Handout #4 – Exercise 2

Toolkit Exercise

Break into groups, working together read each scenario, and identify the issue(s) and locate the corresponding MICS standard using the IT Toolkit. Then write a finding and include a recommendation.

Scenario #1:

Vendor Z has an always on connection between their service center and the Class II server housed in the tribe's server racks. This connection has been approved by IT Security and by the Gaming Commission since 10/03/2012. The vendor has a staff of properly licensed database admins that utilize the connection to perform daily manual database backups and trouble shooting at the tribe's request. On 01/15/2014 Erik Magnus, the external auditor, asks for a log of all remote access to that server from 12/01/2013 to 12/31/2013. He is given a screenshot of windows usernames and logins for the time period.

MICS REFERENCE: _______________

FINDING:

____
____
____
____
____
____
____

RECOMMENDATION:

____
____
____
____
____
____

Handout #4 – Exercise 2

Scenario #2:

The IT Auditor reviewed the Casinos SICS, mapped the card access (ex. HID Card) and key control process. Based on review of the Casino SICS the Auditor noted that access to physical locations are controlled by a combination of two security measures; card access and physical keys. Both the card access and keys are controlled by software. The IT Manager has access to the key box software in order to change an individual's user group. Access to the card access software is limited to the IT Manager, General Manager and the CEO. The Auditor conducted an interview with the IT Manager and learned that card access is reviewed by the IT Manager when there is a change in job status (i.e. new hire, department transfer or termination). Additionally, an IT audit is performed twice a year. Further the Auditor also learned from the interview that access reports and logs exist within the card access software with no review occurring. However, the IT Manager does audit the key box access log on a weekly basis.

MICS REFERENCE: _______________

FINDING:

RECOMMENDATION: