State of Nevada
Gaming Control Board

CPA MICS Compliance Checklist

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

NGC Regulation 6.090(9) requires the CPA to use "criteria established by the chairman" in determining whether a Group I licensee is in compliance with the Minimum Internal Control Standards (MICS). This checklist is to be used by the CPA in determining whether the licensee's information technology operation is in compliance with the Information Technology MICS.

Gaming Department: _____

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, Version 6.
4) Entertainment tax related application and pari-mutuel system - This checklist is not required to be completed for licensees (including another person affording the entertainment at a leased facility of the licensee's gaming establishment) not performing the system's administrative function (includes the maintenance of the system). "Administrative access" is defined above IT MICS #22. In this situation, the licensee has installed only user terminals and printers allowing for the recording of transactions processed by the licensee and for the printing of applicable reports. The user terminals and printers are connected directly to a system physically maintained at an unaffiliated person's or entity's place of business.
5) The checklist may be completed by an information technology (IT) specialist. Alternatively, the results 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.

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Minimum Internal Control Standard Notes (paraphrased from the standards)

Note 1: Unless otherwise specified, all Information Technology (IT) MICS apply to gaming and entertainment tax related applications, and the underlying databases and operating systems. Entertainment tax related applications include systems used to record admission ticket sales and point-of-sale systems used to record food, beverage, merchandise, admission and any other sales subject to live entertainment tax. If a person or entity other than the licensee offers entertainment subject to the entertainment tax on the licensee's premises, the entertainment tax related application being used shall be compliant with the IT MICS.

Note 2: The IT MICS do not apply when a person or entity other than the licensee operates a box office system for handling and recording live entertainment taxable admission sales (e.g., Ticket Master box office system). The IT MICS do apply when a licensee operates a box office system (for in-person sales or sales made through the Internet) for handling and recording live entertainment taxable admission sales.

Note 3: The types of gaming and entertainment tax related applications (including version numbers used) and the procedures and records used to comply with IT MICS #1 - #28, as applicable, must be addressed in detail in each applicable section, including the entertainment section, of the written system of internal control pursuant to Regulation 6.090. The Information Technology section of the written system of internal control pursuant to Regulation 6.090 includes the procedures and records used to comply with IT MICS #29 - #55, as applicable.

Note 4: Definitions. The following terminology and respective definitions are used in these MICS unless the context requires otherwise:

Backup system log is an event, 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.

Critical IT systems and equipment includes all components of systems hardware and software, application software, and database software that individually or in combination are necessary for the stable operation of gaming and entertainment systems. The term does not include user terminals.

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 gaming and entertainment systems and applications.

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 who are independent of the gaming and entertainment department; and have been designated to perform the information technology function for the operation of critical IT systems and equipment.

Physical and logical segregation of the development and testing from the production environment is separating the development and testing of new software in an environment that is isolated from the regular production (live) network. The development environment is located on a separate server and developers are precluded from having access to the production environment.

Verified per representation.
Verified per observation/examination.

State of Nevada
Gaming Control Board

CPA MICS Compliance Checklist

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

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 are dependent to execute. These accounts defined at the operating system level provide a certain level of access necessary for normal operation of applications and/or automated batch processes.

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

Vendor supported system is one type of critical IT systems and equipment; however, this type of system is supported solely by the manufacturer of such system.

Questions	Yes	No	N/A	Comments, W/P Reference
1. Has the licensee's written system of internal control for information technology regarding the gaming department being reviewed been read prior to the completion of this checklist to obtain an understanding of the licensee's information technology procedures for the gaming department being reviewed?				
Physical Access and Maintenance Controls				
2. Are the critical IT systems and equipment for each gaming application (e.g., keno, race and sports, slots, cashless wagering systems, etc.) and each application for entertainment maintained in a secured area? **(1) Verify by observation.**				
3. Is the area housing the critical IT systems and equipment for each gaming and entertainment application and other critical IT systems and equipment equipped with the following:				
a) Redundant power sources to reduce the risk of data loss in case of interruption of power? **(1a)** **Note:** MICS 1(a) does not apply to components in the slot gaming device cabinet. **(1a)**				
b) An adequate security mechanism, such as traditional key locks, biometrics, combination door lock, or electronic key card system to prevent unauthorized physical access? **(1b)**				
4. Is access to areas housing critical IT systems and equipment for gaming and entertainment applications, excluding vendor supported systems, restricted to authorized IT personnel? **(2)**				

Verified per representation.
Verified per observation/examination.

State of Nevada
Gaming Control Board

CPA MICS Compliance Checklist

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
5. Are gaming and entertainment department personnel, including the manufacturers of the gaming and entertainment computer equipment, only allowed access to the areas housing critical IT systems and equipment for gaming and entertainment applications, excluding vendor supported systems, when authorized by IT personnel and with periodic monitoring by IT personnel during each access? **(2)**				
6. 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? **(2) Verify by examination.**				
7. Is access to an area housing a vendor supported system for gaming and entertainment applications restricted to authorized IT personnel, or to system manufacturer's personnel when authorized by management and with periodic monitoring during each access by IT personnel or personnel independent of the department using such application? **(3)**				
8. Is a record of access by system manufacturer personnel to an area housing a vendor supported system for gaming and entertainment applications maintained with the name of the visitor(s), time and date of arrival, time and date of departure, and reason for visit? **(3) Verify by examination.**				
9. Is the administration of the electronic security systems, if they are used to secure areas housing gaming and entertainment critical IT systems and equipment, performed by personnel independent of a gaming or entertainment department? **(4)**				
System Parameters				
10. Are the computer systems, including application software, logically secured through the use of passwords, biometrics, or other means approved by the Board? **(5) Verify by observation.**				
11. Do security parameters for passwords, if configurable, meet the following minimum requirements: **Verify by examination.**				
a) Are the passwords changed at least once every 90 days? **(6a)**				
b) Are the passwords at least 8 characters in length and do they contain a combination of at least two of the following criteria: upper case letters, lower case letters, numeric and/or special characters? **(6b)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
c) Are the passwords not allowed to be re-used for a period of 18 months or within the last 10 password changes? **(6c)**				
d) Are user accounts locked out after 3 failed login attempts? **(6d)** **Note 1:** MICS #6 does not apply to service accounts and generic user accounts. **(6, Note 2)** **Note 2:** For MICS #6d, the system may release a locked out account after 30 minutes has elapsed. **(6, Note 3)**				
12. Does the written system of internal control delineate whether the system is configurable for security parameters for passwords and to what extent the system is configurable in meeting the security parameter requirements? **(6, Note 1) Verify by examination.**				
13. Is a system event log or series of reports/logs for operating systems (including the network layer) and gaming and entertainment applications, if capable of being generated by the system, configured to track the following events: **Verify by examination.**				
a) Failed login attempts? **(7a)**				
b) Changes to live data files occurring outside of normal program and operating system execution, if configurable? **(7b)**				
c) Changes to operating system, database, network, and application policies and parameters, if configurable? **(7c)**				
d) Audit trail of information changed by administrator accounts, if configurable? **(7d)**				
e) Changes to date/time on master time server, if configurable? **(7e)**				
14. For MICS #7, does the written system of internal control delineate whether the system is configurable, and to what extent the system is configurable, in tracking the specified events? **(7, Note) Verify by examination.**				
15. 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 #7? **(8)**				

Verified per representation.
Verified per observation/examination.

State of Nevada
Gaming Control Board

CPA MICS Compliance Checklist

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
16. Are the system event logs (MICS #7) maintained for a minimum of seven days, consisting of the period previously reviewed? **(8)**				
17. Is evidence of the system event log review (e.g., log, checklist, notation on reports) maintained for a minimum of 90 days and does it include the date, time, name of the individual performing the review, the exceptions noted and any follow-up of the noted exception? **(8)**				
Note: For MICS #8 an automated tool that polls the event logs for all gaming and entertainment related servers, and provides the system administrators notification of the above may be used. Maintaining the notification for 90 days may serve as evidence of the review. **(8, Note)**				
18. Are exception reports, if capable of being produced by the system, (e.g., changes to system parameters, corrections, overrides, voids, etc.) for each gaming application and entertainment tax related application maintained? **(9) Verify by examination.**				
19. Do the exception reports, if applicable, mentioned in the previous include, at a minimum, the following: **Verify by examination.**				
a) Date and time of alteration? **(9a)**				
b) Identification of user that performed the alteration? **(9b)**				
c) Data or parameter altered? **(9c)**				
d) Data or parameter value prior to alteration? **(9d)**				
e) Data or parameter value after alteration? **(9e)**				
20. Does the written system of internal control indicate the system's capability of producing an exception report and to what extent this report provides specified information? **(9, Note) Verify by examination.**				
User Accounts				
21. Do management personnel, or persons independent of the department being controlled, establish, or review and approve, user accounts for new employees? **(10)**				

Verified per representation.
Verified per observation/examination.

State of Nevada
Gaming Control Board

CPA MICS Compliance Checklist

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
22. 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? **(10)**				
23. Is provisioning of user accounts for employees who transfer to a new department performed, or reviewed and approved by management personnel, or persons independent of the department being controlled? **(11)**				
24. For employees who transfer to a new department, is any previously assigned application function access for the employee's user account changed to inactive (disabled) prior to the employee accessing their new user account for their role or position in the new department? **(11)**				
25. Do user access listings include, if the system is capable of providing such information, the following at a minimum: **Verify by examination.**				
a) Employee name and title or position? **(12a)**				
b) User login name? **(12b)**				
c) Full list and description of application functions that each group/user account may execute? **(12c)** **Note:** The list for MICS #12c may be available in a separate report if the menu functions are easily referenced between the user access listing report and the menu function report. **(12c, Note)**				
d) Date and time the account was created? **(12d)**				
e) Date and time of last login? **(12e)**				
f) Date of last password change? **(12f)**				
g) Date and time account disabled/deactivated? **(12g)**				
h) Group membership of user account, if applicable? **(12h)**				
26. Does the written system of internal control indicate the system's capability of producing a user access listing and to what extent the system's listing provides specified information? **(12, Note)** **Verify by examination.**				
27. When multiple user accounts for one employee per application are used: **Verify by examination.**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

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 resulting in noncompliance with one or more MICS? **(13)**				
b) Does the user account have a unique prefix/suffix to easily identify the users with multiple user accounts within one application? **(13)**				
28. 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? **(14)**				
b) Upon notification, does the system administrator change the status of the employee's user account from active to inactive (disabled) status? **(14)**				
c) Does the written system of internal control delineate the process and reasonable time period in notifying the system administrator for updating the terminated employee's user account and does it address the procedures established in preventing the employee from having unauthorized access to a user terminal? **(14) Verify by examination. Verify compliance with documented procedures in the written system of internal control.**				
Note: For MICS #14, the reasonable period of time in notifying the system administrator to change the status of the terminated employee's user account assumes that it is relatively unlikely the employee will have unauthorized access to a user terminal during that time period. **(14, Note)**				
29. 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? **(15)**				
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? **(15)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
c) Does the written system of internal control delineate the process in notifying the system administrator as soon as possible for immediately updating the terminated employee's user account with remote access capability and does it address the procedures established in preventing the employee from having unauthorized remote access? **(15) Verify by examination. Verify compliance with documented procedures in the written system of internal control.**				
Note: For MICS #15, during the period of time when the employee is no longer employed and until the user account has been disabled, it is assumed that it is relatively unlikely the employee will have unauthorized remote access to the system during that time period. **(15, Note)**				
30. Are user access listings for gaming applications at the application layer reviewed quarterly by personnel independent of the authorization and user provisioning processes? **(16)**				
31. 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? **(16)**				
32. Relating to the previous question, does the reviewer maintain adequate evidence to support the review process, which includes the identified accounts reviewed, documentation of the results of the review, and e-mails or signatures and dates indicating when the user access listing was reviewed? **(16)**				
33. Are each of the user accounts selected pursuant to MICS #16 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)? **(16a)**				
b) The assigned functions provide an adequate segregation of duties? **(16b)**				
c) Terminated employees user accounts have been changed to inactive (disabled) status? **(16c)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
d) Passwords have been changed within the last 90 days? **(16d)** **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 as required by MICS #6a. **(16d, Note)**				
e) There are no inappropriate assigned functions for group membership, if applicable? **(16e)** **Note:** MICS 16(e) applies to a review of the assigned functions for the selected user account with group membership. **(16, Note 3)**				
Note 1: The review required by MICS #16 does not apply to user access listing for pari-mutuel systems and for any entertainment tax related applications. **(16, Note 1)** **Note 2:** The MICS #16 review applies to user access listings for computerized gaming systems with the following capabilities: • Generates reports identifying gaming revenues; • Generates detailed records of all markers, IOU's, returned checks, hold checks, or other similar credit instruments; • Generates statistical gaming records required by the MICS; or • Generates any other records required by either the MICS or by the licensee's system of internal control. **(16, Note 2)**				
Generic User Accounts				
34. 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? **(17)**				
35. Are generic user accounts configured such that the user is logged out of the operating system automatically upon exiting the application? **(17)**				
36. Are generic user accounts at the application level prohibited unless user access is restricted to inquiry only functions or is specifically allowed in other sections of the MICS? **(18)**				
Service and Default Accounts				

Verified per representation.
Verified per observation/examination.

State of Nevada
Gaming Control Board

CPA MICS Compliance Checklist

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
37. 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 systems? **(19)**				
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. **(19) Verify by reviewing the documentation indicating the process. Additionally, confirm compliance with documented procedures.**				
Note: For MICS #19 the suggested methods to accomplish compliance 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. **(19, Note)**				
38. 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? **(20)**				
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? **(20) Verify by reviewing the documentation indicating the process. Additionally confirm compliance with documented procedures.**				
39. Are any other default accounts that are not administrator, service, or guest accounts disabled unless they are necessary for proper operation of the system? **(21)**				
40. If the accounts mentioned in the previous question must remain enabled, are the passwords changed at least once every 90 days? **(21)**				

Verified per representation.
Verified per observation/examination.

State of Nevada
Gaming Control Board

CPA MICS Compliance Checklist

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
Administrative Access Note: Administrative access means access that would allow a user to: • Add, change, or delete user accounts and associated user provisioning • Modify operating system, database, and application security and policy parameters • Add, change, or delete system exception logging information • Add, change, or delete permissions to data files and folders				
41. Is access to administer the network, operating system, applications, and database security and system parameters either:				
a) Limited to supervisory and/or management employees of the IT department or IT employees under the supervision of supervisory and/or management employees of the IT department? **(22)**, or				
b) If there is no IT department, is it limited to supervisory or management personnel independent of the department using such system and/or application? **(22)**				
42. Are systems being administered enabled to log usage of all administrative accounts, if provided by the system, and, if so, are such logs maintained for 30 days and do they include the time, date, login account name, description of event, the value before the change, and the value after the change? **(23)**				
43. Daily, does an individual independent of the slot department review the requirements of a system based game and a system supported game to ensure the proper use of split or dual passwords by system administrators? **(24)** **Note 1:** MICS #24 requires a review to confirm that the system requires the use of split or dual passwords and that split or dual passwords have been used. **(24, Note)** **Note 2:** The requirements for split or dual passwords are delineated in Regulation 14, Technical Standards 1.084(4) and 1.086(4). **(24)**				
Backups				
44. Are daily backup and recovery procedures in place? **(25)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
45. Relating to the previous question, do the procedures in place, if applicable, include:				
a) Application data? **(25a)** **Note:** This standard only applies if data files have been updated. **(25a, Note)**				
b) Application executable files, unless such files can be reinstalled? **(25b)**				
c) Database contents and transaction logs? **(25c)**				
46. 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? **Verify by observation.** **Note 1:** 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 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. **(26, Note 1)** **Note 2:** MICS #26 does not apply to backup data files for computerized keno and bingo systems except for inter-casino linked keno games or keno games that accept multi-race keno wagers that will not be completed by the end of the next gaming day. **(26, Note 2)**				
47. Are backup system logs, if provided by the system, 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? **(27)**				

Verified per representation.
Verified per observation/examination.

Auditor's Name and Date

INFORMATION TECHNOLOGY
MICS #1 - #28

Licensee _____ Review Period _____

Questions	Yes	No	N/A	Comments, W/P Reference
48. 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? **(28) Verify by reviewing the documentation indicating the process. Additionally, confirm compliance with documented procedures.** **Note:** While not mandatory, licensees are encouraged to test recovery procedures at least annually. **(28, Note)**				
Written System of Internal Control				
49. Has the licensee's written system of internal control for information technology regarding the gaming department being reviewed been re-read prior to responding to the following question?				
50. Does the written system of internal control for information technology regarding the gaming department being reviewed 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.