Nevada Gaming Control Board

CPA MICS Compliance Checklist

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

NGC Regulation 6.090(9) requires the CPA to use "criteria established by the chairman" in determining whether an operator of interactive gaming is in compliance with the Interactive Gaming Minimum Internal Control Standards (MICS). This checklist is to be used by the CPA in determining whether the nonrestricted licensee's information technology operation is in compliance with the Information Technology MICS for Interactive Gaming.

Date of Inquiry	Person Interviewed	Position

Manufacturer and Model Type of System in Use	Period in Use

Checklist Completion Notes:

1) Unless otherwise instructed, examine a completed document for compliance for those questions referring to records/documentation and recalculating where appropriate. Indicate (by tickmark) whether the procedures were confirmed via examination/review of documentation, through inquiry of licensee personnel or via observation of procedures. Tickmarks used are to be defined at the bottom of each page.
2) All "no" answers require referencing and/or comment, and should be cited as regulation violations, unless adequate alternative procedures exist (i.e., approval of alternative procedure granted by the Board Chairman, including computerized applications) or the question requires a "no" answer for acceptability. All "N/A" answers require referencing and/or comment, as to the reason the MICS is not applicable.
3) "(#)" refers to the Minimum Internal Control Standards for Information Technology for Interactive Gaming, Version 8.
4) The checklist may be completed by an information technology (IT) specialist. Alternatively, the results of an IT specialist's work during related audit procedures performed (e.g., Sarbanes-Oxley procedures) may be utilized. The procedures performed through the use of an IT specialist is identified as such by documenting in the checklist.

Interactive Gaming Minimum Internal Control Standard Notes

Note 1: Pursuant to Regulation 5A.140, interactive gaming is limited to the game of poker. Furthermore, the Card Games MICS do not apply to interactive gaming.

Note 2: Unless otherwise specified, all Information Technology for Interactive Gaming MICS apply to an interactive gaming application, the underlying database, operating system, and network layer.

Verified per representation.
Verified per observation/examination.

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Note 3: An operator of interactive gaming must specify in their written system of internal control pursuant to Regulation 6.090 which functions (if any) are performed by a service provider. Operators remain responsible for the proper design and operational effectiveness of all required minimum internal control standards, regardless of who is performing the function.

Note 4: For these MICS, a system password is acceptable as the "signature" of the employee authorizing a transaction through the interactive gaming system. An "electronic signature" is allowed only when being used as part of a Board-authorized interactive gaming system. The "electronic signature" is to be linked with an electronic document which identifies the individual entering the "signature". An "electronic signature" may also be attached to some biometric measurement. For instance, fingerprints or iris patterns are common biometric measurements.

Note 5: As used in these MICS, "interactive gaming account" has the same meaning as "wagering account" as defined in Regulation 5.225, as applicable.

Information Technology for Interactive Gaming

Note 1: As used in these MICS, the following terms have the same meanings as delineated in Regulation 14 Technical Standard 6.010, as applicable: Authorized player system; Critical components; Game session; Player session and Table session.

Note 2: Definitions. The following terminology and respective definitions are used in these MICS unless the context requires otherwise:

Backup system log is an event log, a job log or an activity file created by the program or batch process that performs backups of application and data files. These event logs, job logs or activity files usually provide detail on the type of backup performed, success or failure of the operation, and a list of errors.

Default accounts are user accounts with predefined access levels usually created by default at installation for operating systems, databases, and applications. These accounts tend to be used for training purposes.

Generic user accounts are user accounts that are shared by multiple users (using the same password) to gain access to any component of an interactive gaming system: application, database, or operating system.

Group membership (group profile) is a method of organizing user accounts into a single unit (by job position) whereby access to application functions may be modified at the unit level and the changes take effect for all user accounts assigned to the unit.

IT personnel are employees of the operator or an IT Service provider who are independent of the operation of interactive gaming; and who have been designated to perform the information technology function for the operation of critical components of the interactive gaming system.

IT service provider is a person or an entity engaged by the operator, and licensed pursuant to Regulation 5.240, to provide management, including system administration, support, security, or disaster recovery services for Board regulated hardware or software.

Secured repository is a secured environment that is used to store software source code once it has been approved for introduction into the production (live) environment. The repository is secured such that developers cannot modify code once it has been stored. In this way, the repository provides a history of a given software system order by version.

Service accounts are accounts on which automated system functions (services) are dependent to execute. A service account does not correspond to an actual person. These are often built-in accounts that an automated system function (service) uses to access resources they need to perform its activities. However, some automated services may require actual user accounts to perform certain functions, and may be employed using domain accounts to run services.

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

System administrator is the individual(s) responsible for maintaining the stable operation of the IT environment (including software and hardware infrastructure and application software).

Questions	Yes	No	N/A	Comments, W/P Reference
1. Has the licensee's written system of internal control regarding interactive gaming been read prior to the completion of this checklist to obtain an understanding of the licensee's interactive gaming procedures?				
Physical Access and Maintenance Controls				
2. Does the written system of internal control delineate the physical location of each component of the interactive gaming system, including the location of staff (operator, service provider, datacenter operator if the datacenter is maintained by an independent party)? **(1) Verify by examination.**				
3. Is system documentation for all in-use components of the interactive gaming system (versions of application, database, network hardware, and operating system), including descriptions of both hardware and software (including version numbers), operator manuals, etc. maintained? **(2) Verify by examination.**				
4. Does the written system of internal control delineate the responsibilities of staff (operator, service provider, datacenter operator if the datacenter operator is maintained by an independent party) for operation, service and maintenance of the interactive gaming system and/or its components? **(3) Verify by examination.**				
5. Are the critical components of the interactive gaming system maintained in a secured area? **(4) Verify by observation.**				
6. Is the area equipped with controls to provide physical protection against damage from flood, fire, earthquake and other forms of natural or manmade disasters and does it include the following: **(4) Verify by observation.**				
a) Redundant power sources to reduce the risk of data loss in case of interruption of power? **(4a)**				
b) Adequate climate control and fire suppression equipment? **(4b)**				
c) Other measures to ensure physical protection of hardware and software? **(4c)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
d) Adequate security mechanisms, such as traditional key locks, biometrics, combination door lock, or electronic key card system to prevent unauthorized physical access to areas housing critical components of the interactive gaming system? **(4d)**				
7. Relating to the previous question, does the written system of internal control delineate the methods, processes and practices used in meeting the requirements of MICS 4 (a through d)? **(4, Note) Verify by examination.**				
8. Is access to areas housing critical components of the interactive gaming system restricted to authorized IT personnel? **(5)**				
9. Are non-IT personnel, including the manufacturers of the interactive gaming system's computer equipment, only allowed access to the areas housing critical components of the interactive gaming system, when authorized and accompanied by IT personnel and with continuous monitoring by IT personnel during each access? **(5)**				
10. Is a record of each access by non-IT personnel maintained with the name of the visitor(s), time and date of arrival, time and date of departure, reason for visit and the name of IT personnel authorizing such access? **(5) Verify by examination.**				
11. Is the administration of the physical access security mechanism used to secure areas housing the interactive gaming critical components performed by authorized IT personnel? **(6)**				
12. Does the IT department maintain current documentation with respect to the network topology (e.g., flowchart/diagram), deployment of server(s) housing application and database, and inventory of software and hardware deployed (available upon request by authorized internal and external auditors and by Board personnel), and is the employee responsible for maintaining the current documentation on the network topology delineated in the written system of internal control? **(7) Verify by examination**.				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
Network Security 13. Are production networks serving an interactive gaming system and its components secured from outside traffic (e.g., firewall and routers) such that the systems are configured to detect and report security-related events? **(8)** **Note:** A suggested method for complying with MICS #8 is to configure the system to log unauthorized logins, failed login attempts, and other security-related events; and block all unused ports and any in-bound connections originating from outside the network. **(8, Note)**				
14. Relating to the previous question, is the employee responsible for the documentation indicating the procedures for detecting and reporting security-related events delineated in the written system of internal control? **(8) Verify by examination.**				
15. Are network shared drives containing application files and data for the interactive gaming system secured such that only authorized personnel may gain access? **(9)**				
16. Are login accounts and passwords required to administer network and other equipment secured such that only authorized IT personnel may gain access to these devices? **(10)**				
17. Do the passwords for the accounts mentioned in the preceding question meet the security parameters of MICS #23, and are those accounts immediately disabled when IT personnel are terminated? **(10)**				
Remote Access **Note:** For the purposes of the following standards, remote access allows a user access to the operator's network from outside of this network through some form of a data link. Remote access typically involves the use of the Internet, a dial-up modem, and/or Virtual Private Network (VPN) or similar technology. **(Note before 11)**				
18. Is remote access to the interactive gaming system components (production servers, operating system, network infrastructure, application, database and other components) limited to authorized IT department personnel employed by the operator of the interactive gaming system? **(11)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
19. Is remote access by vendor personnel to any component of the interactive gaming system allowed for purposes of support or updates and is it enabled only when approved by authorized IT personnel employed by the interactive gaming system operator? **(12)**				
20. Relating to the previous question, if the remote access to a database is performed by unlicensed vendor personnel, is the remote access continuously monitored by IT personnel employed by the operator of the interactive gaming system? **(12)**				
21. When the interactive gaming system (or its components) can be accessed remotely for purposes of obtaining vendor support, does the written system of internal control specifically address remote access procedures and do the written procedures include, at a minimum, the following: **(13) Verify compliance with documented procedures in the written system of internal control.**				
a) The component(s) of an interactive gaming system requiring vendor support and vendor name(s)? **(13a)**				
b) The method and procedures used to gain access remotely, including the use of passwords and other logical controls? **(13b)**				
c) The procedures to be used by IT personnel employed by the operator of the interactive gaming system to further control and monitor access, and to ensure that vendors have only the access needed to perform authorized support and update functions? **(13c)**				
22. In the event of remote access by a vendor, is a complete record of the access created and includes the following: **Verify by examination.**				
a) The name or identifier of the licensee's employee authorizing access? **(14a)**				
b) The name of the vendor? **(14b)**				
c) The name or identifier of the vendor employee accessing the system? **(14c)**				
d) The name of the user account through which the vendor employee accessed the system? **(14d)**				
e) The system component(s) accessed by the vendor? **(14e)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
f) An adequate and detailed description of work performed? **(14f)**				
g) The date, time and duration of the access? **(14g)**				
23. Are vendor accounts restricted through logical security controls which have the ability to access only the application(s) and/or database(s) that are necessary for the purposes of support or providing updates/upgrades? **(15)**				
24. Does the interactive gaming operator comply with the security methods employed in addition to passwords to verify the identity of the vendor personnel prior to authorizing any remote access for that vendor? **(16)**				
25. Do user accounts used by vendors remain disabled on all operating systems, databases, network devices, and applications until needed by such vendor? **(17) Perform an examination of the system to determine that user accounts remain disabled when not in use.**				
26. Subsequent to an authorized use by a vendor is the account returned to a disabled state? **(17)**				
27. If remote access is allowed for non-IT personnel (management personnel or other authorized employees of the interactive gaming operator) is it limited to only the application functions necessary to perform their job duties? **(18)**				
28. Relating to the previous question, are non-IT personnel precluded from directly accessing any databases or operating systems of any of the interactive gaming system and other production environment servers? **(18) Verify by examination.**				
29. Does the interactive gaming operator comply with the additional security methods employed beyond passwords for user accounts to ensure that the interactive gaming system application and data integrity are maintained and secure? **(18) Verify by examination.**				
30. Relating to the previous question, are the additional security methods delineated in the written system of internal control? **(18) Verify by examination.**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
31. Is any instance of remote access to the interactive gaming system components (by vendor, IT personnel, management personnel, or other authorized employee) automatically logged by a device or software where it is established? **(19)**				
32. Relating to the previous question, at a minimum, does the log indicate the date/time of such access and the identification of the individual accessing the interactive gaming system? **(19) Verify by examination.**				
33. For at least one day each quarter, is the remote access log required by MICS #19 reviewed for remote access for the selected day by accounting/auditing personnel to reasonably ensure that: **(20)**				
a) Each remote access session by a vendor has been appropriately documented (as required by MICS #14)? **(20a)**				
b) Each remote access by non-vendor personnel (IT employee, management personnel, or other authorized employee) is performed by an individual who has been authorized to have such access? **(20b)**				
34. Relating to the previous question, does the written system of internal control delineate the procedures and documentation used to perform the review? **(20, Note) Verify by examination.**				
35. Is evidence of the review of remote access logs maintained for the last four quarterly periods and do they include, at a minimum, the following: **(21) Verify by examination.**				
a) The date and time of the review? **(21a)**				
b) The name and title of the person performing the review? **(21b)**				
c) The remote access log reviewed? **(21c)**				
d) Any exceptions, follow-up and resolution of exceptions? **(21d)**				
System Parameters				
36. Is the interactive gaming system, including application software, logically secured through the use of passwords, biometrics, or other means approved by the Board? (**22) Verify by examination/testing.**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
37. Do security parameters for passwords meet the following minimum requirements: **(23) Verify by examination.**				
a) Are the passwords changed at least once every 90 days? **(23a)**				
b) Are the passwords at least 8 characters in length and contain a combination of at least two of the following criteria: upper case letters, lower case letters, numeric and/or special characters? **(23b)**				
c) Are passwords not allowed to be re-used for a period of 18 months; or are passwords not allowed to be re-used within the last ten password changes? **(23c)**				
d) Are user accounts automatically locked out after 3 consecutive failed login attempts? **(23d)** **Note 1:** MICS #23 does not apply to service accounts and generic user accounts. **(23, Note 2)** **Note 2:** For MICS #23d, the system may automatically release a locked out account after 30 minutes has elapsed. If an employee assists with releasing a locked out account and is reasonably certain of no unauthorized user access, the elapse time of 30 minutes is not applicable. The involvement of an employee assisting in the release of a locked out account is to be delineated in the written system of internal control. **(23, Note 3)**				
38. Does the written system of internal control delineate the methods used to comply with MICS #23(b) and (c)? **(23, Note 1) Verify by examination.**				
39. Is a system event log or series of reports/logs for operating systems (including the database layer and network layer) and applications configured to track at least the following events: **Verify by examination. State names/titles of reports/logs used for tracking each event.**				
a) Failed login attempts? **(24a)**				
b) Changes to live data files occurring outside of normal program and operating system execution? **(24b)**				
c) Changes to operating system, database, network, and application policies and parameters? **(24c)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
d) Audit trail of information changed by administrator accounts? **(24d)**				
e) Changes to date/time on master time server? **(24e)**				
f) Significant periods of unavailability of the interactive gaming system or any critical component of the interactive gaming system? **(24f)** **Note:** A significant period may be any length of time when a transaction cannot be performed. **(Note, 24f)**				
g) Other significant events? **(24g) Describe other significant events that are logged.**				
h) For MICS #24(g), does the written system of internal control delineate what other events are to be logged? **(24g) Verify by examination.**				
40. Are all critical components of the interactive gaming system operational in order for the interactive gaming system to operate and commence interactive gaming? **(25)**				
41. Does the interactive gaming system detect and record information regarding failure or non-operation of any component within the interactive gaming system and is a log of this event generated? **(25) Verify by examination. State the name of the log.**				
42. Are the daily system event logs reviewed at least once a week (for each day of the entire previous week) by IT personnel, other than the system administrator, for events listed in MICS #24 and #25? **(26)**				
43. Are the system event logs (MICS #24 and #25) maintained for a minimum of seven days following the review? **(26)**				
44. Is evidence of the daily system event log review described in MICS #26 documented and maintained for 18 months following the completion of the review and does it include the following: **(27) Verify by examination.**				
a) Date and time of review? **(27a)**				
b) Name and title of person performing the review? **(27b)**				
c) Any exceptions noted? **(27c)**				
d) Follow-up and resolution of exceptions? **(27d)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
Note: Compliance with MICS #26 and #27 may involve the use of an automated tool that "flags" the events for the interactive gaming system and provides the person assigned to complete the review with notification. A record of the notification should include the date and time of the notification. **(27, Note)**				
45. Are exception reports for the interactive gaming system configured to track the following events that require employee intervention including, but not limited to, the following: **(28) Verify by examination.**				
a) Adjustments to an authorized player's interactive gaming account balance? **(28a)**				
b) Changes made to information recorded in an authorized player's interactive gaming account? **(28b)**				
c) Changes made to an authorized player's self-exclusion limits? **(28c)**				
d) Changes made to game parameters (e.g., game rules, payout schedules, rake percentage)? **(28d)**				
e) Changes made to payout parameters? **(28e)**				
f) Voids, overrides, corrections? **(28f)**				
g) Mandatory deactivation of an authorized player? **(28g)**				
h) Any other activity requiring employee intervention and occurring outside of the normal scope of system operation? **(28h)**				
46. Do the exception reports produced for the interactive gaming system for the events listed in MICS #28 include, at a minimum, the following: **Verify by examination.**				
a) Date and time of the exception event? **(29a)**				
b) Unique transaction identifier? **(29b)**				
c) Identification of user who performed and/or authorized alteration? **(29c)**				
d) Data or parameter altered? **(29d)**				
e) Data or parameter value prior to alteration? **(29e)**				
f) Data parameter value after alteration? **(29f)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
Structure of Information Technology Department				
47. Are IT personnel precluded from having access to any physical forms/documentation associated with patrons' accounts and interactive gaming (e.g., deposit/withdrawal slips, checks, etc.)? **(30)**				
Note: Administrative access means access that would allow a user (i.e., system administrator) to: • Add, change, or delete user accounts and associated user provisioning; • Modify operating system, network, database, and application layers' security and policy parameters; • Add, change, or delete system exception logging information; or • Add, change, or delete permission to data files, folders, libraries, tables, or databases. **(Note before 31)**				
48. Is access to administer the network, operating system, applications, and database security and system parameters limited to:				
a) Supervisory and/or management employees of the IT department or; **(31a)**				
b) IT employees under the supervision of supervisory and/or management employees of the IT department or; **(31b)**				
c) Employees of operator/service provider of interactive gaming under the supervision of supervisory and/or management employees of the IT department or; **(31c)**				
d) Employees of IT service provider? **(31d)**				
49. For MICS #31, does the written system of internal control delineate the assignment of administrative access and function for various components of the interactive gaming system? **(31, Note) Verify by examination.**				
50. Are the interactive gaming system and its components being administered enabled to log all administrative account's activity? **(32)**				

Verified per representation.
Verified per observation/examination.

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
51. Regarding the previous question, are such logs maintained and do they include the time, date, login account name, description of event, the value before the change, and the value after the change? **(32) Verify by examination.**				
52. Is administrative access at the operating system level for all servers that support or are part of the interactive gaming system reviewed quarterly? **(33)**				
53. Are the reviews mentioned in the previous question performed by personnel independent of the IT department and do they include a complete review of all user accounts with administrative access? Does the reviewer perform the following: **(33)**				
a) Review all administrative groups and groups with elevated privileges to ensure membership is appropriate? **(33a)**				
b) Review the last login date and time for all administrative accounts to determine whether any "stale" accounts exist (e.g., users on extended leave or terminated IT employees remain active in the system)? **(33b)**				
c) Review administrative accounts to ensure that passwords have been changed at least once every 90 days? **(33c)**				
d) Examine user list to determine whether IT personnel utilize normal user accounts for regular use and administrator accounts for administrative functions? **(33d)**				
e) Document the results of the review along with the date, time, and name and title of the person performing the review and retain it for a period of 18 months. **(33e) Verify by examination.**				
User Accounts				
54. Does a system administrator establish user accounts for new employees and employees who transfer to a new department? **(34)**				
55. Does provisioning for user accounts consist of assigning application functions matching the employee's current job responsibilities, unless otherwise authorized by management personnel, to ensure adequate separation of duties? **(34)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
56. Do transferred employees have access appropriate for the new position only when the access for the previous position has been removed or disabled? **(34)**				
57. Is the access provisioning process documented and does the documentation evidence authorization by the appropriate management personnel, original user access and each subsequent change to user account? **(35)**				
58. Regarding the previous question, is the documentation maintained and made available upon request? **(35) Verify by examination.**				
59. Is a "User Access Listing" report produced by the interactive gaming system and does it include, at a minimum, the following: **Verify by examination.**				
a) Employee name and title or position? **(36a)**				
b) User login name? **(36b)**				
c) Full list and description of application functions that each group/user account may execute? **(36c)**				
d) Date and time the account was created? **(36d)**				
e) Date and time of last login? **(36e)**				
f) Date of last password change? **(36f)**				
g) Date and time account disabled/deactivated? **(36g)**				
h) Group membership of user account, if applicable? **(36h)**				
60. Are the "User Access Listing" reports for the interactive gaming system retained for at least one day of each month for the most recent five years? The reports may be archived electronically if the listing is written to unalterable media (secured to preclude alteration). **(37) Verify by examination.**				
61. Is the list of users and user access for an interactive gaming system available in electronic format which can be analyzed by analytical tools (e.g., spreadsheet or database) that may be employed by Board agents? **(37) Verify by examination.**				
62. When multiple user accounts for one employee within a single application are used: **Verify by examination.**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
a) Can only one user account be active (enabled) at a time if the concurrent use of the multiple accounts by the employee could create a segregation of duties deficiency? **(38)**				
b) Does the user account have a unique prefix/suffix to easily identify the users with multiple user accounts within one application? **(38)**				
63. When an employee is known to be no longer employed (e.g., voluntary or involuntary termination of employment):				
a) Is the system administrator notified within a reasonable period of time, established by management? **(39)**				
b) Upon notification, does the system administrator change the status of the employee's user account from active to inactive (disabled) status? **(39)**				
c) Does the written system of internal control delineate the process and time period in notifying the system administrator for updating the terminated employee's user account and does it address the procedures established for updating the account status and preventing the employee from having unauthorized access to a user terminal? **(39)** **Verify by examination. Verify compliance with documented procedures in the written system of internal control.**				
Note: For MICS #39, the period of time for notification of the system administrator is to be set such that it is unlikely that the terminated employee would gain access to a user terminal within the notification period. **(39, Note)**				
64. When an employee who has a user account with remote access capability is known to be no longer employed (e.g., voluntary or involuntary termination of employment):				
a) Is the system administrator notified as soon as possible? **(40)**				
b) Upon notification, does the system administrator change the status of an employee's user account with remote access capability from active to inactive (disabled) status? **(40)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
c) Does the written system of internal control delineate the process and time period in notifying the system administrator and does it address the procedures established for updating the account status and preventing the employee from having unauthorized remote access? **(40) Verify by examination. Verify compliance with documented procedures in the written system of internal control.**				
Note: For MICS #40, the period of time for notification of the system administrator is to be set such that it is unlikely that the terminated employee would gain remote access within the notification period. **(40, Note)**				
65. Are user access listings reports produced at the application layer reviewed quarterly by personnel independent of the authorization and user provisioning processes? **(41)**				
66. Does the review mentioned in the previous question consist of examining a sample of at least 10% (with a maximum of 25) of the users included in the listing? **(41)**				
67. Does the reviewer maintain adequate evidence to support the review process, which includes the selected user accounts reviewed, documentation of the results of the review, and e-mails or signatures and dates indicating the individual(s) performing the review and when the access listing was reviewed? **(41) Verify by examination.**				
68. Pursuant to MICS #41, are each of the randomly selected user accounts reviewed to determine whether:				
a) The assigned system functions are being used as authorized (i.e., system functions are appropriate for user's job position)? **(41a)**				
b) The assigned functions provide an adequate segregation of duties? **(41b)**				
c) Terminated employees' user accounts have been changed to inactive (disabled) status? **(41c)**				
d) Passwords have been changed within the last 90 days? **(41d)** **Note:** The review for password changes within 90 days applies regardless of whether the system parameter has been configured to have the password changed at least once every 90 days. **(41d, Note)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
e) There are no inappropriate assigned functions for group membership, if applicable? **(41e)** **Note:** MICS #41(e) applies to a review of the assigned functions for the selected user account with group membership. **(41e, Note)**				
Generic User Accounts, Service & Default Accounts				
69. Are generic user accounts at the operating system level, if used, configured such that the user is automatically brought to the application logon screen immediately upon logging into the operating system? **(42)**				
70. Are generic user accounts configured such that the user is logged out of the operating system automatically upon exiting the application? **(42)**				
71. Are generic user accounts at the application level prohibited unless user access is restricted to inquiry only functions? **(43)**				
72. If service accounts are used:				
a) Are they utilized in a manner to prevent unauthorized and inappropriate usage to gain logical access to an application and the underlying databases and operating system? **(44)**				
b) Is the employee responsible for the documentation indicating the method used to prevent unauthorized and inappropriate usage of these service accounts (available upon request by authorized internal and external auditors and by Board personnel) delineated in the written system of internal control. **(44) Verify by reviewing the documentation indicating the process. Additionally, confirm compliance with documented procedures.**				
Note: For MICS #44, the suggested methods include: (1) Service accounts are configured such that the account cannot be used to directly log in to the console of a server or workstation; (2) Service account passwords are to be changed at least once every 90 days, and immediately upon termination of system administrators. **(44, Note)**				
73. For user accounts created by default (default accounts) upon installation of any operating system, database or application:				
a) Are they configured to minimize the possibility that these accounts may be utilized to gain unauthorized access to system resources and data? **(45)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
b) Is the employee responsible for the documentation indicating the procedures implemented to restrict access through the use of default accounts (available upon request by authorized internal and external auditors and by Board personnel) delineated in the written system of internal control? **(45) Verify by reviewing the documentation indicating the process. Additionally confirm compliance with documented procedures.**				
74. Are any other default accounts that are not administrator, service, or guest accounts disabled unless they are necessary for proper operation of the system? **(46)**				
75. If the accounts mentioned in the previous question must remain enabled, are the passwords changed at least once every 90 days? **(46)**				
76. Do system administrators maintain a current list of all enabled generic, system, and default accounts? **(47) Verify by examination.**				
77. Relating to the previous question, does the documentation include, at a minimum, the following:				
a) Name of system (i.e., the application, operating system, or database)? **(47a)**				
b) The user account login name? **(47b)**				
c) A description of the account's purpose? **(47c)**				
d) A record (or reference to a record) of the authorization for the account to remain enabled? **(47d)**				
78. Is the current list reviewed by IT management in addition to the system administrator at least once every 6 months? **(48)**				
79. Relating to the previous question, are the following necessary procedures performed:				
a) To identify any authorized or outdated accounts? **(48a)**				
b) To ensure that all service, generic, and default accounts are not enabled for remote access? **(48b)**				
c) To determine that the method used is a properly designed control process and is effectively operating to secure the generic, service, and default accounts from unauthorized usage? **(48c)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
Backup and Recovery Procedures				
80. Are daily backup and recovery procedures in place? **(49)**				
81. Relating to the previous question, do the procedures in place, if applicable, include:				
a) Application data? **(49a)**				
b) Application executable files, unless such files can be reinstalled? **(49b)**				
c) Database contents and transaction logs? **(49c)**				
82. Upon completion of the backup process, is the backup media immediately transferred to a location separate from the location housing the servers and data being backed up (for temporary and permanent storage), is the storage location secured to prevent unauthorized access and does it provide adequate protection to prevent the permanent loss of any data? **(50) Verify by observation.** **Note:** Backup data files and programs can be maintained in a secured manner in another building on the premises that is physically separated from the building where the system's hardware and software are located. They may also be stored in the same building as the hardware/software, but not in the same immediate area, as long as they are secured in a fireproof safe or some other manner that will ensure the safety of the files and programs in the event of a fire or other disaster. **(50, Note)**				
83. Are backup system logs reviewed daily by IT personnel or individuals authorized by IT personnel to ensure that backup jobs execute correctly and on schedule and are the backup system logs maintained for the most recent 30 days? **(51)**				
84. Is the employee responsible for the documentation indicating the procedures implemented for the backup processes and restoring data and application files (available upon request by authorized internal and external auditors and by Board personnel) delineated in the written system of internal control? **(52) Verify by reviewing the documentation indicating the process. Additionally, confirm compliance with documented procedures.**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
85. On a quarterly basis, do IT personnel test the recovery procedures? Is a record maintained indicating the date a test of the recovery procedures was performed and the results of the recovery test? **(53) Verify by examination.**				
Electronic Storage of Documentation				
86. If reports and other documents/records are directly written to an electronic document retention system in a portable document format (PDF), stored to a Board approved document retention system, or scanned to an electronic document retention system into either a portable document format or standard image format does the system meet the following conditions: **(54)**				
a) Is it properly configured to maintain the original version along with all subsequent versions reflecting all changes to the document? **(54a)**				
b) Is a unique "hash" signature for each version of the document maintained, including the original? **(54b)**				
c) Retains and reports a complete log of changes to all documents including who (user ID and name) performed the changes and when (date and time)? **(54c)**				
d) Provides a method of complete indexing for easily locating and identifying the document including at least the following (which may be input by the user): **(54d)**				
i. Date and time document was generated? **(54d)(i)**				
ii. Application or system generating the document? **(54d)(ii)**				
iii. Title and description of the document? **(54d) (iii)**				
iv. Name and title of the user/employee generating the document? **(54d) (iv)**				
v. Any other information that may be useful in identifying the document and its purpose? **(54d) (v)**				
e) Is it configured to limit access to modify or add documents to the system through logical security of specific user accounts? **(54e)**				
f) Is it configured to provide a complete audit trail of all administrative user account activity? **(54f)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
87. If scanned, is the documentation verified by at least one additional person when being added to the electronic document storage system to ensure that the scanned version is identical to the original document? **(55)**				
88. Relating to the previous question, does the second person provide an electronic signature or other method of sign-off verification with the date and time to demonstrate that the review was performed prior to the document being added to the system? **(55)**				
89. If the electronic document retention systems utilize CD-ROM, DVD-ROM, Hard Drive, or other type of storage, is the system properly secured through use of logical security measures (user accounts with appropriate access, proper levels of event logging, and document the version control, etc.)? **(56)**				
90. Relating to the previous question, is the system physically secured with all other critical components of the interactive gaming system? **(56)**				
91. Are electronic document retention systems equipped to prevent disruption of document availability and loss of data through hardware and software redundancy best practices, and backup processes? **(57)**				
92. On a quarterly basis, do accounting/audit personnel perform the following procedures: **(58) Verify by examination.**				
a) Review a minimum of 20 documents added to the electronic retention system to determine that:				
i. The documents are accurate reproductions of the original and the hash signatures match to the signatures recorded when the documents were added to the system? **(58ai)**				
ii. The documents are readable and version control is functioning properly (i.e., all changes after the original was added are reflected in subsequent versions)? **(58aii)**				
iii. Indexing is correct (i.e., all information is accurate and the document is easily identified)? **(58aiii)**				
b) Verify that user access to add or modify documents is set to an appropriate level of access to administer the electronic document retention system, and no terminated employees have active user accounts on the system? **(58b)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
c) Verify that event recording and reporting is functioning as designed and the logs are being reviewed by the appropriate personnel regularly? **(58c)**				
d) Verify that redundancy exists and is adequately functional to limit the level of risk that an outage or loss of records may occur in the event of hardware failure or other unforeseen event? **(58f)**				
93. Is evidence of all reviews and verifications listed in MICS #58 made available upon request? **(59)**				
94. For MICS #'s 54-59 does the written system of internal control delineate the name and components of the electronic storage system, all procedures used for electronic document retention and the titles for all employees responsible for administering and maintaining the system? **(Note before 54) Verify by reviewing the documentation indicating the process. Additionally, confirm compliance with documented procedures.**				
Production Environment Change Control Processes				
95. Has the interactive gaming system operator adopted a comprehensive and robust change control process to prevent unauthorized changes from being incorporated into the production environment at any layer? **(60)**				
96. Does the process include ALL changes to the interactive gaming production environment (operating system, network, databases, and applications)? **(60) Verify by reviewing the documentation indicating the process.**				
97. Is the change control process, including the titles of individuals responsible for all key decision points in the process documented in the written system of internal control? **(60) Verify compliance with written system of internal control.**				
98. Does the change control process include, at a minimum, the following: **(60) Verify by examination.**				
a) Are proposed changes to the production environment evaluated sufficiently for the impact on all aspects of production environment and authorized by management personnel prior to implementation? **(60a)**				
b) Are proposed changes properly and sufficiently tested prior to implementation into the production environment? **(60b)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
c) Is a strategy of reverting back to the last implementation (rollback plan) used if the install is unsuccessful and is the rollback plan tested prior to implementation to the production environment? **(60c)**				
d) Is sufficient documentation maintained evidencing management evaluation, approvals, testing procedures and results, rollback plans, and any issues/resolutions encountered during implementation? **(60d)**				
99. Relating to the questions above, are all changes sufficiently documented and maintained and include at a minimum, the following: **(61) Verify by examination.**				
a) The date the program was placed into service? **(61a)**				
b) The nature of the change (if applicable)? **(61b)**				
c) A description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.)? **(61c)**				
d) An indication of who performed all such procedures? **(61d)**				
100. Is a copy of the associated equipment reporting form submitted to the Board pursuant to Regulation 14 for each new program or program change and is a record indicating Board approval maintained? **(62)**				
101. Quarterly, do audit/accounting personnel review a sample of changes made during the prior period to determine that such changes were properly approved, adequately documented, properly tested, and issues resolved and rollback procedures applied? **(63)**				
102. Is evidence of the review documented and maintained and does it include, at a minimum, the date of the review, the name of the individual(s) who performed the review and the exceptions noted and any related follow-up on the noted exceptions? **(63) Verify by examination.**				
103. Does the interactive gaming system operator develop any software that interfaces with the interactive gaming application, or develop any or all source code for interactive gaming application modules? **(64) If yes, answer the next questions. If no, the next questions are not applicable.**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
104. If the previous question was answered yes, did the operator adopt and document in its system of internal control a comprehensive and robust software development change control process and does the software development change control process incorporate the following requirements: **(64) Verify by examination.**				
a) The source code is maintained in a secured repository for code history and version control? **(64a)**				
b) The technical documentation, including all regulatory submission and approval forms is maintained and available upon request. Technical documentation must include approvals, development, testing, results of testing, and implementation into production. Documentation also includes a record of the final program or program changes, including evidence of user acceptance, date placed in service, programmer sign-off, and explanation of the changes? **(64b)**				
c) The production environment is logically and physically segregated from the test/development environment(s)? **(64c)**				
d) All enhancements and changes are reviewed and approved by management prior to development and the review and approval process is documented. Review and approval documentation, along with technical documentation, is maintained by an individual independent of the development process? **(64d)**				
e) Developers are precluded from having access to promote code changes into the production environment. All changes must be promoted into production by someone independent of the development and testing function? **(64e)**				
f) End user documentation is maintained and remains current to reflect the most recent software changes (this documentation may be available electronically to the end user)? **(64f)**				
g) Adequate segregation of duties exists among developers, testing personnel, administrators, personnel who may promote changes into production, personnel who may access frozen code, etc.? **(64g)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY FOR INTERACTIVE GAMING
MICS #1 - #64

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
h) An evaluation of the impact of changes on all parts of the production environment and interactive gaming application is performed, and a roll-back plan has been developed in case of failed promotion into production? **(64h)**				
i) Analysis and verification processes are performed to establish the integrity of data when conversion or migration occurs as part of the development process? **(64i)**				
Written System of Internal Control				
105. Has the licensee's written system of internal control for interactive gaming been re-read prior to responding to the following question?				
106. Does the written system of internal control for information technology for interactive gaming reflect the actual control procedures in effect for compliance with the MICS, variations from the minimum internal control standards approved pursuant to Regulation 6.090(8), and Regulation 14 associated equipment approvals? **[Regulation 6.090(13)]**				

Verified per representation.
Verified per observation/examination.