Schedule "I" is issued pursuant to section 35(g) of the *Regulations concerning Interactive Gaming*.

## 2. Currency

This schedule is subject to change from time-to-time and without notice. It is the responsibility of the reader to ensure the current version is in use. This copy is version 0.02.001, dated 5 May, 2010.

## 3. Audience

This document is for persons making application to the Kahnawake Gaming Commission for a Client Provider Authorization ("CPA") which, if granted, will entitle the Applicant to operate an interactive gaming system within and from the Mohawk Territory of Kahnawake.

## 4. Purpose

This document provides a template to enable Applicants to make a structured submission to the Kahnawake Gaming Commission. The format of that submission is intended to enable thorough understanding and timely consideration by the Commission.

## 5. Scope

This submission relates to all aspects of the system of controls for the conduct of interactive gaming by an Authorized Client Provider ("ACP") - if such authority is granted - that includes, but is not limited to, information about the following:

- Internal controls and systems mitigating Anti-Money Laundering risk;
- Player protection mechanisms including the system functionality, communications and operating procedures;
- Systems and controls governing player deposits and withdrawals to their gaming accounts;
- Player access to and functionality of complaint and dispute mediation channels;
- System functionality and controls over player gaming records and the allocation of prizes and winnings;
- Responsible gaming mechanisms including the system functionality, communications and internal operating procedures;
- Accounting functions including system functionality and operational competence to produce reliable financial reports; and
- IT security systems governing organisational and player information.

## 6. Objective of control systems

The objective of the control system submission is to measure the ability of the Applicant's internal controls, system functionality, operating procedures and human resource management to comply with the objectives of the Kahnawake Gaming Commission, as provided in the Regulations concerning Interactive Gaming.

## 7. Format of submission

The Applicant shall respond to all items cited in this document. From Section 9 Anti-Money Laundering respondents shall place an "X" in the appropriate column. Applicants may provide an affirmative response to items to which they will comply with as at the date of offering interactive gaming to the public on a Kahnawá:ke Gaming Commission permit. Where a "No" answer is indicated, the Applicant may provide further detail such as mitigating controls or projected implementation dates under section 167 – "Additional Information".

Applicants should note that this response forms the basis of a statement-of-claims. On authority of regulation 42 of the Regulations concerning Interactive Gaming, the Approved Agent will audit the submission as part of the Continuous Compliance Program within six (6) months of the Applicant offering interactive gaming to the public under a CPA issued by the Kahnawake Gaming Commission.

The Commission may consider false or misleading responses are a reflection of the character of the Applicant and consider this in determining if the respondent is suitable to operate, or continue to operate an interactive gaming system within or from the Mohawk Territory of Kahnawake.

All responses shall be in writing and provided in electronic format.

## 8. Accounting systems, procedures and chart of accounts

### **Chart of accounts**

A full chart of accounts should be provided for the licensee's operations as a supplement to this submission.

### **Management accounts**

The internal management accounts shall be produced in accordance with the internal accounting policies and made available to the Commission on request.

**ANTI-MONEY LAUNDERING**

<b>Policy and Implementation</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
9. Has the Applicant developed and implemented a policy for the prevention of money laundering and the anticipation of suspicious activities potentially connected to money laundering?	Internal Controls		
10. Is the anti-money laundering policy formally documented and approved by management?	Policy Document		
11. Has the Applicant implemented internal controls, processes and procedures to support the anti-money laundering policy?	Internal Controls		
12. Has the Applicant appointed an official Money Laundering Reporting Officer ("MLRO") for ensuring the effective operation of the anti-money laundering policy and internal controls?	Human Resources		
13. Is positive identity verification requested from unverified players upon either a deposit or withdrawal, that exceeds \$10,000.00 (whether in a single transaction or series of linked transactions) or where there is reason to suspect money laundering or terrorist activity?	Internal Controls		

<b>Reporting</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
14. Does the anti-money laundering policy document provide for the monitoring, identification and escalation of transactions potentially associated with money laundering?	Policy Document		
15. Do employment contracts include provisions for the prevention of tipping-off of suspicious persons or identified offenders that are under investigation for money laundering?	Human Resources		
16. Has reporting functionality been developed within the back-office application or through data extracts from the database to produce reports on: 16.1 All transactions (single or cumulative) per individual exceeding \$10,000.00 within a 24 hour period; and 16.2 All suspicious transactions (single or cumulative) exceeding \$5,000.00 by a connected group of people?	System Functionality		
17. Are the following transactions retained for a minimum period of five years: 17.1 All transactions (single or cumulative) per individual exceeding \$10,000.00 within a 24 hour period; and 17.2 All suspicious transactions (single or cumulative) exceeding \$5,000.00 by a connected group of people?	System Functionality		
18. Is a legal disclaimer displayed on all of the Applicant's websites stating that any criminal or suspicious activities may be reported?	Website		

<b>Financial Action Task Force</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
19. Does the formal anti-money laundering policy document provide for the FATF requirements including: 19.1 "Tipping off"; 19.2 The retention of verification documents; 19.3 The identification, escalation and reporting of suspicious transactions; and 19.4 Anti-money laundering responsibilities between the Applicant and third party service providers)?	Policy Document		

**PLAYER PROTECTION**

<b>Minimum Age Requirements</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
20. Is a formal documented policy regarding underage play implemented?	Policy Document		
21. Do the homepages of all the Applicant's websites display a "no under 18's" sign, which hyperlinks through to a clear message regarding underage play?	Website		
22. Does the player registration process include: 22.1 A clear message regarding underage play; and 22.2 A requirement for registrants to capture their date of birth?	Website		
23. Do the terms and conditions on all of the Applicant's websites contain a clause prohibiting underage play?	Website		
24. Do the responsible gaming pages on all of the Applicant's websites contain an active link to a recognised filtering programme?	Website		

<b>Prevention of Underage Play</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
25. Are internal controls in place for the identification and prevention of underage play?	Internal Controls		
26. Are automated controls implemented within the registration process, for all of the Applicant's websites, to prevent underage players from successfully registering a player account?	System Functionality		
27. Does the back-office application have functionality to flag player accounts that have been locked due to underage play?	System Functionality		
28. Are automated or manual controls in place to identify and lock multiple or linked accounts of identified underage players?	System Functionality		
29. Does the Applicant have a formal documented process for age and player verification, including the instances where verification of players is required?	Policy Document		

<b>Treatment of Underage Players' Funds</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
30. Does the Applicant have a formal documented process for the treatment of deposits and winnings of players that are subsequently identified as underage?	Policy Document		
31. Does the formal documented process state that all (non-disputed) deposits received from underage players will be refunded to the player or funding source?	Policy Document		
32. Do the terms and conditions on all of the Applicant's websites indicate that players identified as underage will forfeit their accrued winnings?	Website		

Schedule "I" Control Systems Submission

Inappropriate Names	Control Area	Yes	No
33. Has the Applicant implemented a policy and related internal controls to prevent the use of obscene, indecent or offensive names by players?	Internal Controls		

Player Registration	Control Area	Yes	No
34. Does the player registration process ensure that the following details are required to be captured by players prior to successful registration: 34.1 Full names; 34.2 Residential address; 34.3 Age or date of birth; 34.4 Contact details; 34.5 A password to access the registered account; and 34.6 Positive confirmation of acceptance of a legally enforceable contract defining the terms and conditions of play?	System Functionality		
35. Are internal controls in place to ensure that changes to the terms and conditions on all of the Applicant's websites are appropriately approved prior to deployment?	Internal Controls		
36. Do the terms and conditions on all of the Applicant's websites include the date and time of the latest revision?	Website		
37. Does the Applicant restrict all players from registering more than one account on each of the Applicant's websites?	Internal Controls		
38. Do the terms and conditions on all of the Applicant's websites indicate that players are permitted to register no more than one account?	Website		
39. Are automated controls in place for the identification of players that attempt to register multiple accounts?	System Functionality		
40. Are automated controls in place for the identification of players that have successfully registered multiple accounts?	System Functionality		
41. Is the back-office application able to generate exception reports on player accounts that contain duplicate or similar player information?	System Functionality		
42. Where multiple accounts that have been successfully registered by a single player are identified by the Applicant, are these player accounts locked in a timely manner?	Internal Controls		

Schedule "I" Control Systems Submission

<b>Player Accounts</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
43. Does the website or gaming software provide players with integrated functionality to perform the following activities online: <ul style="list-style-type: none"> <li>43.1 To create a unique username and password to access the player account;</li> <li>43.2 To change the player account password;</li> <li>43.3 To view the player account balance and the financial transactions that have resulted in movements to the player's account balance;</li> <li>43.4 To access the funds in the player's account for purposes of participating and wagering in a game offered by the Applicant; and</li> <li>43.5 To withdraw all or part of the account balance (in accordance with the terms and conditions on the Applicant's website); and</li> <li>43.6 To close the player account?</li> </ul>	System Functionality		

<b>Adequate Player Funds</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
44. Does the Applicant restrict player participation in gaming activity and real game play until player funds that have been deposited have cleared to the Applicant's holding account?	Internal Controls		

<b>Rules of Play</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
45. Does the Applicant have access to directly affect changes to the game rules?	System Functionality		
46. Are game rules made available to players within the gaming software or on the websites of the Applicant?	System Functionality		
47. If a sports book product is offered by the Applicant, are sports betting rules made available to players within the gaming software or on the Applicant's websites?	System Functionality		
48. Where game rules are provided on the Applicant's website/s, do management control and authorise all changes to game rules that are deployed to the website?	Internal Controls		
49. Are all game rules that are provided for players to view, made available in the English language?	Website		
50. Do all of the Applicant's websites that offer foreign languages provide the game rules to players in the relevant foreign language?	Website		

<b>Gaming Fairness</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
51. Has an approved agent performed a statistical analysis of the RNG and game outputs?	Internal Controls		
52. Has an approved agent examined the RNG, scaling and mapping components to assess whether they operate in accordance with the rules of the virtual game or event? This review shall include a source code review of the RNG and scaling and mapping components for malicious/incorrect code where considered appropriate by the Commission.	Internal Controls		

Schedule "I" Control Systems Submission

<b>Compliance with Rules of Play</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
53. In respect of the poker games offered by the Applicant: 53.1 Have preventative and detective controls been implemented to mitigate the risk of player collusion? 53.2 Are collusion detection controls automated? 53.3 Does collusion detection include monitoring of suspicious game play? 53.4 Have controls been implemented to prevent and detect players using poker bots?	Internal Controls		
54. In respect of the sports betting games offered by the Applicant 54.1 Are internal controls or mechanisms in place to prevent individuals with material insider knowledge from participating in betting activities? 54.2 Does the Applicant monitor the betting activities of individuals known to have material influence on the outcome of results (e.g. players, referees, coaches)?	Internal Controls		

<b>Remittance of Funds</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
55. Does the Applicant have a formal documented policy on the processing of player deposits and player withdrawals?	Policy Document		
56. Does the formal documented policy require that uncontested player withdrawals must be processed within five (5) working days?	Policy Document		

<b>Segregation of Accounts</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
57. Are players' funds held in separate and dedicated bank accounts that are isolated from the Applicant's operating funds?	Internal Controls		
58. Are all player funds held in accounts with accredited financial institutions?	Internal Controls		
59. Are player balances disclosed as a separate liability on the Applicant's financial accounts?	Internal Controls		

<b>Payment Methods</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
60. Does the Applicant prohibit non-electronic forms of funding for all player accounts (such as acceptance of physical cash)?	Internal Controls		

<b>No Credit</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
61. Does the Applicant expressly prohibit the provision of credit by the Applicant to any player?	Internal Controls		

<b>No Recourse to Player Funds</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
62. Does the back-office application restrict access, to the processing of manual adjustments on player accounts, to authorized employees only?	System Functionality		
63. Does the back-office application maintain an audit log of all manual and bulk adjustments to player balances?	System Functionality		

Schedule "I" Control Systems Submission

<b>No Recourse to Player Funds</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
64. Does the back-office application functionality include a management report on all negative adjustments to player balances?	System Functionality		
65. Does the Applicant maintain a formal process to review and approve negative manual and bulk adjustments on player accounts (including adjustments relating to the purging of player funds)?	Internal Controls		
66. Are manual adjustment reports prepared and authorized on a regular basis and are these retained?	Internal Controls		

<b>Dormant Player Accounts</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
67. Does the Applicant have a formal documented policy (the 'Dormant Player Account Policy') that includes: 67.1 The definition of a dormant player account; 67.2 The process to be followed on protecting player funds in dormant accounts and the clearing thereof; 67.3 The policy on remitting player balances remaining in dormant accounts to players; 67.4 The policy on purging player balances remaining in dormant accounts, to the Applicant or the Commission; 67.5 Player notification requirements and grace periods prior to purging; and 67.6 The refunding of purged funds from dormant accounts to players upon their request?	Policy Document		
68. Do the terms and conditions on all of the Applicant's websites clearly communicate the provisions of the 'Dormant Player Account Policy', including the inactivity period and consequences to player balances on such accounts?	Website		
69. Does the back-office application have the functionality to record and retain complete and accurate records of transactions affecting dormant player account balances?	System Functionality		

<b>Confidentiality of Player Information</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
70. Do all employment contracts and relevant third party service provider contracts include an appropriate confidentiality clause, preventing the signatories from disclosing player information?	Human Resources		
71. Do the back-office application/s and relevant databases have the capability to securely store credit card details and other sensitive player information?	System Functionality		
72. Is access to view credit card details and other sensitive player information restricted to authorized users only (at an application and database level)?	System Functionality		
73. Is sensitive player information stored in an encrypted format at database level?	System Functionality		
74. Is administrator access to view credit card details and other sensitive player information in the back-office application controlled?	System Functionality		
75. Does the system maintain an audit log of restricted and sensitive player information that has been viewed by system users?	System Functionality		

Schedule "I" Control Systems Submission

<b>Authorisation for Disclosure of Information</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
76. Has the Applicant implemented a privacy policy that permits the disclosure of player information only where: 76.1 Reasonably necessary for the conduct of authorized games; or 76.2 Required for the administration or enforcement of law or regulations.	Policy Document		
77. Is the Applicant's privacy policy made available to players on the all of the Applicant's websites?	Website		

<b>Interrupted Games</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
78. Does the system allow players to complete interrupted games?	System Functionality		
79. Does the system retain the results of the gaming activity that have not been transmitted to players due to connectivity interruptions?	System Functionality		
80. Does the system allow players to view non-retrieved gaming and financial information resulting from system interruptions?	System Functionality		
81. Are players provided, upon request, with non-retrieved gaming and financial information resulting from system interruptions?	System Functionality		
82. Do the website terms and conditions and/or gaming software communicate: 82.1 The procedures to be followed by players for information recovery and game continuity; and 82.2 The relevant terms and conditions applicable to game play that is affected by system interruptions or loss of connectivity?	Website		
83. Do the terms and conditions and game recovery procedures on all of the Applicant's websites or download gaming software appropriately address system interruptions relating to single player gaming activities (e.g. casino) and multiplayer gaming activities (e.g. poker)?	Website		

**COMPLAINTS AND DISPUTE RESOLUTION**

<b>Process</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
84. Has the Applicant developed and implemented a formal documented process over player complaints and disputes that provides for: 84.1 Receiving and addressing player complaints; 84.2 An appropriate dispute resolution process; and 84.3 Escalating player complaints?	Policy Document		
85. Does the Applicant communicate the mechanisms in place for players to lodge a complaint?	Website		
86. Do all of the Applicant's websites communicate the complaint and dispute mediation alternatives offered to players?	Website		
87. Are the Customer Support personnel appropriately trained on the process for handling player complaints and disputes?	Human Resources		

<b>Records</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
----------------	---------------------	------------	-----------

Schedule "I" Control Systems Submission

<b>Records</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
88. Does the system retain player complaint and dispute records and the associated correspondence in a manner that will allow for a detailed response, to enquiries by the Commission, in a timely manner?	System Functionality		
89. Are all player complaints and disputes recorded and retained in a centralised storage facility?	System Functionality		

**PRIZES**

<b>Crediting Prize Amount</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
90. Are player's account balances updated automatically and immediately subsequent to a player winning a monetary prize from gaming activity?	System Functionality		
91. Where prizes are withheld by the Applicant, are players provided with written notice and the reasons thereof?	Internal Controls		

**RESPONSIBLE GAMING**

<b>Limits</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
92. Do the Applicant's websites and/or gaming software provide players with the functionality to set individual deposit limits, and/or gaming limits, on a daily, weekly and monthly basis?	System Functionality		
93. Do all of the Applicant's websites clearly communicate the facility of limiting deposit and gaming activity to players?	Website		
94. Does the system automatically prevent the players from exceeding preset deposit or gaming limits?	System Functionality		
95. Are internal controls and procedures in place to allow players to request increases and decreases to deposit or gaming limits by contacting Customer Support?	System Functionality		

<b>Exclusion Options</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
96. Does the system provide a facility for players to set their deposit or gaming limits to zero?	System Functionality		
97. Is the processing of player requests for zero deposit or gaming limits processed automatically and made effective immediately?	System Functionality		

<b>Problem Gambling Self Exclusion</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
98. Does the system allow players to elect a zero limit or close the player account due to problem gambling?	System Functionality		
99. Does the website clearly communicate the facility of setting a zero limit or closing the player account due to problem gambling?	Website		
100. Do internal controls exist to prevent players, that have elected a zero limit or have requested closure their account due to problem gambling, from increasing the limit or reopening the closed account for a minimum period of six (6) months?	System Functionality		

Schedule "I" Control Systems Submission

<b>Problem Gambling Self Exclusion</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
101. Once a player has requested a zero limit or account closure due to problem gambling, does the Applicant take reasonable steps to ensure that the player does not receive any promotional materials during the elected exclusion period?	System Functionality		

<b>Temporary Exclusion</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
102. Does the system allow players to elect a zero limit for temporary cooling off reasons?	System Functionality		
103. Does the website clearly communicate the option for players to set a zero limit to temporarily cool off?	Website		
104. Do the Applicant's internal controls restrict a reversal or increase of a zero limit, elected by a player to temporarily cool off, to written confirmation (or equivalent) from the player?	Internal Controls		

<b>Warning, Advice and Mechanisms</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
105. Does the Applicant provide training to appropriate employees on the issues of problem gambling?	Human Resources		
106. Does the homepage of the Applicant's website contain a clear link to a player protection and responsible gaming page that includes: 106.1 A warning that gaming could be harmful if not controlled and kept in moderation; 106.2 Advice on responsible gaming and a link to sources of help on problem gambling, including helpline numbers; 106.3 An accepted and simple self-assessment process to determine risk potential; 106.4 A list of player protection measures (deposit or gaming limits including zero limits for self-exclusion and temporary cooling off) that are available on the site, and access to these measures; and 106.5 Details of the Applicant's responsible gaming policy?	Website		

**RECORDS AND REPORTING**

<b>Gaming Records</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
107. Will the Applicant store the gaming records in a facility within the Kahnawake Territory?	Other		
108. Will the Applicant store the gaming records at the "approved place" as agreed with the Commission within the Territory?	Other		

<b>Retention of Gaming Records</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
109. Do the Applicant's systems have adequate mechanisms and available storage to retain all player financial transactions for a minimum period of 5 years?	System Functionality		

Schedule "I" Control Systems Submission

110. Where the Applicant's systems do not have available storage to retain all player financial transactions for a minimum period of 5 years, are these transactions accessible in archived or backed up storage facilities?	Internal Control		
--	------------------	--	--

<b>Retention of Player Verification Documents</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
111. Do the Applicant's systems have adequate mechanisms and available storage to retain all player verification documents for a minimum period of 5 years?	System Functionality		
112. Where the Applicant's systems do not have available storage to retain all player verification documents for a minimum period of 5 years, will these documents be accessible in archived or backed up storage facilities?	Internal Control		

<b>Accounting Records</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
113. Is the Applicant's accounting software integrated with the back-office application or other relevant gaming systems?	System Functionality		
114. Is the generation of general ledgers, trial balances and financial statements automated by packaged accounting software or an internally developed financial application?	System Functionality		
115. Is accounting software utilized to produce the following financial statements and accounting records: 115.1 Trading accounts, if applicable, for each financial year; 115.2 Profit and loss accounts (income statement) for each financial year; and 115.3 Statement of financial position (balance sheets) as at the end of each financial year.	System Functionality		
116. Does the Applicant have sufficiently qualified staff members that maintain the accounting records and prepare annual financial statements in a manner that can be conveniently and properly audited, if required by the Commission?	Human Resources		

<b>Statutory Audit on Annual Financial Statements</b> <i>(Note: This is not a requirement)</i>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
117. Will the Applicant elect to have its financial statements at an operational level annually audited by an independent third party?	Internal Control		
118. Where the annual financial statements have been audited by an independent third party previously, was an unqualified audit opinion issued?	Internal Control		

**ADVERTISING**

<b>Advertising Must Not Be Indecent or Offensive</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
119. Will management review and formally approve all marketing and advertising material prior to publication?	Internal Control		

<b>Advertising Must Not Be Indecent or Offensive</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
120. Does the Applicant have a verifiable advertising and marketing policy that clearly discourages: 120.1 Advertising content and placement thereof that entices the underage to gamble or bet; 120.2 False or misleading marketing and advertising content; 120.3 Indecent or offensive marketing and advertising content; 120.4 Marketing and advertising content that is not based on fact; and 120.5 The distribution of unsolicited advertisement (i.e. SPAM) either directly or through third parties?	Internal Control		
121. Does the Applicant include an 'unsubscribe' or 'opt out' function on all email marketing and advertisements?	System Functionality		

**INFORMATION SECURITY**

<b>Information security policy</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
122. Has the Applicant formally documented and implemented an information security policy?	Policy Document		
123. Is the information security policy document reviewed at least annually and in the event of material changes?	Internal Control		
124. Has the Applicant developed user awareness material and/or a training manual on the information security policy?	Policy Document		

<b>IT Security Reviews</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
125. Does the Applicant, or a third party on the Applicant's behalf, conduct security reviews over the internal network, including patch level testing, at least annually?	System Functionality		
126. Does the Applicant, or a third party on the Applicant's behalf, perform security reviews over the external perimeter, including penetration testing, at least annually?	Internal Control		
127. Does the Applicant have internal processes in place to address the risks and recommendations resulting from security reviews?	Internal Control		

<b>Security Administration</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
128. Does the information security policy provide for security administration procedures including the review and authorisation of additional employee access rights granted to systems as well as the removal of access rights in a timely manner?	Policy Document		
129. Does a formal documented procedure exist for new or changed user access rights?	Internal Control		
130. Are all access right changes performed by a designated Security Administrator?	Internal Control		
131. Are all new access rights granted to the Applicant's approved by management?	Internal Control		
132. Does management regularly review user access rights and ensure that they are commensurate with job responsibilities?	Internal Control		
133. Is segregation of duties enforced for incompatible functions through controlling access rights granted?	Internal Control		

Schedule "I" Control Systems Submission

<b>Security Administration</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
134. Does a Human Resources representative notify the Security Administrator where employees have been dismissed or where employees change job functions?	Human Resources		

<b>Virus Scanners and detection programs</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
135. Is anti-virus software installed on all relevant servers, desktops and laptops?	Internal Control		
136. Do all machines that are not protected with anti-virus software have compensating controls or low virus risk?	Internal Control		
137. Are processes in place to ensure that the anti-virus software is regularly updated with the latest virus definitions?	Internal Control		
138. Are firewalls implemented and located appropriately in the network environment?	Internal Control		
139. Does the Applicant make use of an intrusion detection system (IDS)/intrusion prevention system (IPS) to detect/prevent possible network threats?	Internal Control		

<b>IT Security Environment Change Control</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
140. Has the Applicant developed a formal documented process for changes to the IT security environment (all hardware and software with IT processing capability), which provides for the logging, approval and implementation of change requests?	Policy Document		
141. Is a change control application used for the logging of all change requests?	Internal Control		
142. Do all change requests require approval prior to implementation?	Internal Control		
143. Does an audit trail exist within the change control application to track who has requested and approved each change request?	Internal Control		
144. Are all requests for changes (RFC) captured and managed from a central repository?	Internal Control		
145. Are change management meetings held on a frequent basis and are minutes of these meetings maintained?	Internal Control		
146. Are change management processes and standards consistent across applications, infrastructure, business units and geographically dispersed locations?	Internal Control		
147. Are processes in place for managing the application of infrastructure-related patches for hardware and software?	Internal Control		

<b>User Access Control</b>	<b>Control Area</b>	<b>Yes</b>	<b>No</b>
148. Do users require a username and password to gain access to the network domain?	System Functionality		
149. Are systems such as the back-office application and development system (if applicable) subject to user authentication controls?	System Functionality		
150. Do the password configuration controls include appropriate settings on the password minimum age, password maximum age, password minimum length, password complexity, password history and account lockout?	System Functionality		
151. Does management have a controlled process in place for evaluating and approving the business rationale for every external network connection (including, but not limited to, Internet, electronic mail, EDI, EFT, dial-in, extranet partners, etc.)?	Internal Control		
152. Are users able to change their network domain passwords?	System Functionality		

User Access Control	Control Area	Yes	No
153. Are users able to change their back-office application passwords?	System Functionality		

**BACKUP AND DISASTER RECOVERY**

Backup and Restore Procedures	Control Area	Yes	No
154. Has the Applicant developed and implemented formally documented backup and recovery procedures?	Policy Document		
155. Does the Applicant backup all critical data including operational servers, database servers and web servers on a daily basis?	Internal Control		
156. Does the Applicant replicate or mirror live gaming data?	Internal Control		
157. Does the Applicant perform major backup restores on a regular basis?	Internal Control		

Offsite Storage	Control Area	Yes	No
158. Are backups stored in a secure offsite location?	Internal Control		
159. Is live gaming data replicated or mirrored to a secure offsite location?	Internal Control		

Disaster Recovery Procedures	Control Area	Yes	No
160. Are disaster recovery responsibilities defined and documented in the agreements between the Applicant and relevant third party providers (e.g. software providers)?	Policy Document		
161. In the event of a disaster, is the Applicant able to recover all gaming data and player information?	Internal Control		
162. Have disaster recovery responsibilities been defined and included in agreements between the operator and the software provider?	Internal Control		

**RECEIPTS AND PAYMENTS FROM PLAYERS**

Financial Reconciliations	Control Area	Yes	No
163. Are the receipts and payments from the back-office application reconciled to the payment processors on a regular basis?	Internal Control		
164. Are the reconciliations of receipts and payments reviewed and approved by management?	Internal Control		
165. Are internal controls in place for the detection and correction of time-out receipts, in a timely manner?	Internal Control		

Financial Transactions	Control Area	Yes	No
166. Do the Applicant's systems have adequate mechanisms and available storage to retain all financial transactions for a minimum period of 12 months?	System Functionality		



