KPMG

Report to the Shareholders

Atlantic Lottery Corporation – Control Review

January 24, 2008

Contents

1 Executive Summary

KPMG Forensic Inc. (KPMG) was engaged by the Shareholders of Atlantic Lottery Corporation (Shareholders) under the terms and conditions of our June 27, 2007 engagement letter to undertake a review of the following areas within Atlantic Lottery Corporation (ALC):

- Tickets (traditional scratch and national/regional shared lottery tickets)
- Video Lottery
- Break-Open Tickets
- e-Gaming (ALC's Online Gaming)
- Linked Bingo
- Charlottetown Driving Park Entertainment Center (CDPEC)
- Finance
- Marketing
- Distribution
- Procurement.

As outlined in our engagement letter of June 27, 2007, this engagement has been commissioned by the Shareholders of ALC to perform a broad scope business review to determine:

1) If appropriate controls exist within the various product categories operated by ALC to limit gaming integrity issues

2) If there are opportunities where controls could be adopted by ALC to derive additional operational or strategic value for its Shareholders.

Our review was limited to a point in time with our fieldwork starting principally on July 3, 2007 and ending principally on October 31, 2007. For certain elements of this review, we had to look to recent history for evidence of some controls and/or undertake sufficient investigation prior to formally developing our findings.

Since the end of our fieldwork, ALC Management has reviewed all of the findings, and met with KPMG to gain additional insight and context to our findings. They have provided their responses to our findings and recommendations as of January 24, 2008.

At a high level, our main focus on controls can be broken down into one of the following areas:

Segregation of Duties – refers to assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets and is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of the person's duties.[1]

Computer Configuration – refers to ALC's ability to set or limit controls within their IT controls to minimize the risk of unauthorized access, change or disruption of IT assets.

Documentation – refers to the formally retained records within ALC over each policy, procedure and relevant audit evidence supporting the existence and operations of each area.

Evidence of Approval – refers to ALC's ability to provide sufficient audit evidence that an event / action / comment or decision was made by the appropriate person(s) within the organization and that these actions were consistent with the stated ALC policies.

Monitoring Controls – refers to controls that identify and detect to ALC if a violation of a policy or procedure has occurred. These controls are essential to the lottery industry as it operates in a distributed sales model with a product that has inherently more risks of theft and compromise.

Compliance – refers to ALC's ability to adhere to its stated rules and regulations.

Policy / Process – refers to ALC's formalization of rules and regulations which it uses to monitor its operations in a consistent and appropriately controlled environment.

Overall Findings:

Based on the scope of our review and findings, we believe that the following items help reduce the overall risk to ALC and its Shareholders:

[1] Canadian Institute of Chartered Accountants –"General Assurance and Auditing Section 5141 - understanding the entity and its environment and assessing the risks of material misstatement"

- The senior management team of ALC has an appropriate mix of lottery business, operational and risk management professionals to ensure that risks are identified and dealt with in a complete and timely manner. Additionally, the risk management group within ALC, including Security & Compliance, has an appropriate staff compliment to operate ALC's new investigative processes.

- ALC has access to a broad collection of lottery specialists within its employee base, many of whom have more than 10 years of ALC specific experience. Furthermore, turnover of key personnel at ALC has traditionally been low, resulting in retention of much of this collective lottery industry knowledge.

- ALC is an early adopter of emerging technology that is aimed at increasing game integrity within the products they offer. Many of these emerging technologies i.e., self ticket checkers, requiring the player to sign their ticket prior to validation, use of pack-activation, etc., have been adopted by other Canadian lotteries and are now considered industry best practice.

- ALC has established controls for all business units, which are reviewed on a regular basis, and modifications made as required.

Based on the scope of our review and findings, we believe that the following items represent the most risk to ALC and its Shareholders:

- Notwithstanding the cash cage and casino game controls, which are consistent with industry practices, CDPEC appears to lack an appropriate control environment including a lack of roles and responsibility around ALC's oversight around technology, Security & Compliance and operations. Our findings point to an overall issue in the consistent application of controls within CDPEC, lack of appropriate oversight and monitoring controls and segregation of duties issues.

- ALC lacks consistent documentation standards in some areas resulting in incomplete audit evidence that the controls are working appropriately. Without this level of documentation, it is difficult to determine the extent to which ALC complies with its policies and procedures.

- ALC's e-Gaming environment contains some vendor related and configuration issues that weakened its general IT controls.

- A vendor related issue within ALC's secured backend gaming network resulted in an ability to capture sensitive information, from within a secured area of ALC's internal data center, during our testing procedures. While the exploitation of this risk would be highly remote, and would require collusion and a highly sophisticated computer user, ALC Management should review their compliance with both the credit card Payment Card Industry (PCI) and Personal Information Protection and Electronic Documents Act (PIPEDA) standards.

- We identified service offerings that are using older technology with less robust infrastructure, increasing the risk that known flaws could be used by a sophisticated computer operator to compromise ALC's systems or games. For example, we have noted that the lottery retail terminals are running end of life software and hardware which do not support the newest security enhancements available in the market due to the age of the equipment being used.

The tables below outline our findings of control deficiencies by findings type and scope area. The individual findings are outlined in the various sections within this report.

Finding Type	**Number of Findings**
Segregation of Duties	**4**
Computer Configuration	**15**
Documentation	**3**
Evidence of Approval	**5**
Monitoring Controls	**8**
Compliance	**8**
Policy / Process	**9**
Total	**52**

Scope Area	High Risk Findings	Medium Risk Findings	Low Risk Findings	Total
Tickets	**0**	**1**	**8**	**9**
Video Lottery	**0**	**3**	**2**	**5**
Break-Open Tickets	**1**	**0**	**2**	**3**
e-Gaming	**1**	**6**	**1**	**8**
Linked Bingo	**0**	**0**	**2**	**2**
CDPEC	**6**	**4**	**6**	**16**
Finance	**0**	**1**	**0**	**1**
Marketing	**0**	**1**	**0**	**1**
Procurement	**1**	**2**	**3**	**6**
Distribution	**0**	**0**	**1**	**1**
Total	**9**	**18**	**25**	**52**

Legend

High – Control deficiencies exist that have a higher likelihood of causing a game integrity issue, or represent significant break-downs in controls.

Medium – Control deficiencies exist that have a medium likelihood of causing a game integrity issue, or represent moderate break-downs in controls.

Low – Control deficiencies are not likely to cause a game integrity issue, or represent only small deviations from the stated controls.

The Management of ALC has reviewed our findings for factual accuracy, and has indicated that they accept all of the recommendations and have completed remediation of 27 of the 52 recommendations, and are working on an additional 25 of the 52 recommendations.

KPMG has not audited, reviewed or otherwise undertaken any steps to determine if the remediations by Management are complete, or appropriate to achieve our recommendations.

Our review was based only on the information provided by ALC and/or pertaining to ALC. We did not undertake to review similar issues within other lottery jurisdictions. This report and the comments and conclusions expressed herein are valid only in the context of the whole report. Selected comments or conclusions should not be examined outside of the context of the report in its entirety.

During our review, we were provided with all information requested by us and available to ALC. As well, ALC made available to us additional resources that we could use to further investigate and follow up on any items determined to be relevant. During our review we have not uncovered any acts or omissions of acts which we believe warrant disclosure. Additionally, we have not uncovered any acts or attempts by ALC, its senior management team or other related stakeholders, to alter or influence our investigation or the outcomes of this report.

Our recommendations are bench marked, where appropriate, on KPMG's collective experience in assessing generally accepted best practices within other lottery and/or casino organizations for which KPMG has undertaken similar reviews. Additionally, we have reviewed the finding reports of similar undertakings in other lottery jurisdictions that are publicly available.

2 Limitations and Restrictions

This report has been prepared for the sole use of the Shareholders in determining:

1) If appropriate controls exist within the various product categories operated by ALC to limit gaming integrity issues

2) If there are opportunities where controls could be adopted by ALC to derive additional operational or strategic value for its Shareholders.

We have had access to the information as set out in each scope area of this report in order to arrive at our conclusions, but should additional documentation or other information become available which impacts upon the conclusions reached in our report, we will reserve the right, if we consider it necessary, to amend our findings accordingly.

This report and the comments and conclusions expressed herein are valid only in the context of the whole report. Selected comments or conclusions should not be examined outside of the context of the report in its entirety.

KPMG has not audited, reviewed or otherwise undertaken any steps to assess the design, implementation, nor operational effectiveness of management actions, as described in their management comment responses.

For any avoidance of doubt, our report and related schedules (if any) may not be disclosed, copied, quoted or referred to in whole or in part, by anyone whether for the purposes of litigation, disciplinary proceedings or otherwise, without our prior written consent in each specific instance. Such consent, which will be reasonably given, may be on conditions, including without limitation an indemnity against any claims by third parties arising from release of any part of our report and related schedules.

We will not assume any responsibility or liability for any costs, damages, losses, liabilities or expenses suffered by ALC, or its Shareholders as a result of circulation, publication, reproduction, use of or reliance upon our report and related appendices contrary to the provisions of this section. We will not assume any responsibility or liability for any costs, damages, losses, liabilities or

expenses incurred by anyone else as a result of circulation, publication, reproduction, use of or reliance upon our report.

The comments and findings in our report are not intended, nor should they be interpreted to be legal advice or legal opinion.

3 Scope and Objectives

As outlined in our engagement letter of June 27, 2007, this engagement has been commissioned by the Shareholders of ALC to perform a broad scope business review to determine:

1) If appropriate controls exist within the various product categories operated by ALC to limit gaming integrity issues

2) If there are opportunities where controls could be adopted by ALC to derive additional operational or strategic value for its Shareholders.

For each of the product offerings outlined in the Executive Summary, we have conducted interviews with key ALC employees, reviewed relevant documents, and performed specific review procedures to determine the existence and operational appropriateness of the various controls within ALC. We have also interviewed and performed limited walkthrough testing of controls at various key vendors to ALC and within the Interprovincial Lottery Corporation (ILC).

Where we have identified areas of control deficiencies, we have reviewed our findings with the management of ALC pursuant to normal practice and as authorized by the Shareholders. This validation was taken to ensure that additional controls were not available to address the risks and that management agreed with the risks identified.

Additionally, during the course of our review, we have interviewed and/or discussed the recently revised retailer winning investigation and customer complaint processes with the individuals that we considered relevant to our review. We were assisted by other individuals in ALC's Internal Audit, Security & Compliance, the various business units and IT support in collecting data and additional support materials.

A glossary of terms and definitions used within our report is included in Appendix A.

4 Entity Controls Relating to Tickets

Tickets are the traditional lottery service offering by ALC and are sold throughout Atlantic Canada through ALC's Lottery Retailer Network (LRN). Games include both national online games such as Lotto 6/49 and Scratch'n Win tickets.

This product offering represents the majority of the lottery products offered by ALC and includes the following two main types of tickets:

1. Scratch tickets which require the player to scratch off security latex from the ticket face to determine if the ticket is a winning ticket. With the scratch ticket products, a player will know instantly if and the value of what they have won. Winning ALC tickets can result in free product, monetary awards and / or tangible assets for the players.

   ALC has two main suppliers of instant scratch tickets and several Lottery Retail Terminal (LRT) and supporting infrastructure i.e., paper, ink, consumables, suppliers; however, the processes around game development, integrity and prize payout are the same within each. Our review covered the various controls within each specific product line.

2. Online tickets are offered as part of a national or regional "pari-mutuel", some within a shared pool and prize distribution. Several of these games are operated in connection with the Interprovincial Lottery Corporation (ILC) which acts as a clearing house for the various lotteries within Canada who participate in these games. The online tickets are sold through retailers who have a LRT.

4.1 Approach

We examined various controls within each gaming product including the design phase controls, interactions between gaming vendors and ALC, prize payout calculation and integration with the central gaming system AEGIS, which is used to track all available tickets. Additionally, we examined both technical controls around the LRT network and the various control files provided by scratch ticket vendors that get uploaded to the backend AEGIS system to allow for centralized ticket validation.

For the scratch tickets, we specifically reviewed:

- Ticket design and development
- Ticket testing and quality assurance
- Ticket production
- Ticket distribution (covered below in a separate section)
- Ticket validation
- A review of a Section 5970 (as governed by the handbook of the Canadian Institute of Chartered Accountants) report provided by the external ticket vendor which provided an independent assessment of the production controls.

For the online traditional games (such as LOTTO 6/49), we examined:

- The IT general controls around the LRN including:
    - Change controls
    - Logical access controls
    - Monitoring controls
    - Backup and recovery controls
- Network design and data encryption
- Physical security of the LRTs
- Monitoring controls in place to ensure that any processing deviations, unauthorized access or other remote events are identified.

The distribution and marketing of scratch tickets have been reviewed in separate sections of this report.

4.2 Evidence Reviewed

Our review was carried out on information, evidence and records obtained from ALC directly or through interviews with staff of ALC.

4.3 Findings, Recommendations and Management Comments

We noted the following items which we believe **reduce** potential risks around Tickets:

- ALC has an in-house testing facility that is used to assess the security of scratch, Break-Open and online tickets, including production techniques, ticket stock, ink, latex and built in security features.

- ALC's testing lab is equipped to test for ticket paper, ink and latex related quality issues, randomness of winner distribution, and for testing the various security controls built into the ticket games.

- Over the last 12 months, ALC has implemented additional controls around the investigation and monitoring of winners of all ticket products.

- ALC has hired individuals who are tasked with additional Security & Compliance activities that further allows for analysis of identified LRT issues.

- ALC's LRT network is a stable environment which they have been operating for many years. As such, the internal expertise around the monitoring and operating of the LRT is well defined and issues are identified and remediated in a timely fashion.

- ALC has well defined processes around the maintenance and support for the LRT network.

High Risk:

We have no high risk findings.

We noted the following items which we believe **increase** the potential risks around Tickets and, as a result of our review, we offer the following recommendations for consideration:

Finding # 1 - Medium Risk

Notwithstanding the various controls within the 'pack activation' processes in place within ALC, certain Lottery Support Services (LSS) staff at ALC can activate the tickets remotely in the event that a non-activated ticket were somehow distributed and presented as a winner. The process by LSS of activating the individual ticket will result in all tickets within the original ticket pack being activated. Furthermore, the activation will appear as if the retailer who was assigned the ticket package was the one who activated it.

Typically, a ticket pack is activated at the retailer level prior to displaying the ticket for sale. The pack activation process is a key revenue recognition trigger for ALC and allows ALC to mitigate its risk on shipping live tickets to retailers. The current LSS process could result in lost, stolen, or otherwise obtained inactive tickets being activated within ALC's game system, and the tickets eligible for prize pay outs. Furthermore, future investigations would not identify the tickets as activated by LSS.

Recommendation # 1

We have recommended, and ALC is investigating their ability to implement, limitation of the pack activation process to individuals within ALC. ALC is ensuring that this level of activation by individuals within ALC, and not the retailer, is limited and that each occurrence of activation by proxy is documented and approved.

Management Comments # 1

Management accepts this recommendation - Complete

As per the standard practice at ALC, the pack activation process is limited to our retailers and specific individuals internally who work in the distribution department. Lottery Support Services only has the ability to activate packs that are in the "received" status by the retailer. For all activating transactions, an existing audit report is in place which records both internal users by their user id, as well as external users by their retailer id.

A modification was made to the report to now include LSS user ids. Lottery Support Services is responsible for submitting tickets to Security & Compliance (SCMS) for every instance of retailers selling tickets from packs that are not activated since this is a breach to the retailer policy. Prior to activating received packs, LSS also checks for previous logs of stolen tickets. This process has

been in place since the distribution of the retailer policy in September 2007. Additionally, LSS logs all calls in which a store is not able to validate a ticket.

Finding # 2 – Low Risk

The LRT network connection on the retailer side used to connect the LRT unit to ALC's backend system could be used by an individual with an unauthorized computer to gain some level of access to the central gaming system network. Such access could result in game or system disruption.

Recommendation # 2

We recommend that ALC implement additional controls within the LRN to ensure that only authorized computers are connected. ALC should consider enforcing Media Access Control (MAC) address filtering, or other similar logical access restrictions, whereby a known unique identifier for each LRT unit would be required for access to the LRN. This would require the connecting computer to have pre-established configurations which ALC could use to enforce only known machines to the LRN, thereby Monitoring for end-point compliance within the LRN.

Management Comments # 2

Management accepts this recommendation - Complete

ALC agrees this control provides additional security in many circumstances and where unacceptable risk levels exist. ALC's multi-layered protection of defense in depth includes encryption, proprietary communications, firewalls, intrusion detection systems and 7/24 monitoring. ALC will assess the viability of MAC addressing filtering, or similar logical access restrictions at the end of the current LRN and LRT asset lifecycle.

Finding # 3 – Low Risk

The LRT machines are physically secured using locks that are easily compromised and once access is gained to the LRT, access to the LRN can be gained without ALC's knowledge.

Compounding the issue, we have noted that no active central monitoring occurs when the LRT case is opened as this event is currently only logged to the local LRT hard drive. Furthermore, once opened, an individual can gain unauthorized access to the operating system of the LRT by attaching a keyboard to the internal computer components.

We have noted that ALC has mitigated this risk to some degree by using encryption; however, with sufficient time, a sophisticated computer operator could break this encryption and further access the LRN.

Recommendation # 3

ALC should review with the vendor of the LRT units, the ability to increase the relative strength of the locks currently in use to limit the risk of unauthorized physical access. Additionally, we recommend that ALC include additional processes to ensure that all door open activities to the machine are monitored for appropriateness centrally by LSS.

Management Comments # 3

Management accepts this recommendation - Complete

ALC, on a daily basis, verifies remotely the software version of each LRT, and if any non-compliance is detected, the terminal is replaced. This provides a detection mechanism for possible tampering of the LRT software.

In addition the current LRTs will be replaced. ALC will be issuing an RFP in Q4 2007/08, for the purchase of new LRT and the new system is planned to be rolled-out by late 2009. The physical security requirements of this new terminal will be enhanced to limit the physical access and all access will be monitored centrally.

Finding # 4 – Low Risk

When the ticket printers send the game file with the winning ticket numbers to ALC, the game file is sent encrypted to ALC. This is the minimal amount of security that could be implemented and once received by ALC we have noted that it sits in a corporate area that is accessible to most ALC employees. This file remains on the ALC network until ALC receives the game design working papers and the email from the printer confirming the transfer. The file is subsequently uploaded to the gaming network so that tickets can be activated and validated. By not enforcing strict logical access security to the game file within the ALC network, there is an increased risk of unauthorized access to the file by individuals who do not need to access these files.

Recommendation # 4

We have recommended, and ALC has started to implement, a review of the logical access to the game winning files provided by the ticket vendors, and subsequently loaded into the secure central gaming system to allow for online validation of tickets. We have noted that the loading process is restricted to a very limited group which is appropriate, and believe that the access to the underlying files should be similarly restricted.

Management Comments # 4

Management accepts this recommendation - Complete

The underlying game files have been restricted to only those ALC resources that have access to the loading process. This is a very limited group, which KPMG has stated as being appropriate within their recommendation.

Finding # 5 – Low Risk

When a person purchases a scratch ticket, the prize distribution is based on the entire lot of tickets and not what is distributed. We recognize that it is neither feasible nor practical that all tickets be distributed and available for potential purchase after production. As such, a disclaimer should be included. Currently, the ticket does not have a disclaimer to note that the prize distribution is over the entire production of tickets and not the amount of tickets in circulation at the time.

Recommendation # 5

We recommend that ALC change the wording on the back of all tickets to include a disclaimer that the prize payout values are based on the overall ticket production and not the actual tickets that have been distributed and activated in the retail distribution chains. Furthermore, ALC's legal group should ensure that this same (or similar wording) is available on the various ALC websites and literature.

Management Comments # 5

Management accepts this recommendation - Complete

For all games on a go-forward basis, the wording on the back of the ticket has been changed, as noted by KPMG, on all instant and Break-Open tickets. The new wording is "Total overall prize payout for xxx game is approx. xx%. Overall chances of winning are approximately 1 in xx."

Finding # 6 – Low Risk

Tickets are currently tested for adherence to the game design work papers, production quality and appropriateness of the security features required, by only one skilled person within the testing department of ALC. Having one internal resource for this testing could result in a potential issue if that individual leaves or is unavailable. ALC has other individuals who historically have done some ticket testing, but would not be as knowledgeable about emerging security risks associated with scratch or Break-Open tickets.

Recommendation # 6

We recommended and ALC has identified additional resources that can be appropriately trained and used in the ticket testing processes. ALC should also develop a process to ensure that all their ticket testing resources remain current on industry best practices and emerging ticket testing approaches.

Management Comments # 6

Management accepts this recommendation - In process

Security & Compliance have a trained back-up resource to be used in the ticket testing process. The Manager of Integrity and Compliance, to whom this resource and the Ticket Testing Lab resource report has assessed the current state of training and arrange for further training was completed.

On a go-forward basis, Security & Compliance will implement a protocol of communication and continuous transfer of knowledge between the Ticket Testing Lab and alternate resources to remain current on industry best practices and emerging ticket testing approaches.

Finding # 7 – Low Risk

The lab where instant tickets are tested is a controlled environment as a result of having live tickets, testing documentation, sophisticated equipment and game design working papers. We have noted access is very restricted within ALC, except after hours, when building facilities personnel have

access for emergencies. However, it is not clear that after-hour access is monitored or followed up for appropriateness.

Recommendation # 7

We recommend that ALC implement a process whereby non-authorized after-hour access to the ticket testing lab be monitored for appropriateness and followed up to identify the nature of such access by building personnel.

Management Comments # 7

Management accepts this recommendation - Complete

While current controls were sufficient to manage the noted risk, a formalization of the monitoring process was necessary to demonstrate evidence of process compliance.

The Physical Security group within Security & Compliance is monitoring access logs on a daily basis to detect after hour access to the ticket testing lab. The monitoring of the access logs is a day to day operational component of a recently hired physical security resource under the supervision of the Manager, Physical and Information Security. Any occurrences of unauthorized access are logged as an incident and investigated by Security & Compliance.

Finding # 8 – Low Risk

We have noted that when a retailer calls LSS for a LRT password, either a new one or reminder of the current one, LSS confirms the contact name and provides the password. LSS does not consistently verify the contract number or other information. As a result, there is an increased chance that the password could be divulged inappropriately. This could result in unauthorized access to the LRT units and the various reporting screens on the LRT for that particular location.

Recommendation # 8

We recommend that ALC alter their current processes for LSS to require additional information prior to issuing the retailer terminal password. Additionally, we recommend that, if this information is requested, ALC contact the individual outlined in the retailer contract (or designate) prior to providing this password. Furthermore, it would be prudent for LSS to provide a follow up call the

next day to the main contact advising of this request, thereby allowing the retailer to ensure that their password was only given to authorized individuals.

Management Comments # 8

Management accepts this recommendation - Complete

Lottery Support Services will only give the LRT passwords to the contact person(s) listed in RDMS as authorized contacts. Lottery Support Services current process is also to ensure that the contact person(s) have the retailer ID as part of the verification process. As for new installs/change of ownerships, these contacts would not have their agent number (or retailer ID); however, the BDM is always present to provide training.

Lottery Support Services will also implement a new process of providing a follow up call within an hour to the main contact advising them of the request for their LRT password. This process was implemented on December 14, 2007. All follow up calls are tracked in LSS call log system. Also, to help ensure LSS are able to reach the appropriate contact they do not identify themselves when completing the call back.

Finding # 9 – Low Risk

We have noted that the LRTs use encryption to communicate with the backend game servers located within ALC's datacenters from a LRT site. The version of encryption used is known to be a weak method of encryption for data and can be easily deciphered using existing technologies and methodologies. In the event that the encryption is broken, it would be possible for a sophisticated computer operator to attempt to perform advanced computer attacks. This could ultimately result in a disruption to the LRN machines, or games.

Recommendation # 9

We recommend that ALC work with the vendor of the LRN protocols to implement a more robust encryption process than the current encryption method. If the older LRT terminals do not support the use of a more robust encryption process, we recommend that ALC review the need for more robust LRT units that are capable of handling additional safeguards.

Management Comments # 9

Management accepts this recommendation - In process

The protective mechanisms currently employed by ALC provide a multi-layered defensive protection for the online gaming system. This multi-layered protection of defense in depth included encryption coupled with proprietary communications, firewalls, intrusion detection systems and 7/24 monitoring.

ALC is currently reviewing the enhanced requirements for the communication front end services which include stronger encryption. This review will be completed by March 31, 2008.

5 Entity Controls Relating to Video Lottery

Video Lottery is a product which provides an interactive playing environment for patrons of approved establishments who play the game(s) at a Video Lottery Terminal (VLT). ALC has a series of responsible gaming initiatives built into the various VLTs in the wide area gaming network to ensure that patrons are aware of the risks and available resources for responsible gambling. The VLT program in Atlantic Canada offers a variety of games including line games, poker games, and keno games.

Key areas of controls include:

Placement

Placement of VLTs in the wide area gaming network is subject to a series of minimum site considerations, an on-site visitation by a VLT technician and/or Security & Compliance, background and other subjective tests for the potential retailers, and final acceptance of the VLT site approval committee.

Operation

The VLT units, excluding those at the Charlottetown Driving Park Entertainment Center (CDPEC), are centrally managed by ALC which uses its centralized testing lab facilities to test and approve software configuration and games prior to placement within the wide area network. Once approved, the changes are pushed to the VLTs remotely and/or physically imprinted on a microchip for physical distribution through the VLT technician group.

All approved changes are encoded into a start up routine that is forced to run daily on all VLTs in the wide area network that performs automated code comparisons to ensure that integrity of the software code running on the VLT units have not been compromised or subject to unauthorized changes. This approach ensures that the VLT machines are running approved games and are configured according to defined standards. Additionally, this supports the concept of appropriate segregation of duties within ALC as the individuals tasked with maintaining the VLT units are not the same group that is configuring and approving the various software and games being played through the VLTs.

Monitoring

All VLT gaming activities in the wide area gaming network are collected to the Video Site Controllers (VSC), which are linked to the Enterprise Series Video (ES Video) backend system. This allows for Lottery Support Services (LSS) to poll information about the various games that were played and any issues that were encountered. Additionally, LSS acts as a monitoring group for all alarms or issues within the VLT units and is responsible for the monitoring of VLT technicians activities on a particular VLT unit.

The monitoring capabilities of the LSS include various VLT alarms, i.e., unauthorized VLT access, printer issues, abnormal termination of games, etc., and are used to dispatch and ensure that VLT technicians are performing authorized service or upgrades to a VLT in the wide area gaming network.

5.1 Approach

We have examined VLTs in the wide area gaming network to ensure appropriateness and application of policies, procedures and technical infrastructure.

Specifically, we have reviewed the following items:

- Game development life cycle
- Testing and change management of software and configurations within the VLT environment
- Appropriateness of the random number generator used on the VLT to operate the game
- Prize payout and redemption configuration and processes
- Physical placement of the VLT units
- Oversight and monitoring of VLT activities in the wide area gaming environment.

5.2 Evidence Reviewed

Our review was carried out on information, evidence and records obtained from ALC directly or through interviews with staff of ALC.

5.3 Findings, Recommendations and Management Comments

We noted the following items which we believe **reduce** potential risks around Video Lottery:

- An appropriate segregation of duties between the VLT technicians and the individuals that test and approve changes to the VLT configuration and software is well defined and implemented.

- Daily, ALC forces a 'polite shutdown' for all ALC operated VLT units in the wide area gaming network to enforce hours of operation. ALC initiates an automated routine to verify the integrity of the software on the VLT logic boards, on at least a daily basis or if other system defined events occur.

- ALC maintains an effective physical inventory of all sensitive parts used within the VLTs and has implemented the use of validation routines that ensure the software within the remote VLTs is consistent with the ones registered centrally and that no changes have been made to these chips.

- ALC has defined placement standards which must be met for all potential VLT locations prior to the final VLT placement. These standards include a placement committee which reviews various aspects of the potential site including segregation from public areas, consideration against potential access by minors, and appropriate physical security of the VLT units. The outcomes from these placement meetings are retained as a component of the VLT placement agreement.

- All VLT units are equipped with remote alarm units referred to as Program Validation Disable (PVD) alarms that must be investigated by LSS. This centralized monitoring allows LSS to identify issues within the wide area gaming network that could be the cause of system failure or human intervention. In the event that LSS identifies an unauthorized access to the VLT unit, they have the ability to dispatch a VLT technician, reinstate play on the unit, or increase the monitoring around that VLT's operations.

- All maintenance work to be performed to a VLT is centrally managed, resulting in an enhanced level of logging of all VLT activities in the wide area gaming network. This also results in VLT technicians being assigned jobs centrally, thereby increasing the level of segregation between the technicians and the VLT retailers. This is an important control as it limits the ability for collusion between a VLT retailer and a technician to circumvent controls.

- ALC uses serialized tamper-proof plastic seals to alert a VLT technician of unauthorized access to a VLT logic boards. The seal serial number is maintained by LSS and is the first control that the VLT technician confirms if dispatched for service. Once removed, the seals cannot be re-used thereby providing a control against unauthorized changes to the VLT logic boards.

High Risk:

We have no high risk findings.

We noted the following items which we believe **increase** the potential risks around Video Lottery and, as a result of our review, we offer the following recommendations for consideration:

Finding # 10 – Medium Risk

We have noted that prize validation codes which are printed on tickets and used as a key control within the prize validation process are available to a large number of employees within ALC. These individuals do not appear to have a business need for this access, and we perceive a further conflict as they also have access to the list of non-claimed winning tickets. We believe that an individual with access to these files could use the information contained in these file to create and cash a ticket that has not been previously collected within seven days. To do this an individual would need to identify the specific bar code and font used by the VLT printer units, a roll of ALC paper stock and a thermal printer. The needed elements could be obtained with little advanced skills.

Recommendation # 10

We recommend that ALC implement stricter access controls over who has access to prize validation codes within the system. Specifically, we recommend limiting access to the ES Video Unclaimed Ticket report. It has been noted that ALC's Security & Compliance department are currently reviewing access to this report and will be restricting access to a small number of authorized ALC employees.

Management Comments # 10

Management accepts this recommendation - Complete

In April 2007, ALC implemented a maintenance upgrade of ES Video which provides the ability to ALC to limit access to certain functionality, including the access of unclaimed prize validation

numbers. The current risk is limited to 7 days, after which the holder must present himself at ALC for redemption. Security & Compliance is currently reviewing access and will be recommending restricted access by January 15, 2008.

Finding # 11 – Medium Risk

The VLT Protocol Standard document is defined and maintained within a central document owned by the game vendors. As such, the vendors make all decisions on modifications and distribution; however, each decision could impact ALC's VLT operations. This document details how a VLT talks to the central system at ALC and is used by all vendors who create games for use on VLTs. It could, however, be used to target and create potential applications that could be used inappropriately. We have further noted that there appears to be no audit trail of the distribution of the document.

Recommendation # 11

We recommend that improved controls over the distribution of the VLT Protocol Standard document be implemented. We recommend that due to the sensitive nature of the information contained in the document that a proper audit trail and sign-off of the initial receipt of the document be kept.

Furthermore, we recommend that, as changes to this document are made, the vendor provides all registered recipients the revised document to ensure that the changes are known and appropriate. ALC should work with the vendor to ensure that any particularly sensitive elements of the document are appropriately restricted from distribution unless formally requested and approved.

Management Comments # 11

Management accepts this recommendation - Complete

In the standard process, ALC notifies its gaming suppliers of approved vendors and authorizes them to release the document to that vendor once an NDA is signed between the vendor and the registered recipient (Approved Vendor).

As of January 15, 2008, ALC established a process with the vendor and registered recipients providing a proper audit trail and sign-off of the issuance and receipt of the document. The same process will be used for any Protocol Standard updates.

A copy of the signed NDA and an "Acknowledgement of Receipt" of the Protocol Standard shall be provided to ALC by the registered recipient(s).

Finding # 12 – Medium Risk

We have observed that LSS currently provide retailers unknown validation codes over the phone to allow for manual validation of a ticket that is damaged and cannot be automatically validated for some reason. In addition to the ability to obtain the validation code, each retailer has access to a report listing all tickets not paid out at their site including the actual ticket number. With these two pieces of information, an individual could manually validate and cash out these unclaimed tickets with limited detection.

Recommendation # 12

We recommend that all damaged tickets or tickets that cannot be automatically validated be forwarded to ALC for investigation and follow-up. This will allow ALC to closely control the validation controls and track the payouts of these tickets for any inappropriate trending.

Management Comments # 12

Management accepts this recommendation - Complete

Since September 15, 2007, LSS no longer provides validation numbers to the retailers. Also, the retailers do not have access to the un-validated ticket numbers. Only the last ticket can be re-printed. If the last re-print is not available, any unreadable ticket or damaged ticket is sent to ALC head office with a prize claim form.

The accounts payable department will review the terminal accounting system to ensure the prize claim is valid. In addition, the next system release will result in LSS not being able to access or view the validation numbers.

Finding # 13 – Low Risk

For each VLT site, there is a video site controller (VSC) that runs a Linux operating system which collects video lottery playing data from the VLT units and transmits this information back to ALC. The VSC is currently running an older version of Secure Socket Shell (SSH) protocol to add a layer of security within the communication processes between the site and ALC. This protocol is known to contain vulnerabilities which could be exploited by a sophisticated computer operator. Additionally, the VSC only has limited accounts defined which leaves the system potentially vulnerable to increased susceptibility to a brute force attack.

Recommendation # 13

We recommend that the SSH protocol be enabled only during special circumstances where ALC requires remote command-line access to VSC. We also recommend that ALC, in conjunction with their vendors, review the version of SSH installed on the VSC and install the most up to date version. Additionally, we recommend that ALC implement MAC address level access controls whereby a known unique identifier for each VLT unit is required for access to the video lottery network. This would eliminate the potential for unauthorized access and limit network access to authorized VLTs and related ALC systems.

Furthermore, we recommend ALC implement an additional local account that can be used to initially access the VSC remotely from ALC's network so that the administrative account is not accessed directly. If this is not technically feasible, we recommend that ALC explore with the VSC vendors the use of the Switch User (SU) or SuperUser Do (SUDO) Unix commands that can be used to better control the use of the administrative account and provide additional audit log functionality. These logs could then be monitored centrally for appropriateness.

Management Comments # 13

Management accepts this recommendation - In process

ALC has previously identified this issue with the Vendor and has had discussions to assess the possibility of upgrading the remote access software. A change request has been placed with the vendor.

ALC will review the remote access software configuration of the VSCs and ensure that all hardware, where remote access is not required, will be disabled. This review will be completed by January 31, and changes which require site visits will be implemented by March 31, 2008.

Finding # 14 – Low Risk

There is limited oversight or validation for consistency of responses to questions regarding the operations of the VLT units. Currently each of the queries and responses is retained through ALC's helpdesk system. There is, however, no requirement to search other closed tickets for previously provided answers or issues. This process improvement could streamline VLT investigations and ensure a consistent message for each call.

Recommendation # 14

We recommend that ALC periodically review the closed helpdesk tickets to ensure that all known VLT issues are consistently documented and resolved. Additionally, as any trends emerging about VLTs are identified, the VLT technician group should be made aware of all known issues. This could result in more efficient knowledge sharing and more robust customer service.

Management Comments # 14

Management accepts this recommendation - Complete

As per standard process, on the operational side, the Field Service Managers and Supervisors are required to review a sample of call logs on a weekly basis to ensure completeness and accuracy of data. Also, the CHATS system (used to record and track VLT problems) is reviewed to determine trends and frequency of problem areas. The Field Service Managers review reports that are produced monthly on the top problems with the various VLTs in the field.

This information is also shared with individual supervisors/technicians. LSS also consistently trends top call drivers as part of their weekly/monthly reporting in order to identify issues and ensure they are consistently communicated. LSS also does call monitoring evaluations on all LSS staff to ensure that consistent service is given to all customers as well as the accuracy of the information documented in CHATS. Each LSS staff is monitored on 4 calls per month as part of their performance management.

6 Entity Controls Relating to Break-Open Tickets

Break-Open tickets are a form of instant tickets that are provided within retail outlets that are meant to be played immediately.

Break-Open tickets are not subject to the same redemption policies of ALC on other tickets as the winning Break-Open tickets must be returned to the original retailer for redemption. If the vendor is unknown for various reasons, i.e., received as a gift, ALC can arrange for payment of winning tickets centrally after which they invoice the selling retailer.

There is a difference in the Break-Open products in comparison to traditional ticket or online games offered by ALC, primarily as a result of the prize structure. The prize structure and profit margins for Break-Open tickets are standard within each box and in addition all winners must redeem their prizes with the selling retailer. It is possible to determine if the sale of the remaining tickets in a box is less than the remaining prizes in the box. As such, it may be more advantageous to forego the sale of the remaining tickets. This is referred to as "dumping" within the lottery industry and ALC has policies, procedures and controls in place to minimize this. The design issues noted with the prize payout and distribution model are not isolated to ALC, but rather, are the fundamental play mechanics of Break-Open tickets for all lotteries offering this product. However, the risk will only be fully minimized if Break-Open tickets are distributed in the same manner as other ticket products, with the prize structure being defined over the whole ticket run and redeemable within any ALC retailer.

6.1 Approach

We have reviewed the controls around the new game development and observed through an onsite visit with the vendor the controls by the vendor around the following areas:

- Ticket development and design
- Ticket testing and pre-production run validation
- Ticket printing and randomization
- Ticket packaging, storage and shipment to ALC.

Additionally, we have reviewed other controls with the retail locations to address general issues that were historically associated with Break-Open tickets, such as Break-Open box dumping.

6.2 Evidence Reviewed

Our review was carried out on information, evidence and records obtained from ALC directly or through interviews with staff of ALC.

6.3 Findings, Recommendations and Management Comments

We noted the following items which we believe **reduce** potential risks around Break-Open lottery tickets:

- ALC's primary vendor of Break-Open tickets has a new plant that has been ISO 9001 certified as a result of its processes and production approaches.

- The packaging processes used by the vendor results in the winning Break-Open tickets to be distributed within various areas for each box, i.e., pseudo random placement.

- The printing process involves a print press technology that requires individual non-reusable print plates be created for each individual run. These print plates are manually reviewed by the vendor and ALC to ensure that the games conform to ALC game specifications.. These plates are retained as a component of the game files by the vendor to allow for future investigations.

- ALC performs a series of manual tests of the Break-Open ticket files and associated proof sheets to ensure random distribution of winning tickets within a print run, the number of winning tickets is consistent with approved game design, and that winning tickets can only be identified once opened.

- ALC has undertaken a physical review of the production processes. On a regular basis, ALC reviews controls within the production facilities of the vendor of their Break-Open tickets.

Medium Risk:

We have no medium risk findings.

We noted the following items which we believe **increase** the potential risks around Break-Open tickets and, as a result of our review, we offer the following recommendations for consideration:

Finding # 15 – High Risk

ALC's Break-Open tickets do not have a signature line or bar code similar to their other tickets. As a result, the recently applied controls for online and Scratch'n Win products, i.e., signature line and self checker units, cannot be used with the Break-Open tickets. Additionally, without a system validation barcode, it is not possible to have the ticket validated centrally, which could result in a player not fully understanding the prize amount that they should receive.

Recommendation # 15

ALC should implement an appropriate mix of security features that are available, i.e., customer signature line, validation code which could be used to validate the ticket centrally, various security watermarks, and the wording 'WINNER' on each winning ticket in order to meet the spirit of other recently introduced customer protection controls.

Furthermore, ALC should review the feasibility of changing the payout process so that Break-Open tickets could be cashed at any ALC retailer site.

This may require ALC to operate as a clearing house for Break-Open tickets not cashed at the selling retailer using the technology and finance related processes already in place. It may, however, not be administratively appropriate given the work effort involved which is currently unknown. By allowing individuals to cash their Break-Open tickets at any location, ALC may lead the lottery industry in a new control over Break-Open tickets and may further reduce the risk of dumping, while not altering the defined profitability for the vendor on each box.

Management Comments # 15

Management accepts this recommendation - In process

As per standard process, the retailers must follow a minimum fill line policy on the bins to mitigate any manipulation of the prize structure. Additionally, the Break-Open winning tickets have text "Winner" on the inside of the ticket to clearly identify a winning ticket by the player. Marketing will continue to include game information cards with each box of Break-Open tickets, reminding retailers to deface the ticket after validating a prize.

In addition to the current controls Marketing is aggressively investigating technologies with its supplier to further enhance the integrity of these products and will provide a full and detailed action program by the end of March 2008. The review will include printing enhancements including bar coding, signature lines as well as the identification of dispensing distribution opportunities.

Finding # 16 – Low Risk

ALC's vendor of the Break-Open tickets uses a proprietary computer application that randomly distributes the various symbols and prize structure on the ticket printing plates. This program is currently maintained and modified by the original programmer with limited oversight or testing by other individuals at the vendor or within ALC. This results in a segregation of duties issue whereby the programmer could make unauthorized changes to the random distribution application. This would only be picked up during a manual validation of the pre-print plates and game design review by ALC.

Recommendation # 16

ALC should require their vendor to implement appropriate change management and software testing procedures for all changes to the application used to randomize the tickets. ALC should require that the version of the random distribution application be noted within the game working papers. Furthermore, ALC should ensure that the integrity of the application is tested for unauthorized changes prior to each ticket run by comparing a known version of the application code to the one used for the particular game. This would provide an additional layer of controls within this process and mitigate the risk associated with a manual review of the game print plates.

Management Comments # 16

Management accepts this recommendation - In process

Management will work with Break-Open suppliers to facilitate a review of key applications used in the manufacturing process.

The following provide the standard controls that have been in place for each new Break-Open game. Before a game goes to press, the color proof sheets for the set of printing plates, are confirmed to have: the correct prize structure of winning tickets; the correct security codes on the tickets; and the correct symbol arrangements to correspond to winning/non winning windows.

Additionally, for each new game after manufacture, the ticket testing lab performs a Ticket Distribution test on randomly selected units to confirm: 1) winning tickets are randomly distributed within units; 2) the correct numbers of each prize level winner are present in the units; and 3) winning tickets cannot be identified before opening them. During the manufacturing process, tickets are shuffled prior to being packaged. This step in the process overcomes any deficiencies that could be present in the randomness of placement on the printing plate of winners. In conclusion, defects in the computer program would be identified during lab validation of the color proofs, which show the position and symbol arrangement of each game side on each sheet's plate. Finally, manufactured units are confirmed to have randomly distributed winners and the correct number of winning tickets in each

Security & Compliance has written a letter to the ticket vendor requesting that these requirements be implemented and their timeline for doing so. Security & Compliance has requested a response from the vendor by January 28, 2008.

Finding # 17 – Low Risk

We have noted that ALC does not require the Break-Open tickets it procures to have been subject to random distribution applications that have been independently reviewed by a certified testing lab. As a result, additional substantive manual procedures need to be performed each production run to ensure that the distribution of the symbols on the tickets is random. This process is a time consuming manual process that could be minimized if the randomness of the application was independently verified.

Recommendation # 17

ALC should ensure that the applications used to produce the Break-Open tickets ALC procures are independently reviewed by a certified application testing lab that has other lottery experience. The testing on the applications should ensure that the random distribution code is truly random and that the code logic is appropriate and secure.

Management Comments # 17

Management accepts this recommendation - In process

ALC believes that strong controls are available to mitigate this risk as outlined in response number sixteen. Management will work with their suppliers to facilitate a review of key applications used in the various manufacturing processes.

Security & Compliance has written a letter to the ticket vendor requesting that these requirements be implemented and their timeline for doing so. Security & Compliance has requested a response from the vendor by January 28, 2008.

7 Entity controls relating to e-Gaming

e-Gaming is ALC's Internet distribution channel where ALC lottery products can be purchased through the main gaming website www.playsphere.alc.ca (Playsphere) and www.spheredejeu.alc.ca (French version). Playsphere is a secure site requiring player registration through the ALC player portal eClub. e-Gaming is limited to individuals within ALC's jurisdiction, and allows registered patrons to purchase the traditional instant products such as Lotto 6/49, Super7 as well as several interactive games like iBingo and Pick 'n Click.

7.1 Approach

We have reviewed the general IT controls, operating and monitoring controls and change management processes used in conjunction with ALC's e-Gaming infrastructure. Specifically, we examined controls around the following e-Gaming elements:

- Firewalls and routers
- Intrusion protection system
- Centralized logging system
- Server and database configuration
- Web hosting infrastructure
- ALC's centralized detection, escalation and reporting capabilities
- Network and VLAN architecture design
- Redundancy of the e-Gaming infrastructure.

Additionally, we performed a controlled external penetration test against www.playsphere.alc.ca, and www.spheredejeu.alc.ca. These external tests were performed from our secure computer testing labs in Halifax and Montreal. Our tests were specifically designed to identify external access points to ALC's e-Gaming environment, logic or software coding within the various websites or games

contained within them, or any other configuration issues that would allow an individual to gain unauthorized access.

7.2 Evidence Reviewed

Our review was carried out on information, evidence and records obtained from ALC directly or through interviews with staff of ALC.

7.3 Findings, Recommendations and Management Comments

We noted the following items which we believe **reduce** potential risks around e-Gaming:

- ALC's network infrastructure and IT Security Group have skilled and certified individuals involved in the planning, development, building and oversight of the e-Gaming environment.
- ALC has implemented a security in depth approach to their network architecture to segregate the various gaming elements, thereby limiting the potential for exposure in the event that the systems were to become compromised.
- ALC uses a combination of automated controls to monitor the gaming network.

We noted the following items which we believe **increase** the potential risks around e-Gaming and, as a result of our review, we offer the following recommendations for consideration:

Finding # 18 – High Risk

Within ALC's Playsphere environment, we have noted that information including sensitive information, i.e., name, address, date of birth, and credit card information including "CCV2" verification numbers, is captured as a component of the credit card billing process. This information is encrypted prior to being submitted from the end users computer to ALC using industry standard encryption, and remains encrypted until it is delivered to ALC's secured gaming network.

Access to this network is controlled by a series of logical access restrictions, physical controls and additional layers of monitoring to detect unauthorized access. Logical access to ALC's secured gaming network is restricted to individuals who require access for authorized business purposes.

These controls collectively are meant to ensure that the collected information is not subject to unauthorized access or disclosure.

Once within the ALC's secured network, the encrypted information is decrypted for processing by the backend middleware servers and, through subsequent processes to the backend database servers, this information is passed in an unencrypted fashion.

We undertook specific tests that required us to gain authorized physical and logical access to this network and, using sophisticated techniques, we were able to capture this information. While the exploitation of this risk would be highly remote, and would require collusion and a highly sophisticated computer user, ALC Management should review their compliance with both the credit card Payment Card Industry (PCI) and Personal Information Protection and Electronic Documents Act (PIPEDA) standards.

Recommendation # 18

We recommend that ALC implement added encryption to protect against leakage of sensitive data. This should include extending the encryption during every phase of the transaction, i.e., communication between the front-end web servers and the middleware servers and the back-end database servers.

Furthermore, we recommend that field-level encryption be implemented within the backend database servers used to store this sensitive information. This field-level encryption will obfuscate the sensitive data within the database limiting the potential of unauthorized access by individuals within ALC that have database access.

Management Comments # 18

Management accepts this recommendation - In process

While there are several strong controls in place to prevent unauthorized access to confidential data, ALC accepts the recommendation to encrypt the backend database. ALC believes that the protective mechanisms currently employed by ALC provide a multi-layered defensive protection against unauthorized access to sensitive data and the risk of information "hacking" is extremely low. This multi-layered protection of defense in depth includes encryption from player's device through to ALC's secured backend network, firewalls, and enterprise system monitoring.

To provide additional context, it is significant to note that this KPMG's finding section references the information was captured from within a secured area of ALC's internal data center. This event was facilitated by granting KPMG escorted access to ALC's highly secured computer room under the direct accompaniment of ALC staff. This provides additional context to the KPMG finding that "the risk is limited to a select group of individuals within ALC's control room only".

While the risk of information "hacking" is extremely remote, the risk rating has been assessed as high by KPMG as result of concerns with ALC's compliance with PCI and PIPEDA standards. With respect to the PCI standards, ALC has reviewed this standard and believes the risk is moderate given our understanding of the standard's content and extremely strong control environment that is currently in place. ALC has reviewed the PIPEDA standards and acknowledges that although the e-Gaming application is within a highly secure area of our network, a change is required to address the risk of compliance with the aforementioned standard.

The application impact of encrypting the database is being assessed by ALC and Vendor and a plan will be formulated for remedial action. This plan will be submitted to senior management for acceptance and prioritization by March 31, 2008.

Finding # 19 – Medium Risk

We noted that certain demo games, are susceptible to an arbitrary flash inclusion attack that allows a potential attacker to redirect a player to a non-ALC flash site while keeping the player believing they are still within the ALC website. Furthermore, validation is not performed to verify if the flash file is coming from the Playsphere site.

We believe that only certain games are affected by this issue in the demo viewing section. Our testing was performed using the most common internet browsers (Firefox, Internet Explorer 6 and Internet Explorer 7) each having their phishing filters enabled during the testing. These filters are generally thought to help an individual identify potential threats. This could introduce additional public harm to ALC if it is determined that the Playsphere site was serving content from another arbitrary site. This could lead to potential phishing and/or spyware attacks.

Recommendation # 19

We recommend that ALC, in conjunction with their vendor, implement controls within the application demo.jsp to deny the use of arbitrary flash parameters. It has been noted that ALC has identified this issue with their vendor and a software fix is being developed to remediate this issue.

Management Comments # 19

Management accepts this recommendation - Complete

The issue has been addressed and ALC has implemented the necessary system changes.

Finding # 20 – Medium Risk

We have identified an information leakage issue within the Playsphere environment whereby remaining funds from other users can be viewed, although cashing or playing their credits was not possible. While it is not possible to affect players' funds through this method, it does provide a mechanism that potentially results in unauthorized disclosure of personal information of players and could impact PEPIDA standards.

Recommendation # 20

We recommend that ALC, in conjunction with their vendor, implement controls within the Playsphere web application to verify the authenticity of the session ID (or token) being submitted after the initial login process. It has been noted that ALC has identified this issue with their vendor and a software fix is being developed to remediate this issue.

Management Comments # 20

Management accepts this recommendation - Complete

The issue has been addressed and ALC has implemented the necessary system changes.

Finding # 21 – Medium Risk

The protocol used by iBingo and Pick 'n Click games allowed us to communicate directly with the Web service without being authenticated within the system. Exploiting this vulnerability, we were able to determine the currently logged in users on iBingo and Pick 'n Click games. While this does

not provide us with an ability to alter the game integrity, it could be used to gather personal information and/or player information, such as frequency, play or duration of play, etc.

Recommendation # 21

We recommend that ALC work with the vendor of these products to lock the use of these commands to authorized administrators only.

Management Comments # 21

Management accepts this recommendation - Complete

The issue has been addressed and ALC has implemented the necessary system changes.

Finding # 22 – Medium Risk

There are no host based Intrusion Detection Systems (IDS) on the servers running the Playsphere environment. This is inconsistent with the use of IDS on ALC's gaming infrastructure to provide proactive monitoring capabilities, and increases the risk of system compromise or manipulation going unnoticed by ALC.

Recommendation # 22

We recommend that the current system used by ALC to collect and monitor network activity be installed to adequately monitor intrusion attempts logged by the servers to the front-end web servers. We also recommend that ALC implement a stricter monitoring process at the network operations level to require help desk staff to monitor and escalate intrusion issues from monitoring software installed on the front-end web servers.

Management Comments # 22

Management accepts this recommendation - In process

ALC's current controls include a solution considered by many in the IT industry to be a form of host-based intrusion detection. Taking all of these controls into consideration, management feels comfortable that the IDS software issue has been addressed until a compatible IDS solution is available.

ALC acknowledges that a stricter IDS monitoring process is needed and has prepared a plan of action. This 45 day plan includes KPMG's recommendation within its scope which will be addressed by March 31, 2008.

To accommodate host based intrusion detection, application architecture would require an earlier version of the operating system which is not compliant with PCI standards. ALC decided to pursue an application firewall approach as an alternative solution until such time that the application architecture can support host based intrusion detection solution.

Finding # 23 – Medium Risk

Although the ALC e-Gaming infrastructure uses redundant equipment at the primary datacenter site in the event of failure, there are no redundant systems at the backup ALC site nor is there redundant internet connectivity at the backup site. This increases the potential for business continuity challenges for ALC's online games.

Recommendation # 23

We recommend that ALC implement redundant internet peering at their alternate datacenter site. We also recommend that hardware be put in place at the alternate site to allow for the continued operations of the e-Gaming systems in the event of a disaster.

Management Comments # 23

Management accepts this recommendation - In process

ALC, in keeping with normal business practices, is in the process of evaluating Business Continuity Plans (BCPs) plans in key areas with the objective of re-assessing assumptions.

The initial assessment of the technical implications of the BCP for this area of the business will be completed by February 18, 2008 with final recommendations presented to senior management by February 29, 2008.

The current environment provides for fault tolerance, data redundancy and real time off site data storage to preserve the data integrity of all Playsphere transactions.

Finding # 24 – Medium Risk

During our penetration testing, a significant amount of abnormal suspicious network traffic was identified by the IT Operations Group. However, they did not open a network trouble ticket nor direct the abnormal traffic patterns to the IT Security Group for follow up as is defined in their IT Operation policies.

We did note that by the end of tests, which lasted approximately 10 business days, ALC's IT Operations Group did alert the IT Security Group. However, their notification was not timely, and could have resulted in system compromise if not part of a controlled testing engagement.

Recommendation # 24

We recommend that ALC implement a process to ensure that all abnormal traffic is logged and directed to individuals within IT Security Group for investigation and follow-up. This will ensure that potentially inappropriate network traffic is appropriately interpreted and handled prior to a system compromise.

Additionally, we recommend that ALC ensure that all individuals within the IT Operations Group be trained on the identification of abnormal traffic and potential security related events that are occurring against the ALC computer infrastructure.

Management Comments # 24

Management accepts this recommendation - In process

A review of Operation's monitoring of the Intrusion Detection System (IDS) and event escalation process has been completed. IT Security and Operations agree with the audit findings. An action plan to address these operational issues has begun implementation and will be completed by March 31, 2008.

Responsibility for investigating IDS events will continue to be placed within IT Security including initial investigation of alerts. Operations Monitoring will monitor IDS events.

Finding # 25 – Low Risk

We have identified a vulnerability within the "session manager" used on the front end web servers by ALC for its e-Gaming environment. The use of this vulnerability would allow a sophisticated

computer operator to capture, and use the session ID of another active player and inject it back to the e-Gaming environment thereby intercepting the playing session of a legitimate user. This risk relates only to player sessions that are active and as such represent a low risk to ALC.

Recommendation # 25

We recommend that ALC implement a stricter monitoring process within their IT Operations Group to identify and direct to the IT Security Group all intrusion issues from mod_security installed on the front-end web servers. Additionally, we recommend that ALC centrally log all the mod_security logs to the IBM Site Protector application they are currently using to collect and analyze other network attack information.

Management Comments # 25

Management accepts this recommendation - Complete

The issue has been addressed and ALC has implemented the necessary system changes.

8 Entity Controls Relating to Linked Bingo

Linked Bingo is an electronically linked bingo game operating under the brand name of SuperStar Bingo, which connects participating bingo halls throughout Nova Scotia. This product allows for the province-wide playing of bingo in a connected and live environment which results in shared prizes.

8.1 Approach

SuperStar Bingo is a relatively new product for ALC and has limited revenues associated with it. Additionally, the infrastructure is relatively simple in architecture and implementation. Our review consisted of an examination of the network architecture and the general IT controls associated with SuperStar Bingo.

Our testing was conducted within the SuperStar Bingo test environment which management has represented is consistent with its production environment.

8.2 Evidence Reviewed

Our review was carried out on information, evidence and records obtained from ALC directly or through interviews with staff of ALC.

8.3 Findings, Recommendations and Management Comments

High Risk:

We have no high risk findings.

Medium Risk:

We have no medium risk findings.

We noted the following items which we believe **increase** the potential risks SuperStar Bingo, and as a result of our review, we offer the following recommendations for consideration:

Finding # 26 – Low Risk

The various bingo hall workstations are connected to the central gaming system network which allows backend access to ALC's backend gaming environment. This could be used by a sophisticated computer operator to cause system disruption.

Recommendation # 26

We recommend that ALC investigate the separation of the Linked Bingo network from the central gaming system network to further mitigate this risk.

Management Comments # 26

Management accepts this recommendation - Complete

ALC has investigated the separation of the Linked Bingo network from the central gaming system network and believes the current controls are sufficient to manage the note risk.

Management's decision was based on the current protection mechanisms including encryption, firewall controls, and intrusion detection monitoring. Additionally, Management believes the risk is further mitigated as LRT and bingo stations are unable to communicate directly with one another based on the logical access restrictions in our network design and the bingo stations currently authenticate to their own servers and do not share infrastructure with other networks, including the central gaming network.

ALC will reassess the network separation should there be any change in current business model or network design and controls.

Finding # 27 – Low Risk

The domain controllers used to authenticate the Bingo hall computers are also running the transaction processing for the bingo software. Typically, domain controllers are not used for purposes other than network authentication and logical access enforcement, and are not used to actually run production applications. This could result in a system outage in the event that the domain controller is unavailable.

Recommendation # 27

We recommend that Management continue its plan to implement new domain controller servers that are not used for running any transaction processing.

Management Comments # 27

Management accepts this recommendation - Complete

The current performance and availability requirements for Bingo Hall operators are being met given the current business model.

ALC will continue to assess the requirement for new domain controllers should the business model undergo changes that necessitate a reevaluation of performance and availability needs.

9 Entity Controls Relating to Charlottetown Driving Park Entertainment Centre (CDPEC)

This phase of the engagement was undertaken at the request of the Shareholder representing the Government of Prince Edward Island who is the sole shareholder responsible for CDPEC. Our scope of review covered Electronic Game Devices (EGD), live poker, casino style cage and money handling policies, and casino-related gaming practices.

CDPEC is an ALC operated entertainment centre which offers live and simulcast harness racing, EGD products, table poker and various food and beverage services. CDPEC is a traditional racino style venue that has its own operational and executive management team in-house which functionally reports into ALC. CDPEC represents a new game offering for ALC as this is the first such venue that ALC is responsible for operating. ALC is not responsible for the simulcast harness racing operations of CDPEC which is independently operated by another group.

9.1 Approach

Our approach for reviewing the controls within CDPEC was to test the compliance of CDPEC operations against the policies and procedures of ALC and CDPEC.

Specifically, we performed the following:

- A review of CDPEC policies and procedures for completeness and appropriateness with a focus on industry best practice
- A review of CDPEC monitoring capabilities as the Security & Compliance monitoring function was a key control element in many of the operational controls
- A review of CDPEC roles and responsibilities with an emphasis on segregation of duties and conflicting roles
- A review of cash counting / handling controls within CDPEC
- A review of EGD operating processes and procedures including:

- Change management
- IT General controls, such as gaming network design and logical access
- Game integrity controls
- Monitoring
- Maintenance

- Compliance with provincial gaming guidelines for gaming centers.

9.2 Evidence Reviewed

Our review was carried out on information, evidence and records obtained from CDPEC and ALC directly or through interviews with staff of CDPEC and ALC.

9.3 Findings, Recommendations and Management Comments

We noted the following items which we believe **reduce** potential risks around CDPEC:

- The controls around cash collection and handling within CDPEC are well defined and consistent with similar controls in other casinos.
- CDPEC management has developed an internal control manual that outlines a series of processes and controls for CDPEC employees in relation to CDPEC operations. This handbook is comprehensive in nature and concisely written.
- CDPEC's rules and regulations have been adopted from other Canadian jurisdictions where the controls are seen to be best practice within the Racino gaming industry.
- ALC Security & Compliance is tasked with compliance oversight on the CDPEC operations and has undertaken audits of specific areas.

We noted the following items which we believe **increase** the potential risks around CDPEC and, as a result of our review, we offer the following recommendations for consideration:

Finding # 28 – High Risk

Individuals within CDPEC have the ability to install unauthorized computers within the central video lottery gaming network. Specifically, we have noted that a senior technician has an ALC corporate computer with direct access to the gaming network in their office. This is against ALC standards and could result in this machine being used to gain unauthorized access to the gaming environment or introduce unauthorized changes.

This issue is further compounded as the technicians at CDPEC maintain the lottery network on their own, rather than follow ALC's process which is initiated with a call to Lottery Support Services (LSS) who centrally monitors all issues of the wide area network video lottery network. LSS then identifies if similar issues have been noted elsewhere in ALC's network and deploys VLT technicians to address the issue. The centralized logging and dispatch processes are defined within ALC's standard policies and procedures.

Recommendation # 28

We recommend that ALC review all logical access controls within CDPEC and remove inconsistent or excessive logical access rights from individuals. Furthermore, we recommend that CDPEC adopt the defined ALC control framework for logical access. This would include limiting individuals with direct access to the central video lottery gaming environment, a centralized logging of all gaming activities, and the use of LSS to centrally monitor issues and dispatch technicians to fix the CDPEC VLT systems.

Management Comments # 28

Management accepts this recommendation - Complete

Process enhancements have been developed which include limiting centralized gaming system access from the CDPEC technicians and using Lottery Support Services to centrally process system configuration changes and a call handling system to centrally log all gaming related activities. These changes were put in place in December 2007.

It is important to note that in relation to introducing unauthorized changes into the gaming environment at CDPEC, the central video lottery gaming system acts only as a detective control. In order to introduce changes to the gaming environment at CDPEC that affect the game, changes are required to be made directly on the EGD. There are a number of effective preventative controls in

place over changes made to EGDs that include segregation of duties, approved documentation of the work to be performed, physical controls over access to the logic area of EGDs, and a security representative must be present for all logic area access. There are a number of detective controls also in place such as surveillance camera coverage that records machine access, documentation of machine access entry and independent audit of EGD game parameters on EGDs shortly after they have had logic board access.

In addition, procedures have been updated as of November, 2007 so that Security & Compliance representatives from Moncton have physical oversight over EGD moves, adds and changes, physically sealing the games and ensuring the values entered on the ES Video system in Moncton, correspond to changes made at the terminal level before the game is placed in service.

Finding # 29 – High Risk

EGD technicians have unrestricted access to the complete central video lottery gaming server used by CDPEC to operate their EGD games. This unrestricted access allows an individual to alter the individual games being played on a particular VLT and the individual game payouts.

Furthermore, we have noted that technicians have access to change payout percentages as well as other game parameters directly on the terminals as evidenced by the audit findings, on routine game configuration compliance audits. We did not observe other compensating controls that were working effectively to mitigate the identified risk.

This problem appears to be CDPEC specific as ALC does not provide their technicians with the ability to access the EGD management system, nor make changes to the prize payout configurations. Within ALC all these functions are handled centrally by a small group of individuals who have no physical access to the EGD machines and are not able to make unauthorized changes and propagate them to the EGD units.

We believe this excessive access results in a segregation of duties issue and could lead to unauthorized changes affected to the EGD units within CDPEC.

Recommendation # 29

We recommend that ALC restrict logical access to the central video lottery gaming server to individuals that do not have conflicting roles with the ongoing maintenance and monitoring of EGD

gaming activities. This would preclude the ability for individuals with physical access to the EGD machines from altering configurations of prize payouts, game configuration and the EGD management system.

Management Comments # 29

Management accepts this recommendation - Complete

Process enhancements have been developed which include limiting centralized gaming system access from the CDPEC technicians and using Lottery Support Services to centrally process system configuration changes and a call handling system to centrally log all gaming related activities. These changes were put in place in December, 2007.

It is important to note that in relation to introducing unauthorized changes into the gaming environment at CDPEC, the central video lottery gaming system acts only as a detective control. In order to introduce changes to the gaming environment at CDPEC that affect the game, changes are required to be made directly on the EGD. There are a number of effective preventative controls in place over changes made to EGDs that include segregation of duties, approved documentation of the work to be performed, physical controls over access to the logic area of EGDs, and a security representative must be present for all logic area access. There are a number of detective controls also in place such as surveillance camera coverage that records machine access, documentation of machine access entry and independent audit of EGD game parameters on EGDs shortly after they have had logic board access.

In addition, procedures have been updated as of November 2007 so that Security & Compliance representatives from Moncton have physical oversight over EGD moves, adds and changes, physically sealing the games and ensuring the values entered on the ES Video system in Moncton, correspond to changes made at the terminal level before the game is placed in service.

Finding # 30 – High Risk

CDPEC's EGD technicians can clear automated system logs and alarms on the EGDs without following the stated policies of notifying ALC's LSS group. These alarms are automatically generated to ensure that changes to the EGD are identified by a central group and are considered within the industry to be a strong control. For example, when a logic board is removed from an EGD, an alarm would be generated. Within ALC, these alarms are centrally monitored by LSS.

LSS then compares the alarm details with known maintenance and correlates the log of the EGD technician requesting physical access to the EGD. The ability to clear the alarms without monitoring or oversight by an independent group could allow an individual within CDPEC to operate the various EGDs under non-standard playing parameters. Furthermore, we did not identify sufficient compensating controls that would effectively mitigate the risk associated with this finding.

Recommendation # 30

We recommend that all alarm notifications within CDPEC be reviewed by ALC's LSS in a manner consistent with those used within the wide area gaming network. This would require that LSS be responsible for monitoring all PVD alarms, and for dispatching technicians to fix the issues identified.

Management Comments # 30

Management accepts this recommendation - Complete

Changes to system access for the CDPEC technicians will now require un-cleared PVD alarms to be logged and cleared by LSS. This change was put in place in December 2007.

It is important to note that, while alarm monitoring and clearing by LSS adds an additional level of independence and central oversight, there already exists a number of compensating preventative controls over introducing unauthorized changes into the gaming environment at CDPEC that serve to mitigate this risk.

Finding # 31 – High Risk

On regular EGD compliance audits, discrepancies existed between the configurations that were supposed to be defined in CDPEC's EGDs and what was actually defined. Specifically, we noted that the number of lines, bets per line and max bet parameters were incorrect.

We observed that discrepancies are manually tracked on an excel spreadsheet by the EGD technicians and contain transposition and clerical errors. This is not consistent within ALC where this information is retained centrally by an independent group and routinely audited, resulting in limited or no errors. Additionally, we noted that the audit control sheet we had reviewed at CDPEC on this particular routine audit was marked off as fixed before the EGD Supervisor had verified that the EGD technician had changed anything within the game parameters.

We also noted that the machine audits are only being carried out on machines that have been opened during the previous day due to faults or due to negative payouts. Therefore, it is possible for a machine to remain un-audited for significant periods of time during which the payouts or game parameters could be incorrect.

Recommendation # 31

We recommend that CDPEC work closely with ALC Video Lottery Product Compliance and Process as well as Security & Compliance to develop better processes around managing EGD game parameters. This includes a method to consistently update and document game parameters. We also note, as in previous recommendations that CDPEC should work closely with ALC to develop a stricter audit process to eliminate inconsistencies in their game parameters configuration.

Management Comments # 31

Management accepts this recommendation - Complete

Process enhancements have been developed whereby Security & Compliance representatives from Moncton have physical oversight over EGD moves, adds and changes, physically sealing the games and ensuring the values entered on the ES Video system in Moncton, correspond to changes made at the terminal level before the game is placed in service. In addition, enhancements will be made to the audit process such that Security & Compliance representatives will have oversight on the results of machine audits to ensure they are carried out on a timely basis and also to review the results of the audits to ensure that discrepancies are followed up on a timely basis. These changes have been put in place by December 2007.

It is important to note that inconsistencies in game parameter configurations among various data sources do not negatively impact game function or integrity. EGD compliance audits are performed on 100% of machines that have had logic board access and there has never been any finding of unauthorized changes. An independent annual review of game payouts is conducted to ensure that games are performing within defined volatility ranges according to provincial regulations.

Finding # 32 – High Risk

Through the application of computer aided auditing techniques on the EGD transaction and centralized validation logs at CDPEC, we identified several data anomalies, specifically the

processing of transactions outside of normal business hours around cashouts and payouts. Cashouts refer to the process of ceasing play on an EGD, and having a paper ticket printed for the remaining credits the player has. Payout refers to the conversion of the paper ticket that was printed from the EGD for a monetary sum by the cash cage at CDPEC, or for use within another EGD machine to continue play, subject to authentication and validation to the central system.

While it is not uncommon to find anomalies within large populations of data, we felt that the existence of these anomalies and our observation of transaction records occurring during non-business hours warranted additional procedures. Upon investigation, we understand that these data anomalies could be the result of system related delays, software limitations within the EGD networks, or reporting inconsistencies. System delays, EGD testing or computer glitches which would result in some of the anomalies would be expected in EGD play environment.

Management has represented that the transactions occurring during non-business hours are the result of the system communication issues within CDPEC. In the event that a computerized validation is not possible, a manual pay form is used by the cage to record and pay out tickets to patrons once the authenticity of the ticket is established. Thereafter, CDPEC engages in a manual process to validate the manually paid tickets once the system communication issue is cleared. It is our understanding that this is often done by the cage supervisors during non-business hours.

Our additional analysis identified the following weaknesses:

- CDPEC relies on a series of manual controls to address the technical issues identified. Manual controls by their nature have limitations on operating effectiveness, and consistent application.

- While documentation existed in support of the manual controls, it was incomplete for items within our audit sample.

- There was no evidence of CDPEC management's identification, follow-up and oversight of the occurrence of the data anomalies.

Accordingly, we were unable to validate management's representation that the data anomalies we identified were fully the result of system communication issues.

Recommendation # 32

We recommend that ALC implement a more robust EGD infrastructure to limit the system communication issues currently encountered. This should minimize the need for the quantum of manual processes being used at CDPEC, and allow for a fully automated validation of tickets from the EGD machines.

Where manual controls are used to compensate for system related issues, we recommend that ALC ensure that the manual processes, documentation standards and controls are consistently applied, and provide a complete audit trail.

Finally, ALC should develop and implement processes to identify, report on and follow up on any data anomalies. Additionally, an investigation into the patterns associated with future data anomalies, if any, would be an appropriate element to a future investigation by ALC's Security & Compliance Group.

Management Comments # 32

Management accepts this recommendation - In process

A review of cash outs within CDPEC was performed by Internal Audit in January 2008. The review examined cash outs that occurred outside of normal business hours. The engagement reviewed the controls and processes that are in place. The Audit team was able to successfully trace 100% of the audit sample to appropriate documentation and explanation. On further data analysis, IA found 7 transactions for a total value of $133.30 that could not be fully explained. This was from a data set of 408,000 transactions with a dollar value of approximately $22,000,000. Based on the findings in this review, Management concludes that there are not material unexplained cash outs and as a result, this finding is not considered to be of a high risk nature given the existing processes and controls that are in place.

Management will complete a technical review of the infrastructure in order to determine the root cause of the communication errors and develop an action plan based on the results of the review. This review will be completed by March 2008.

Finding # 33 – High Risk

CDPEC has a stated policy whereby winners of over $10,000 within CDPEC are required to present identification in order to be paid the prize. We selected a sample of winners of over $10,000 to assess compliance with the stated policy. We noted that for items within our sample, winners of over $10,000 within CDPEC had been paid out their prize without presenting identification. We were informed that CDPEC staff paid the prize in the absence of identification if their staff recognized the winner or the winner had a previous Large Cash Transaction within CDPEC.

Specifically, we have noted an example where an individual won in excess of $32,000 over a four month period, yet the circumstances around each large win were never investigated formally by CDPEC. Additionally, on the third occasion of winning over $10,000 on an EGD game, the individual did not have any identification and was still paid out on the basis that an employee recognized the winner.

This violates CDPEC stated policies and could result in inappropriate payouts to individuals.

Recommendation # 33

We recommend that when large cash outs are performed at CDPEC, ALC's stated Winner Claim policy, including requiring government issued identification and signed declaration, be enforced. Additionally, where a pattern of large wins is identified for a particular individual, ALC Security & Compliance should perform an appropriate level of investigative review prior to releasing the funds. These investigations should be appropriately documented similar to ALC investigations and formally retained.

If these controls cannot be met by the patron, then the funds should not be released until such a time that ALC is confident that the winner is identifiable and the win is legitimate.

Management Comments # 33

Management accepts this recommendation - In process

The CDPEC policy has been revised to ensure photo ID is always collected for all wins of $10,000 or greater effective November, 2007.

The control environment regarding winners of $5,000 or greater at CDPEC is considered by management to be very strong. A win on an EGD of $5,000 or greater immediately causes the terminal to lock-up and sends a notification to CDPEC floor staff and surveillance. A series of procedures are required by CDPEC staff including an investigation of the game chip seal and ROM signature before producing the validation ticket from the EGD at which point the customer is escorted to the cage and cashier area for payment. Under no circumstances are payments made for prizes greater than $5,000 without the presence of the above physical controls, surveillance review and multiple CDPEC staff witnesses.

Security & Compliance will review the level of investigation required where a pattern of large wins is identified for an individual.

Finding # 34 – Medium Risk

While CDPEC's rules and regulations appear consistent with practices in other jurisdictions, they are based on a model that is different than CDPEC's structure. We have noted that there is no independent regulator within Prince Edward Island and, as a result, there is no independent review of CDPEC's gaming operations.

While ALC is the operator of CDPEC, they do not provide independent oversight of the management of CDPEC in the same capacity as an independent regulator would. This leads to a segregation of duties issue that could allow inappropriate changes or decisions to be made in relation to CDPEC operations that could remain un-noticed.

Recommendation # 34

We recommend that the policies and procedures that have been adopted by CDPEC from other jurisdictions be reviewed for appropriateness in CDPEC's environment.

Management Comments # 34

Management accepts this recommendation – In process

Internal Audit has formulated a four phase plan to review the CDPEC operation. As the first major component of this plan, the Internal Audit department has initiated an audit engagement of the CDPEC Gaming Floor Management operational process. The engagement includes a high level review of the control environment and a detailed review of the control activities within the process.

The scope of the audit work includes all of the activities to manage, maintain and secure the EGD machines on the gaming floor.

This first audit engagement will be completed by March 31, 2008. The complete plan will be executed in fiscal year 2008-2009.

Finding # 35 – Medium Risk

Generally accepted industry standards for distribution and configuration management of EGDs are not consistently applied at the CDPEC location. Specifically, we noted that this includes the physical placement and distribution of EGDs, the approach to IT general controls including local server configurations, intrusion detection system, virus protection, and administrative approaches.

As a result, we believe that ALC may be taking on additional risks as an operator by having two processes and approaches to managing a similar gaming product in different control environments.

Recommendation # 35

We recommend that ALC implement the control procedures, processes and environmental restrictions within CDPEC similar to generally accepted industry standards used within ALC.

Management Comments # 35

Management accepts this recommendation - In process

Although there are legitimate process differences between the wide area VLT network and the distribution of Slots within a facility as a result of the different environments, ALC will apply increased consistency to distribution and configuration management of terminals.

Specifically, CDPEC will implement the use of Lottery Support Services to centrally monitor gaming activities and the use of the call handling system to centrally log all gaming activities. These changes have been implemented.

In addition a review of IT General controls will be performed in February 29, 2008 to ensure that CDPEC has the same control standards that are used within ALC.

Finding # 36 – Medium Risk

Reliance is placed on the surveillance group within CDPEC to detect inappropriate activities. In practice, however, there are approximately 180 cameras and routinely 2 individuals who are available to conduct reviews of these cameras. Additionally, we have noted that, within CDPEC, the camera security system only retains 11 to 14 days of footage.

The ratio of cameras to reviewers, the duration of available evidence retention, and the additional roles within the job descriptions of the surveillance group make this control less effective as it is not possible to monitor the activities appropriately. We noted, while on-site, that there were on-screen alarms that were not reviewed as the individual responsible for reviewing them was busy reviewing another item.

Recommendation # 36

We recommend that ALC ensure adequate levels of training, awareness and oversight of the security personnel is sufficient to ensure that adequate levels of monitoring can be achieved. Furthermore, we recommend that CDPEC retain the digital video footage for an extended period, where warranted, to allow for future investigative uses.

Management Comments # 36

Management accepts this recommendation - In process

A functional review of the CDPEC surveillance processes will be completed by February 29, 2008. This review will ensure adequate training, awareness and oversight is in place with the surveillance personnel. In addition, all video footage will be retained as necessary beyond the 7 day period as required.

The Surveillance function at CDPEC reports into ALC's Security & Compliance department to ensure independence from management at the venue. Surveillance is utilized to ensure that the integrity of CDPEC operations is maintained at all times as per the regulations. This utilization is industry standard and although it appears the cameras-to-staff ratio may not be sufficient, there are other compensating controls in place to offset the fact that surveillance staff are not monitoring the results from every camera. On screen alarms are not always investigated immediately due to other priorities within the surveillance room, however the Surveillance operators run reports that will indicate which alarms have occurred so they can investigate them on a timely basis.

Finding # 37 – Medium Risk

The EGD compliance audits are supposed to be carried out in the presence of an EGD technician. However, the compliance audits are sometimes carried out with a supervisor from another area of CDPEC's operations if an EGD technician is not present. These supervisors may not have appropriate training for this task.

Recommendation # 37

We recommend that all EGD compliance audits be carried out in the presence of an EGD supervisor or technician as per the stated CDPEC policy. CDPEC should not substitute trained EGD personnel with other CDPEC employment regardless of their position with the organization. As an alternative, CDPEC could request that ALC Internal Audit and/or Security & Compliance provide an auditor to perform these compliance checks.

Management Comments # 37

Management accepts this recommendation - Complete

EGD compliance audits will only be carried out in the presence of appropriate EGD personnel. In addition, enhancements will be made to the audit process such that Security & Compliance representatives will have oversight on the results of machine audits to ensure they are carried out on a timely basis and also to review the results of the audits to ensure that discrepancies are followed up on a timely basis. These changes have been implemented.

Finding # 38 – Low Risk

The logic boards within the EGDs at CDPEC are covered with tamperproof security tape, which is inconsistent with the controls in place over similar VLTs in the wide area operated by ALC. While CDPEC has physical security control of the EGD machines, the use of the tamperproof seals used by ALC is appropriate to mitigate any risk of unauthorized removal of logic boards.

Recommendation # 38

We recommend that CDPEC implement the use of the tamperproof seals used by ALC within their VLT systems.

Management Comments # 38

Management accepts this recommendation - Complete

ALC will reassess the use of seals if the present business model undergoes changes in operations or technology.

ALC is currently using security tape which is an international industry standard and best practice within the casino industry. Management is satisfied at the current time the control provided by the security tape provides sufficient protection over the logic boards of the Electronic Gaming Devices (EGD). Additionally, CDPEC has Information Technology controls that verify only authorized software is operating. There is also monitored floor surveillance and other protective measures which guard against improper access to the EGD.

Finding # 39 – Low Risk

CDPEC technicians have direct access to vendor contacts thereby allowing full access to sensitive game data. In comparison, this information is only available to three individuals within ALC, all of whom have no physical access to the VLTs.

Recommendation # 39

Consistent with ALC's current policies, we recommend that all vendor contacts be limited to individuals who have a direct business need. Additionally, we recommend that ALC instruct the vendors to limit their contacts with approved individuals.

Management Comments # 39

Management accepts this recommendation - In process

All sensitive data available to the Technicians at CDPEC are available via the websites of these manufacturers. Access to this information is industry standard for the casino environment which differs than the VL environment as the CDPEC Technicians perform repairs to various parts of the terminals where as the VL technicians typically interchange parts.

ALC will review vendor information access to ensure that contact is limited only to those who have a direct business need.

Finding # 40 – Low Risk

There is no consistent approach in terms of vendor updates and games knowledge sharing within CDPEC and ALC. As a result, ALC may not be achieving the efficiencies possible if all dealings were centralized.

Recommendation # 40

We recommend that ALC implement its policy on vendor updates and games knowledge sharing within CDPEC. Additionally, we recommend that ALC ensure that the vendors are made aware of whom they can deal with directly. This group should be limited to those individuals with a defined business need for such access to the vendor.

Management Comments # 40

Management accepts this recommendation - In process

Vendor relationships are necessary at times when technicians are trouble shooting games as the wide area VL network does not carry the games being utilized at the CDPEC. Although this information is regularly shared with the Product Approval department located in Moncton, a new notification process will be developed and implemented to ensure information is shared consistently.

Finding # 41 – Low Risk

ALC carries out minimal tests on the games approved for operation within CDPEC. ALC bases its acceptance of games on the approval of testing carried out by other jurisdictions. This could result in additional risk within CDPEC as the testing by others may not be appropriate for the CDPEC game infrastructure.

Recommendation # 41

We recommend that increased testing of EGD games destined for the CDPEC be conducted by ALC to ensure the games are appropriately controlled for use within CDPEC's game infrastructure.

Management Comments # 41

Management accepts this recommendation - In process

All games implemented at CDPEC are first reviewed and approved by ALC's Product Approval group located in Moncton. While ALC does accept transfers of approval from certain other jurisdictions, requirements are defined for product specification standards to ensure that they meet the requisite standards of integrity required by ALC.

An enhanced testing process to support transfers of approval will be implemented by March 31, 2008.

Finding # 42 – Low Risk

While it is common for organizations to employ individuals that are related or closely affiliated, it is generally expected that such organizations have a policy, and supporting evidence that appropriate segregation of duties are reviewed by management prior to such employment.

Segregation of duties refers to assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets and is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of the person's duties.

Typically, such reviews are formally retained and updated on a regular basis to ensure that changes in roles or job functions do not impact on segregation of duties. We noted that a number of individuals within CDPEC have close working or familial ties, and that CDPEC has a policy to deal with this segregation of duties issue; however, there was no formal evidence that the policy was operationalized. This lack of evidence results in a less robust control environment, and increases the potential for segregation of duties issues not being identified in a timely manner.

Recommendation # 42

We recommend that the roles of individuals within CDPEC be reviewed on a regular basis to determine if segregation of duties is further impacted by familial or close working relationships. This process should be formally documented and retained as a component of the individuals personnel file.

Management Comments # 42

Management accept this recommendation - In process

Management is enhancing the process, including documentation, and this will be completed by March 2008. Management believes there are strong controls currently in place to manage this risk. The CDPEC policy is to ensure there are no potential conflicts or reporting relationships prior to hire. The Site Controller department also ensures when verification signatures of any type are required by 2 or more individuals according to policy, those who have family ties are not verifying one another's work.

Finding # 43 – Low Risk

ALC does not perform a 'Polite Shutdown' of the EGD units within CDPEC, as they do within the wide area gaming network to enforce game play hours.

Recommendation # 43

We recommend that ALC review the use of a 'Polite Shutdown' within the CDPEC EGD infrastructure as an additional method of enforcing game play hours.

Management Comments # 43

Management accepts this recommendation - In process

Management will review the applicability of a "polite shutdown" within the CDPEC environment to further enforce game play hours by March 31, 2008. Management does believe that the physical characteristics of CDPEC provide additional controls that are not under ALC's control in the wide area gaming network, which limit the risk of after-hours game play at CDPEC. Additionally, ALC has the ability to review surveillance tape of the gaming floor and system logs for any after hours EGD use.

10 Entity Controls Relating to Finance

Finance is responsible for reviewing and accepting the various financial aspects of the games prior to being authorized for production, for paying out winning tickets after approval by Security & Compliance and for financial aspects of processes within procurement and distribution.

10.1 Approach

We have reviewed the policies and procedures that Finance has in place over receipts and distribution of cash, approval of prize structures in the game development processes, payouts of winning prize tickets, and inventory related processes.

The majority of Finance's processes are dependent on the control structures of other groups. We undertook a review of the Finance related documentation to ensure it was properly authorized, complete, and compliant with ALC's policies.

10.2 Evidence Reviewed

Our review was carried out on information, evidence and records obtained from ALC directly or through interviews with staff of ALC.

10.3 Findings, Recommendations and Management Comments

We noted the following items which we believe **reduce** potential risks around Finance processes and operations:

- Finance has defined controls in place to ensure that the winner investigative process by Security & Compliance is complete prior to the issuance of a cheque to the winners.

- Finance has defined cash handling processes to mitigate the risk of unauthorized access or loss to the organization.

- ALC engages an independent third party yearly to perform a financial audit. This audit is conducted in accordance with the Canadian Institute of Chartered Accountants Generally Accepted Auditing Standards. During Fiscals 2005/2006 and 2006/2007, there has been no reservation of audit opinion.

High Risk:

We have no high risk findings.

Low Risk:

We have no low risk findings.

We noted the following items which we believe **increase** the potential risks around Finance processes and operations and, as a result of our review, we offer the following recommendations for consideration:

Finding # 44 – Medium Risk

Tickets are recalled by ALC to the distribution centers to be destroyed. ALC's policy is to write off the inventory upon physical destruction of the tickets. ALC's documented processes indicate that tickets recalled would not be destroyed if sufficient budget had not been allocated. As such, recalled tickets could remain on the inventory of ALC's distribution center at their original value.

Notwithstanding the materiality of the value of these tickets, ALC's documented practice is not consistent with amendments to Section 3031 of the CICA Handbook (June 2006), which would require that the ticket value be written off against income in the period they are recalled.

Recommendation # 44

ALC should revise their documented process to be consistent with Section 3031 of the CICA Handbook.

Management Comments # 44

Management accepts this recommendation - Complete

ALC's accounting policy with regards to ticket write-offs is consistent with Section 3031 of the CICA Handbook. ALC currently writes off the value of tickets from inventory or provides an allowance for future write offs for all tickets which have been recalled or expired, regardless of the period in which they are physically destroyed. Furthermore, ALC Finance does not determine the value of ticket write offs based on the estimated annual budget. Although this amount is monitored

throughout the year to understand variances between forecasted results to budget, the annual valuation is performed based on actual destructions, recalls or expirations of tickets.

The documentation for ticket destruction has been revised to reflect the actual process and policy being followed.

11 Entity Controls Relating to Marketing

Marketing is responsible for reviewing and ensuring that the various stakeholders within ALC, including Security & Compliance, Finance and Operations, accept the new games prior to a new game being approved for initial production. Furthermore, Marketing is also responsible for new game development, and the coordination of activities ensuring that the various changes required from time to time addressing responsible gaming are being made and that legal or other wording changes are complete. Additionally, Marketing is currently the group responsible for ensuring that the final gaming working papers are approved and retained in accordance with ALC policies.

11.1 Approach

We have reviewed the controls and processes in place within Marketing throughout the game design life cycle. In addition to developing the new games, Marketing plays a key role in the approval process and launch of new games. Marketing has been tasked as a group to retain all the relevant information for each game and are the ones principally responsible for the creation of game working papers which outline the controls and financial parameters that the ticket vendor(s) must develop into the final tickets.

We specifically reviewed the manner in which game concepts are developed, reviewed by various specialists within ALC and finally approved for production to the various vendors. We have specifically followed this process for the most recent game for each of:

- e-Gaming
- Tickets i.e., Scratch'n Win and national or regional online games
- Online
- Video Lottery.

Additionally, we reviewed the documentation provided to and processes used by Marketing during the release of the new player protection enhancements that ALC recently launched. We reviewed this information to ensure that Marketing complied with ALC's policies.

11.2 Evidence Reviewed

Our review was carried out on information, evidence and records obtained from ALC directly or through interviews with staff of ALC.

11.3 Findings, Recommendations and Management Comments

We noted the following items which we believe **reduce** potential risks around Marketing:

- ALC has well defined processes for the development and approval of games.
- ALC senior management approves all games prior to going live.
- ALC undertakes technical, financial and ticket testing research for each game prior to going live.

High Risk:

We have no high risk findings.

Low Risk:

We have no low risk findings.

We noted the following items which we believe **increase** the potential risks around Marketing and, as a result of our review, we offer the following recommendations for consideration:

Finding # 45 – Medium Risk

The evidence of the final approval of tickets is not formally retained for all approvers. There is a documentation issue around the approval process for instant tickets whereby approval is obtained but not formally documented. This lack of formal documentation is present in Marketing, Finance, Procurement and Security & Compliance. While there is no evidence that unauthorized changes have occurred, without this final approval process being formalized and retained, the potential could exist.

Recommendation # 45

ALC should implement a formal process to record all approvals on key decisions within each business unit. Where multi-divisional approval is required, the approval should be retained on the final approved documents or as a component of the final approval package that gets reviewed by ALC senior management.

Management Comments # 45

Management accepts this recommendation - Complete

With regard to working papers ALC has implemented a new working paper approval process. Marketing will change its current process so that the cross-divisional team who reviews the draft working papers, will receive the final working papers prior to the game being prepared for press. This will give all reviewers an opportunity to review and finalize once again their approval on the final working papers, prior to the product being printed. All approval documentation that Marketing receives on a particular game will continue to be kept in the games file.

12 Entity Controls Relating to Procurement

Procurement is responsible for ensuring that ALC's purchases and contracted vendors are appropriate and follow the policies of ALC. These policies are designed to meet the intent of applicable external binding agreements, principally the Atlantic Procurement Agreement.

This phase of our review was conducted to ensure that Procurement was following stated policies and procedures to ensure a transparent and appropriate procurement process was undertaken by ALC in its routine purchases. We have limited our review to those purchases over $10,000 which require additional controls.

12.1 Approach

We obtained a listing of all purchase orders, including sole, single and limited purchases, issued during the period of April 1, 2006 to September 30, 2007 of $10,000 or more. This file contained 556 purchase contracts entered into by ALC with various vendors. We randomly selected a sample of 26 purchases for further examination.

For each of the 26 items selected, we reviewed the purchase orders, supporting documentation and rationale for the purchase decisions. The supporting documentation was also reviewed for compliance with ALC's internal documentation and the Atlantic Procurement Agreement to the extent required.

12.2 Evidence Reviewed

Our review was carried out on information, evidence and records obtained from ALC directly or through interviews with staff of ALC.

12.3 Findings, Recommendations and Management Comments

We noted the following items which we believe **reduce** potential risks around Procurement:

- ALC has a standard policy in place surrounding the signing authority of purchase orders, requisitions, and contracts.

- ALC has a standard policy in place regarding purchasing rules for dollar thresholds as well as the applicability of sole, single and limited sourcing. The dollar value thresholds are being adhered to and any exceptions noted were justified through sole, single or limited sourcing.

- ALC has a process in place for legal review of all respondents' submissions for RFPs and associated contracts with the successful bidder.

- ALC's procurement policy states that "the procurement policies of the Atlantic Lottery Corporation Inc. will reflect the 'general intent' of the Atlantic Procurement Agreement." The policy also notes that geographical location should be considered in this order: Atlantic Canada, Canada, United States, or other.

We noted the following items which we believe **increase** the potential risks around Procurement and, as a result of our review, we offer the following recommendations for consideration:

Finding # 46 – High Risk

ALC does not use a standardized process to analyze, justify and document sole, single and limited source procurements. We were unable for some of our sample to find evidence that the processes outlined in ALC's procurement policies around research, analysis, approval and conclusions for single sourcing were formally retained on a consistent basis.

Recommendation # 46

ALC should implement a process ensuring all single source justification memos are formally reviewed and approved by Senior Management. This approval by Senior Management should be completed prior to having the President formally review and approve the single sourcing.

Additionally, ALC should revise their policies and procedures around single source justification so that a consistent criteria and formalized checklist would be a required component of the formal documentation. Furthermore, ALC should ensure that all research undertaken on all single sourcing, or large changes and new offerings are formally documented and retained as a component of the procurement process.

Management Comments # 46

Management accept this recommendation - In process

ALC Management is confident that policies and procedures are in place that provides effective management of the procurement function in an open fair manner that returns the highest degree of competition and value for its shareholders. In addition, all exceptions to competitive bidding such as a single or sole sourcing are appropriately justified.

ALC is updating its Supply Chain Management policies and procedures which include standards for the analysis, research, justification and documentation of all exceptions to competitive bidding. These exceptions will require Senior Management and President review and approval. In addition, ALC has been named in the revised Atlantic Procurement Agreement which becomes effective February 18, 2008.

Finding # 47 – Medium Risk

ALC's standard policies for sole, single, and limited source justification are at a very high level. As such, there could be a variety of reasons for justifying the decision and there is no consistent measure for what would be a satisfactory justification.

Recommendation # 47

We recommend that ALC review its standard policies around procurement justifications to include additional metrics around minimum criteria for each type of procurement.

Management Comments # 47

Management accepts this recommendation - In process

ALC is reviewing all Supply Chain Management policies and procedures which will include ensuring that appropriate levels of formal approval are obtained and documented. The specific standards regarding applicability, justification, documentation and retention of alternative procurement processes such as sole, single and limited sourcing will be explicitly outlined to ensure consistency and alignment with Atlantic provincial governments, the Atlantic Procurement Agreement and the Agreement on Internal Trade. The policy and process revisions will be effective in February 29, 2008.

Finding # 48 – Medium Risk

ALC does not have a standard process in place to formally document the sole, single or limited source justification. During our review, we noted this documentation often takes the form of a high level memo that would not necessarily capture the rationale for procurement decisions.

Recommendation # 48

ALC should consider implementing a standard process for a sole, single or limited source decision including standard documentation requirements.

Management Comments # 48

Management accepts this recommendation - In process

ALC is reviewing all Supply Chain Management policies and procedures which will include ensuring that appropriate levels of formal approval are obtained and documented. The specific standards regarding applicability, justification, documentation and retention of alternative procurement processes such as sole, single and limited sourcing will be explicitly outlined to ensure consistency and alignment with Atlantic provincial governments, the Atlantic Procurement Agreement and the Agreement on Internal Trade. The policy and process revisions will be effective in February 29, 2008.

Finding # 49 – Low Risk

ALC uses a Request for Proposal (RFP) Checklist which includes a requirement that all contracts go to internal legal counsel for review prior to being signed; however, we noted that this is not part of a formal ALC policy. We did not find evidence that legal reviews were not being undertaken for RFPs; however, without a section outlining the requirement for such a review compliance cannot be easily enforced.

Recommendation # 49

We recommend that ALC amend its procurement policy to ensure that a legal review is formally required as a component of the RFP process.

Management Comments # 49

Management accepts this recommendation - In process

As part of standard practice, a process is currently in place whereby all contracts have an attachment that requires signoff by internal legal counsel before proceeding to a signing officer for signature.

Management will ensure that legal reviews are formally required as a component of the RFP process**.**

Finding # 50 – Low Risk

ALC's policies for single sourcing require that the agreement be approved by the Vice-President of the requisitioning department while, in comparison, a limited sourcing arrangement must be approved by the President. We would expect that, given the significance of a single source arrangement, a higher onus should be placed on a single sourcing decision rather than a limited sourcing decision. As such, we believe that the control as worded is not appropriate. Furthermore, we have noted instances where there is no evidence of approval by the Vice-President or President for single or limited sourced items.

Recommendation # 50

We recommend that the approval matrix for single and limited sourcing arrangements be reviewed for appropriateness. ALC should implement a process whereby its single and limited sourcing contract awards are formally reviewed and approved by the President as these procurements are typically larger and sensitive in nature. This final approval should be formally documented and retained as a component of the procurement documentation.

Additionally, a procurement audit should be conducted by Internal Audit on a regular basis to ensure that all single and limited sourcing contracts are appropriately documented and follow all stated policies and procedures.

Management Comments # 50

Management accepts this recommendation - In process

ALC is reviewing all Supply Chain Management policies and procedures which will include ensuring that appropriate levels of formal approval are obtained and documented. The specific

standards regarding applicability, justification, documentation and retention of alternative procurement processes such as sole, single and limited sourcing will be explicitly outlined to ensure consistency and alignment with Atlantic provincial governments, the Atlantic Procurement Agreement and the Agreement on Internal Trade. The policy and process revisions will be effective in February 29, 2008.

Finding # 51 – Low Risk

We have noted that ALC Purchase Orders (PO) do not contain sufficient lines to capture the required approval signatures. Specifically, we have noted that POs are signed initially by the procurement officer, and if additional authorization is required, that individual signs on the last page of the PO.

From an audit perspective, it becomes difficult to tell when this additional sign-off occurred as there are no associated dates, i.e., does it occur before the procurement officer places the order, or does it occur afterward. Additionally, the space where the procurement officer signs, is deemed the "authorized signature"; however, they may not necessarily be the authorized signature on the PO. Additionally, we have noted that not all change order forms retain formal approval signatures as required by the procurement policies.

Recommendation # 51

ALC should alter the PO form to allow for additional approvals and dates to be documented.

Management Comments # 51

Management accepts this recommendation - Complete

The PO form has been altered to accommodate all required levels of approval and dates in November 2007.

13 Entity Controls Relating to Distribution

The distribution group within ALC is involved in the receiving, storing, shipping and handling returns of lottery products, e.g., tickets and other lottery supplies, such as VLT lottery ticket paper stock. This group also plays a significant role in ensuring that only appropriate supplies are sent out and used in relation to ALC's various lottery games, marketing materials and responsible gaming collateral. The primary responsibility for the physical security and operations of the distribution centers is also delegated to this group within ALC.

Additionally, this group is responsible for the destruction of tickets that are no longer being offered to the public for gaming consumption, and coordination with Finance to ensure that the destroyed inventory is appropriately recorded.

13.1 Approach

We have split our approach on this section to include a review of physical controls in place within the distribution process and also a review of the documented controls and procedures in place to ensure that controls exist to minimize the risk of unauthorized products being distributed, used or otherwise involved in ALC's gaming processes, e.g., incorrect paper stock for the VLT machines.

Additionally, we reviewed the pack activation process which is a control that ensures all scratch tickets, with the exception of Break-Open tickets, are not considered live until received by the retailers and scanned into the system as available for sale.

13.2 Evidence Reviewed

Our review was carried out on information, evidence and records obtained from ALC directly or through interviews with staff of ALC.

13.3 Findings, Recommendations and Management Comments

We noted the following items which we believe **reduce** potential risks around Distribution:

- ALC's pack activation process is well defined, well implemented and mitigates the risks of theft of full packs of tickets being played, validated as a winning ticket and subsequent attempts to collect money from ALC.

- ALC's inventory controls around tickets are well defined and controlled using a perpetual inventory system that allows for tracking of inventory from the ticket producer to the retailer.

- ALC's processes around physical distribution of tickets from the ticket producer to the distribution centers, physical security within the distribution center and final retailer distribution are well defined and appear to address typical physical security issues.

High Risk:

We have no high risk findings.

Medium Risk:

We have no medium risk findings.

We noted the following items which we believe **increase** the potential risks around Distribution and, as a result of our review, we offer the following recommendations for consideration:

Finding # 52 – Low Risk

Within the distribution centers, individuals share computer passwords to allow them to access the inventory systems. This represents a low risk to ALC overall. However, the use of a generic or shared password does limit the accountability of individuals within the Distribution Group.

Recommendation # 52

ALC should review the logical access needs within the distribution centers and ensure that the appropriate individuals have access commensurate with their business needs.

Management Comments # 52

Management accepts this recommendation - Complete

User access levels have been restructured and the use of generic passwords has been discontinued as of December 2008.

A Glossary of Terms used in our Review

AEGIS – is the backend gaming engine used by ALC to record and track all gaming transactions including validations, sales, redemptions and all retailer related information including date/time of each transaction, LRT number, retailer number and other gaming information. This backend system is not interfaced by players or the majority of ALC employees and is considered highly confidential. Access to this system is limited to individuals (including retailers) with a business need only, and only after appropriate authorization.

ALC – Atlantic Lottery Corporation

BDM – Business Development Manager is a sales position within ALC that operates within the wide area gaming network to provide ticket, game and marketing support for ALC games.

BRUTE FORCE ATTACK – is a method used to decode encrypted information using an automated approach to try random combinations of digits and characters to obtain the correct password used to do the original encryption.

CCV^2 – Credit Card Verification is a unique number used to provide an additional validation control for online purchases using credit cards.

CDPEC – Charlottetown Driving Park Entertainment Center is the racino operations in Charlottetown PEI that are operated on behalf of the Government of PEI by ALC. This location has both VLT, live poker products which are operated by ALC, and live and simulcast horse racing that is not under the control of ALC.

CFE – Communication Front-End is a processing engine allowing the LRT units to communicate with the AEGIS backend system

CENTRAL VIDEO LOTTERY GAMING SYSTEM – an application used to manage the VLT units within the Charlottetown Driving Park Entertainment Center.

ENCRYPTION – Data Encryption Standard is an approach developed in 1977, which applies algorithmic key to a stream of data obfuscating the data to ensure that if it was intercepted it would unreadable.

EGD - Electronic Gaming Device – refers to video lottery terminals within the CDPEC environment.

GAME INTEGRITY – refers to the fairness and transparency of the operation of each game. For our review we have looked at the controls from inception of the various games to the actual playing and redemption of prizes.

ILC – Interprovincial Lottery Corporation is an inter-provincial body that collaborates and facilitates the sharing of information, games, relevant data and policies and procedures amongst the various Canadian lotteries. ILC is also the recipient of yearly minimum control standard reports conducted by the various Canadian Lotteries external auditors.

KOBETRON TESTING – refers to an automated testing of code imprinted on a microchip against a known KOBETRON signature of the information that should be on the microchip. ALC uses this control to ensure that no individual is able to gain unauthorized physical access to a VLT machine and legitimate microchips.

LRN – Lottery Retail Network, which represents the in-store lottery infrastructure which connects the Lottery Retail Terminals used to sell Lotto 6/49 and other instant games, validate tickets to determine winning status and the network infrastructure used to connect these devices back to ALC's datacenters.

LRT – Lottery Retail Terminal are the terminals that are used by retailers to sell and validate online and other instant games.

LSS – Lottery Support Services is a group within ALC that handles the collection of all phone and email related queries and complaints by individuals and retailers about ALC's games or offerings.

ONLINE LOTTERY – represents the traditional lottery products that are shared nationally (such as LOTTO 6/49) and regionally (such as Atlantic 49). These games are centrally tracked in the AEGIS systems and delivered to the retailer chain via the Lottery Retail Network.

PCI - Payment Card Industry security standards that are designed to ensure a common level of security of the end users data.

PIPEDA - Personal Information Protection and Electronic Documents Act is Canadian legislation that outlines the protection of various elements of personal information collected by an organization or agency.

PHISHING ATTACK – refers to an action undertaken to trick an individual to provide private or sensitive information in an attempt to subsequently steal that person's identity. Typically, this is undertaken by sending an email with a link that looks as if it was originated by the correct organization; however, in reality the person who clicks on the link is directed to a second webpage designed to look as if it came from the legitimate organization.

POLITE SHUTDOWN – represents a nightly automated process that ALC initiates to all of its Video Lottery Terminals in the wide area gaming network that powers down and reinitializes the units so that an automated integrity test can be performed. The results of this process are centrally monitored by ALC for completion and accuracy. In the event a VLT unit does not pass the automated integrity test, it is possible that the unit has been subject to unauthorized changes and the machine is put into a non-playable state until a VLT technician can assess and rectify the issues causing the failure.

The polite shut down is also in place to ensure that ALC's responsible gaming initiatives are met and that no off-hour VLT play can occur.

PROGRAM VALIDATION DISABLE – represents an automatic monitoring process that results in a centralized alarm for events occurring within either a VLT or EGD, i.e., access to the logic board area, incorrect game loaded, alteration of the unit, inconsistent security configuration etc.

ROOT ACCOUNT – represents the highest administrative account within a Unix based system.

SECURITY & COMPLIANCE – is a group within ALC that is responsible for investigating all significant wins, all allegations of inappropriate activities and other special investigations required by ALC or its Shareholders.

SEGREGATION OF DUTIES – refers to assigning different people the responsibilities of authorizing transactions, recording transactions, and maintaining custody of assets and is intended to reduce the opportunities to allow any person to be in a position to both perpetrate and conceal errors or fraud in the normal course of the person's duties.

SHAREHOLDERS – refers to Lotteries Commission of New Brunswick, Province of Newfoundland and Labrador, Nova Scotia Gaming Corporation and Prince Edward Island Lotteries Commission.

SOFTWARE EASTER EGG – is unauthorized code that is placed within the main application which could result in non-authorized functionality if the user inputs a predefined series of commands or actions.

SSH – Secure Shell is a Unix-based network protocol for establishing a secure channel between two computers to allow for logical access to a remote computer.

VALIDATION CODE – refers to a uniquely generated number based on the numbers played within a ticket that is used in the determination within AEGIS that the ticket is a legitimate ticket for which a prize is available.

VIDEO SITE CONTROLER – refers to a computer within each Video Lottery Terminal site that connects all the individual VLT units together and is responsible for collecting all game activity and polling this information back to ALC.

VLT – Video Lottery Terminal is the device used by customers of ALC to play video lottery games. These devices are rented out to the public for placement in public places such as restaurants, bars, and lounges.

VLT PROTOCOL STANDARD – is a vendor maintained document that outlines the various computer requirements that all hardware, software applications and games need to have built within them to be able to communicate with ALC's backend gaming environment.

WIDE AREA GAMING NETWORK – represents the collective secure infrastructure connecting the remote VLT machines back to ALC's datacenters. This does not include any VLT systems located within the Charlottetown Driving Park Entertainment Center.