GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Chief Financial Officer

Office of Integrity and Oversight

MEMORANDUM

TO: Jeffery Young, Interim Executive Director
DC Lottery and Charitable Games Control Board

FROM: Mohamad Yusuff, Interim Executive Director
Office of Integrity and Oversight

DATE: October 23, 2009

SUBJECT: Final Report on the Facilitation of the Information Technology (IT) Department's Information Security/Internal Controls "Self Assessment" Process at the D.C. Lottery and Charitable Games Control Board (Report No: IA: DCLB:2804-C11)

Attached for your information and record is the final report on the Facilitation of the Information Technology (IT) Department's Information Security/Internal Controls "Self Assessment" Process at the D.C. Lottery and Charitable Games Control Board (DCLB), prepared by the internal auditors of the Office of Integrity and Oversight (OIO). Because this project was a "self assessment" conducted by DCLB, the objective of our assignment was to facilitate and document the process and make an evaluation.

Our draft report on the DCLB IT "Self Assessment" process (No: IA: DCLB:2804-C11), issued September 25, 2009, noted that after several "learning" sessions, the Lottery IT "Self Assessment" group developed an effective and coherent process of: 1) evaluating critical IT components and/or operational issues; (2) qualitatively measuring the risk, potential loss, and probability of loss for the selected critical components; (3) identifying the potential risk mitigation safeguards and the proposed corresponding plan of actions and milestones (POAM). However, we observed the following deficiencies in the "Self Assessment" process:

- Minutes of the brainstorming sessions were unavailable and caused inefficiencies in the overall "Self Assessment" process.

- The DCLB IT Risk Analysis draft Report was not done until April 2009 and finalized in June 2009, and thus loses much of its information value.

- Lack of Referencing (or Cross-Walk) to NIST SP 800-53 Risk Assessment Procedures in the DCLB IT Risk Analysis Report.

In its response, DCLB concurred with the report's findings and recommendations and has taken, or is in the process of taking corrective actions to address the noted issues. We have attached a copy of the agency's entire response as Appendix 1 of this report. A follow-up review will be conducted within six (6) months from the date of this correspondence to ensure that the agency's planned actions are implemented efficiently and effectively.

Should you have any questions, please contact me at 442-6433 or Nelson Alli at 442-8274.

Attachment

cc: Natwar M. Gandhi, Chief Financial Officer, Government of the District of Columbia
Lucille Dickinson, Chief of Staff, Office of the Chief Financial Officer
Angell Jacobs, Director of Operations, OCFO
Bruce Jones, Director, Information Technology Department, DCLB
Gwen Washington, Audits Coordinator, Executive Office, DCLB
Charles Fultz, Internal Security Director, OIO
Nelson Alli, Interim Internal Audit Director, OIO
Tony The', Audit Manager, OIO

FINAL REPORT ON
THE FACILITATION OF THE INFORMATION SECURITY/INTERNAL CONTROLS "SELF ASSESSMENT" PROCESS AT THE DISTRICT OF COLUMBIA LOTTERY AND CHARITABLE GAMES CONTROL BOARD (DCLB)

TABLE OF CONTENTS

FINAL REPORT ON THE FACILITATION OF THE INFORMATION SECURITY/INTERNAL CONTROLS "SELF ASSESSMENT" PROCESS AT THE DISTRICT OF COLUMBIA LOTTERY AND CHARITABLE GAMES CONTROL BOARD (DCLB)

EXECUTIVE SUMMARY

As part of the annual work plan of the Office of Integrity and Oversight (OIO), the internal auditors of this office performed a facilitation of the DCLB Information Technology (IT) Department's Information Security/Internal Controls "Self Assessment" Process. OIO was involved in the facilitation of the DCLB's "Self Assessment" process during the period between January and September 2008.

The IT Department's Information Security/Internal Controls "Self Assessment" started with a methodology research period that took place between January and March 2008 and continued with a series of brainstorming sessions during the summer of 2008. However, the "Self Assessment" Report was not drafted until April 2009 due to the IT Department's other urgent priorities.

Because this project was a "self assessment" conducted by DCLB, the objective of OIO was to facilitate and document the process and make an evaluation. We are attaching the DCLB Information Technology "self assessment" documentation and the related plan of actions addressing the risks identified during the assessment.

RESULTS OF REVIEW

Our evaluation of the DCLB IT "Self Assessment" process is that after several "learning" sessions, the group developed an effective and coherent process of: (1) evaluating critical IT components and/or operation issues; (2) qualitatively measuring the risk, potential loss, and probability of loss for the selected critical components; (3) identifying the potential risk mitigation safeguards and the proposed corresponding plan of actions and milestones (POAM). However, we observed the following deficiencies in the "Self Assessment" process:

1. *Minutes of the Brainstorming Sessions were Unavailable and Caused Inefficiencies to the Overall "Self Assessment" Process:* Although it was agreed at the beginning of the brainstorming session that minutes were to be kept to record the session results, plan of actions, and milestones; the minutes were not available at the next session, nor were they available at the end of process. Unavailability of the minutes caused inefficiencies as the group had to spend time to recap the previous session's results. In addition, the lack of minutes caused certain important issues discussed at the brainstorming sessions to be omitted from the DCLB IT Risk Analysis Report.

2. *__The DCLB IT Risk Analysis Draft Report was not done until April 2009 and finalized in July 2009, and thus Loses much of its Information Value:__* We understand that the DCLB IT Department needed to devote its scarce resources to other urgent issues after the end of the 2008 brainstorming sessions; however, the Draft Report could have been completed earlier had the session minutes and other documentation been made available soon after the meetings were done. Due to the lack of proper documentation, the risk analysis report was not finalized until July 2009, and thus loses much of its information value.

3. *__Lack of Referencing (or Cross-Walk) to NIST SP 800-53 Risk Assessment Procedures in the DCLB IT Risk Analysis Report:__* Although the brainstorming sessions did consider and attempted to emulate the assessment procedures outlined in the NIST SP 800-53 Appendix F, the procedures were not reflected in the DCLB IT Risk Analysis Report, and thus may have security control gaps in its IT security plan when it is completed.

RECOMMENDATIONS

We present our recommendations in the respective sections of this report.

AGENCY'S RESPONSE

In its response, DCLB concurred with the report's findings and recommendations and has taken, or is in the process of taking corrective actions to address the noted issues. In our evaluation the corrective actions are responsive to the issues identified and when fully implemented should satisfy the intent of our recommendations. We attached a copy of the agency's entire response as Appendix 1 of this report.

FINAL REPORT ON THE FACILITATION OF THE INFORMATION SECURITY/INTERNAL CONTROLS "SELF ASSESSMENT" PROCESS AT THE DISTRICT OF COLUMBIA LOTTERY AND CHARITABLE GAMES CONTROL BOARD (DCLB)

INTRODUCTION AND PURPOSE

As part of the annual work plan of the Office of Integrity and Oversight (OIO), the internal auditors of this office performed a facilitation of the DCLB Information Technology (IT) Department's Information Security/Internal Controls "Self Assessment" Process. OIO was involved in the facilitation of the DCLB's "Self Assessment" process during the period between January and September 2008.

Because this project was a "self assessment" conducted by DCLB, the objective of OIO was to facilitate and document the process and make an evaluation. We are attaching the DCLB Information Technology "self assessment" documentation and the related plan of actions addressing the risks identified during the assessment.

OBJECTIVES, SCOPE, AND METHODOLOGY

Our facilitation of the DCLB Information Technology Department information security/internal controls "self assessment" process will accomplish the following:

- Facilitate and provide guidance on the "self-assessment" process by ensuring that a comprehensive coverage of risks is being addressed through the use of IT Industry/Federal Government information security/internal control checklists.
- Strengthen information security/internal controls of the DCLB in-house information system by identifying the associated risks and mitigating or minimizing them through corrective action plans.

As noted above, the scope of OIO/Internal Audit involvement with the facilitation of the DCLB's "Self Assessment" process was between January 2008 and August 2008.

To accomplish the objectives of our assignment, we performed the following procedures:

- Attended and facilitated DCLB Information Technology Department's Information Security/Internal Controls "Self Assessment" brainstorming and interview sessions – both at the departmental and sub-unit levels.
- Utilized the Information Technology Industry/Federal Government Information Security and Internal Controls publications and/or Checklists to ensure a comprehensive coverage of the "self assessment".
- The basic approach of the DCLB "self assessment" started with risk assessments (what "bad things" could happen to us?) and how the Lottery should mitigate or minimize the risks.
- Because this project was a "self assessment" conducted by DCLB, this report describes the process and makes an evaluation of the assessment. We are attaching herein the DCLB Information Technology "self assessment" documentation and the related plans of action to address the risks identified during the assessment.

FINAL REPORT ON
THE FACILITATION OF THE INFORMATION SECURITY/INTERNAL CONTROLS "SELF ASSESSMENT" PROCESS AT THE DISTRICT OF COLUMBIA LOTTERY AND CHARITABLE GAMES CONTROL BOARD (DCLB)

BACKGROUND

As noted above, the internal auditors of the Office of Integrity and Oversight (OIO) performed a facilitation of the DCLB Information Technology (IT) Department's Information Security/Internal Controls "Self Assessment" Process during the period of January through September 2008.

The IT Department's Information Security/Internal Controls "Self Assessment" started with a methodology research period that took place between January and March 2008 and continued with a series of brainstorming sessions during the summer of 2008. However, the "Self Assessment" Report was not drafted until April 2009 and was finalized in July 2009 due to the IT Department's other urgent priorities.

Among the research materials used by the IT department were IT Security and Internal Controls literatures such as:

1. ISO/IEC 27001:2005 – is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its full name is ISO/IEC 27001:2005 - Information Technology – Security Techniques – Information Security Management Systems – Requirements but it is commonly known as "ISO 27001".'
2. Control Objectives for Information and related Technology (COBIT) - A business-oriented set of standards for guiding management in the sound use of information technology from the Information Systems Audit and Control Association (ISACA). COBIT includes resources such as an executive summary, a framework, control objectives, audit guidelines, an implementation tool set, management guidelines and reference materials.
3. Global Technology Audit Guides (GTAG®) - Prepared by The Institute of Internal Auditors (The IIA), each Global Technology Audit Guide(GTAG) is written in straightforward business language to address a timely issue related to information technology (IT) management, control, and security.
4. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39, Managing Risk from Information Systems: An Organizational Perspective. - SP 800-39 provides a framework for managing the risk arising from the operation and use of information systems and is built upon a common foundation of best security practices.
5. National Institute of Standards and Technology (NIST) Special Publication 800-53 - Recommended Security Controls for Federal Information Systems. The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store,

or transmit federal information. The SP 800-53 guidelines were developed to help achieve more secure information systems within the federal government.

At the beginning of the brainstorming sessions, the IT Department "Self Assessment" group initially decided to use the NIST SP 800-53 Security Control Catalog (Appendix F) list of security topics to assess the related Lottery IT risks. The table below highlights the group's phase 1 Information Security/Internal Control risk rankings (H = High; M = Medium; L = Low):

Control No.	Control Name	Risk Ranking
AC-1	Access Control Policy	H
AC-2	Account Management	H
AC-3	Access Enforcement	H
AC-4	Information Flow Enforcement	M
AC-7	Unsuccessful Login Attempts	M
AC-8	System Use Notification	M
AC-9	Previous Logon Notification	M
AC-13	Supervision and Review – Access Control	H
AC-19	Access Control for Portable and Mobile Devices	H
AT-1	Security Awareness and Training Policy and procedures	L
AT-3	Security Training	L
AU-1	Audit and Accountability Policy and Procedures	H
AU-6	Audit Monitoring, Analysis, and Reporting	H
AU-11	Audit Record Retention	L
CA-2	Security Assessments	H
CA-7	Continuous Monitoring	H
CM-1	Configuration Management Policy and Procedures	H
CM-2	Baseline Configuration	M
CM-3	Configuration Change Control	H
CM-4	Monitoring Configuration Changes	M
CM-5	Access Restrictions for Change	H
CM-6	Configuration Settings	M
CM-7	Least Functionality	H
CM-8	Information System Component Inventory	H
CP-1	Contingency Planning Policy and Procedures	L
CP-2	Contingency Plan	M
CP-3	Contingency Training	M
CP-4	Contingency Plan Testing and Exercises	M
CP-5	Contingency Plan Update	M
CP-6	Alternate Storage Site	L
CP-7	Alternate Processing Site	L
CP-8	Telecommunication Services	H

CP-9	Information System Backup	H
CP-10	Information System Recovery and Reconstitution	H
IR-1	Incident Response Policy and Procedures	M
IR-2	Incident Response Training	L
IR-3	Incident Response Testing and Exercises	L
IR-4	Incident Handling	H
IR-5	Incident Monitoring	H
IR-6	Incident Reporting	H
IR-7	Incident Response Assistance	H
MA-1	System Maintenance Policy and Procedures	H
MA-2	Controlled Maintenance	H
MA-3	Maintenance Tools	M
MA-4	Remote Maintenance	L
MA-5	Maintenance Personnel	H
MA-6	Timely Maintenance	H
MP-1	Media Protection Policy and Procedures	M
PL-1	Security Planning Policy and Procedures	H
PL-5	Privacy Impact Assessment	M
PS-7	Third Party Personnel Security	H
RA-1	Risk Assessment Policy and Procedures	H
RA-2	Security Categorization	H
RA-3	Risk Assessment	H

In an attempt to prioritize and mitigate the above noted risks, the "Self Assessment" group discovered that the above risk topics are designed for a large Federal Agency information system and are not really appropriate for addressing the risks facing the Lottery information system components and related current IT operation issues at DCLB. Therefore, the "Self Assessment" group decided to:

1. Evaluate which Lottery information technology components have high impact to mission-critical business processes.
2. Select the identified critical components for further analysis.
3. Qualitatively measure the risk, potential loss, and probability of loss for the selected critical components.
4. Identify the potential risk mitigation safeguards and the proposed corresponding plan of actions and milestones (POAM) as recommended by NIST SP 800-39.

During the summer brainstorming sessions, the "Self Assessment" group identified the following IT components that have high impact on the Lottery's mission-critical business processes and analyzed the components as described above (for details – see Exhibit I DCLB Information Systems Risk Analysis - Facilitated Risk Self-Assessment of the Lottery's Critical Information Technology Components):

1. The Internal Control System (ICS).
2. Oracle General Ledger.
3. Agent Management System.
4. Claims Processing System.
5. Network Infrastructure and Common Controls – including the IBM p520 migration project and the power interruption issues.

In addition to the above assessments, the group also produced a preliminary skeleton draft report of the Risk Analysis which has the following general structure:

1. General Information (incl. purpose, scope, systems overview, etc.).
2. Project and System Description (incl. summary description, risk management structure, periodic risk assessment, and contingency planning).
3. System Security (incl. baseline security requirement, baseline security safeguards, sensitivity level of data, user security investigation level and access need).
4. Risk and Safeguards (of the identified critical components).
5. Risk Reduction Recommendations (to the Lottery Executive Committee).

Our evaluation of the DCLB IT "Self Assessment" process is that after several "learning" sessions, the group developed an effective process of: (1) evaluating critical IT components and/or operation issues; (2) qualitatively measuring the risk, potential loss, and probability of loss for the selected critical components; (3) identifying the potential risk mitigation safeguards and the proposed corresponding plan of actions and milestones (POAM).

As noted in the DCLB IT Risk Analysis Report (Exhibit 1), the risk self-assessment process led to:

1. The risk of unavailability of a computer operator to handle ICS monitoring **being mitigated** by cross departmental training of other Lottery departments' personnel and new hires.
2. The loss of vendor support for the Oracle General Ledger application **was resolved by** purchasing a Computer Based Training curriculum for Oracle 11i E-Business Suite for Oracle General Ledger. Moreover, Finance department users have taken Oracle12i E-Business Suite (the next version in the migration path) classroom

training, and have subsequently increased their product knowledge and self-support ability.

3. The risk of unauthorized disclosure of privacy data because of unrestricted access to the Agent Management System database **were mitigated by**: (1) application program changes to isolate display of sensitive data; (2) enabling appropriate access level security to the system's Active Directory database shared file.
4. The risk of unauthorized disclosure of privacy data because of unrestricted access to the Claim Processing System (currently under development) database **were mitigated by** (1) application program changes to isolate display of sensitive data; (2) changing the underlying database from Microsoft Access to Microsoft SQL-Server 2005 and thereby providing enterprise security and reliability.

However, the following deficiencies in the "Self Assessment" process were noted:

1. Minutes of the brainstorming sessions were supposed to be done but did not happen – the unavailability of the minutes caused inefficiencies for subsequent sessions and certain issues addressed at the sessions (such as the IBM p520 migration project) were not being documented and thus not reflected in the DCLB IT Risk Analysis Draft Report.
2. The DCLB IT Risk Analysis Draft Report was not done until April 2009 and finalized in July 2009, and thus loses much of its information value.
3. Although the brainstorming sessions did consider and attempted to emulate the assessment procedures outlined in the NIST SP 800-53 Appendix F, the procedures were not reflected in the DCLB IT Risk Analysis Report, and thus may have security control gaps in its IT security plan when it is completed.

RESULTS OF REVIEW

In general, our evaluation of the DCLB IT "Self Assessment" process is that after several "learning" sessions, the group developed an effective and coherent process of: (1) evaluating critical IT components and/or operation issues; (2) qualitatively measuring the risk, potential loss, and probability of loss for the selected critical components; (3) identifying the potential risk mitigation safeguards and the proposed corresponding plan of actions and milestones (POAM). However, as noted above, there were certain deficiencies in the "Self Assessment" process. We understand that the IT department is planning to continue the risk and security "Self Assessment" in the fall of 2009. Therefore, it is critical that the identified deficiencies be corrected to improve the "Self Assessment" process. The noted deficiencies were as follows:

1. Minutes of the Brainstorming Sessions were Unavailable and Caused Inefficiencies to the Overall "Self Assessment" Process.
2. The DCLB IT Risk Analysis draft Report was not done until April 2009 and finalized in June 2009, and thus loses much of its information value

3. Lack of Referencing (or Cross-Walk) to NIST SP 800-53 Risk Assessment Procedures in the DCLB IT Risk Analysis Report.

FINDINGS AND RECOMMENDATION

1. Minutes of the Brainstorming Sessions were Unavailable and Caused Inefficiencies to the Overall "Self Assessment" Process

Although it was agreed at the beginning of the brainstorming session that minutes were to be kept to record the session results, plans of action, and milestones; the minutes were not available at the next session, nor were they available at the end of process. The unavailability of the minutes caused inefficiencies as the group had to spent time to recap the previous session's results. In addition, the lack of the minutes caused certain important issues discussed at the brainstorming sessions to be omitted from the DCLB IT Risk Analysis Report.

Recommendation

We recommend that the minutes be done and approved by the group at the next session of the 2009 DCLB IT "Self Assessment" process.

Agency's Response

DCLB agrees. The IT Department has developed Standard Operating Procedures describing in detail the process for IT "Self Assessment." The SOP mandates that meeting notes be completed within 3 business days and distributed prior to the next meeting for review and approval by the team participants.

OIO Auditor Evaluation

DCLB's planned action is responsive to the issue identified, and when fully implemented should satisfy the intent of our recommendation.

2. The DCLB IT Risk Analysis Draft Report was not done until April 2009 and finalized in July 2009, and thus Loses much of its Information Value

We understand that the DCLB IT Department needed to devote its scarce resources to other urgent issues after the end of the 2008 brainstorming sessions; however, the Draft Report could have been completed earlier, had the session minutes and other documentation been made available soon after the meetings were done. Due to the lack of proper documentation, the risk analysis report was not done until April 2009 and finalized in July 2009, and thus loses much of its information value.

Recommendation

To preserve the information value of the "Self Assessment" process, we recommend that the report should be produced soon after the brainstorming sessions are completed.

Agency's Response

DCLB agrees. The IT Department has developed Standard Operating Procedures describing in detail the process for IT "Self Assessment". The SOP mandates that the Draft Report be completed within 30 days of the fourth Risk Assessment meeting, thus ensuring that the report is complete within 90 days of the IT Risk Self- Assessment Project start.

OIO Auditor Evaluation

DCLB's planned action is responsive to the issue identified, and when fully implemented should satisfy the intent of our recommendation.

3. ***Lack of Referencing (or Cross-Walk) to NIST SP 800-53 Risk Assessment Procedures in the DCLB IT Risk Analysis Report***

Although the brainstorming sessions did consider and attempted to emulate the assessment procedures outlined in the NIST SP 800-53 Appendix F, the procedures were not reflected and were only briefly mentioned in the DCLB IT Risk Analysis Report.

We observed that the group agreed at the early brainstorming sessions that the NIST Special Publication 800-53 be used as a reference in the risk assessment process to give the "Self Assessment" process a more structured guidance. In addition, the group has made an effort to rank the Lottery IT Security Risks using the NIST SP 800-53 Security Control Catalog (Appendix F) list of security topics (see background section above). However, the DCLB IT Risk Analysis Report did not cross-walk the ranked IT security risks to the main results of the "Self Assessment," and thus may have security control gaps in its IT security plan when it is completed.

Recommendation

We recommend that the 2009 Risk Analysis "Self Assessment" report cross-walk an updated IT Security Ranked Risks to the main results of the report and the IT Security Plan when it is completed.

Agency's Response

DCLB agrees. The IT Department has developed Standard Operating Procedures describing in detail the process for IT "Self Assessment". The SOP mandates that the Draft Report contain a traceability matrix which cross-walks the updated IT Security Ranked Risks to the IT Security Plan.

OIO Auditor Evaluation

DCLB's planned action is responsive to the issue identified, and when fully implemented should satisfy the intent of our recommendation.

EXHIBIT 1

Exhibit 1: Report on DCLB Information Technology Risk Analysis – 18 pages

DCLB

INFORMATION TECHNOLOGY

RISK

ANALYSIS

A Facilitated Risk Self-Assessment (FRAP) of the DC Lottery's Critical Information Technology Components

Final Revision - July, 2009

RISK ANALYSIS

TABLE OF CONTENTS

Page #

1.0 GENERAL INFORMATION

1.1 Purpose

This document describes the Risk Self-Assessment tasks and activities conducted during the summer of 2008. Over the course of several months, the DCLB IT Department, facilitated by the OCFO Office of Integrity and Oversight Internal Audit Unit, evaluated as to which the Lottery's information technology components: 1) have high impact to mission-critical business processes; 2) to select critical components for further analysis; 3) to qualitatively measure the risk, potential loss, and probability of loss for the selected critical components; and 4) to identify the potential risk mitigation safeguards and the proposed corresponding plan of actions and milestones to implement these safeguards as recommended in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39.

The Risk Self-Assessment is the process of enumerating risks, determining their classifications, assigning probability and impact scores, and associating controls with each risk.

1.2 Scope

The scope of the Risk Analysis as it relates to the project was identified during the categorization phase, referenced back to the DCLB-Continuity of Operation Planning Documentation (TS-COOP) risk category mapping by critical business processes, as follows:

Identifier	IT Critical Component	Business Process Name	System & Data Owners and IT Support Manager
1	Internal Control System	Proofing of Agent Invoicing, Cash controls	Elsym, Finance S. Sharma
2	Oracle General Ledger	Month End Closing of Gaming Activities	IT Pundits, Finance S. Sharma
3	Agent Management System	Manage Licenses – Provide New Agent Lottery Licenses	DCLB, Licensing B. Gray
4	Claims Processing System	Claim Processing, MUSL Winning ticket approval, Cash controls	DCLB, Customer Service B. Gray
5	Network infrastructure and common controls	All	IT OCTO Network Support

1.3 Systems Overview

This section provides a brief system overview description as a point of reference for the remainder of the document.

1.3.1 Internal Control System (ICS)

- Responsible Department for application data content - Finance
- System name or title - DCLB Lottery Financials Internal Control System
- System code
- System category
  - *Major application*: performs clearly defined functions for which there is a readily identifiable security consideration and need
- Operational status
  - Operational
- System environment and special conditions

1.3.2 Oracle General Ledger

- Responsible Department for application data content - Finance
- System name or title - Oracle 11i E-Business Suite for General Ledger Applications
- System code
- System category
  - *Major application*: performs clearly defined functions for which there is a readily identifiable security consideration and need
- Operational status
  - Undergoing a major modification
- System environment and special conditions

1.3.3 Agent Management System (AMS)

- Responsible Department for application data content - Licensing and Charitable Games
- System name or title - Lottery Retailer (Agent) Management System
- System code
- System category
  - *Major application*: performs clearly defined functions for which there is a readily identifiable security consideration and need
- Operational status
  - Operational
- System environment and special conditions

1.3.4 Claims Processing System

- Responsible Department for application data content - Customer Service
- System name or title - Lottery Winners Claims Processing System
- System code
- System category
  - *Major application*: performs clearly defined functions for which there is a readily identifiable security consideration and need
- Operational status
  - Under development
- System environment and special conditions

1.3.5 Network and Common Controls

- Responsible Department for systems' infrastructure, computer hardware and software maintenance and support - Information Technology
- System name or title - Active Directory and Network Intrusion Detection
- System code
- System category
  - *General support system*: provides general ADP or network support for a variety of users and applications
- Operational status
  - Operational
- System environment and special conditions

1.4 Project References

The following is a list of the references that were used in preparation of this document.

- *DCLB Continuity of Operations Plan*
- *DCLB Business Continuity and Disaster Recovery Executive Plan*
- *DCLB ICS Operators Manual*
- *DCLB Operators Checklist*

1.5 Acronyms and Abbreviations

This section contains a list of the acronyms and abbreviations used in this document and the meaning of each.

1.6 Points of Contact

1.6.1 Information

This section provides a list of the points of organizational contact (POC) who may be needed by the document user for informational and troubleshooting purposes. Include type of contact, contact name, department, telephone number, and e-mail address (if applicable). Points of contact may include, but are not limited to, helpdesk POC, development/maintenance POC, and operations POC.

Name	Role	Responsibility	Contact Number
Bruce Jones	Director, IT department	Chairperson, leads DRM team, delegate tasks to other teams. Reports status to Steering Committee	(202)645-8054(main) (202)645-9268(ext)
Tony The'	Auditor, Office of Integrity and Oversight	Facilitation of risk assessment activities.	(202)645-7900(main) (202)645-9324 (ext)
Position Vacant	Program Manager, IT department	Help chairman to coordinate activities of disaster recovery. Lead specific tasks of system recovery	(202)645-9248(main)
John Ogungbemi	Chief, Network administration	Help chairman to coordinate activities of disaster recovery. Lead tasks of network infrastructure recovery	(202)645-8054(main) (202)645-8061(ext)
Sudipta Sharma	Chief, Network administration	Facilitation of risk assessment activities.	(202)645-7900(main) (202)645-8075(ext)
Anthony Samuel	Network Administrator	Help chairman to coordinate activities of disaster recovery.	(202)258-0799(mobile)
Keith Cunningham	Telecommunications Specialist	Help chairman to coordinate activities of disaster recovery. Lead lottery drawing-associated tasks of disaster recovery	(202)645-8055(main) (202)645-8969(ext)
William Gray	Software Developer	Help chairman to coordinate activities of disaster recovery. Lead license-associated tasks of disaster recovery	(202)645-8090(main) (202)645-8968(ext)

Major Application	Technical Contact	Departments Involved	List Employee Contacts (primary and backup)
1. ICS	Elsym Consulting, Inc Ken Wyman Vice President, Lottery Services (678) 564-5061 ken.wyman@elsym.com	Budget and Finance	Mike Brown 645-8085 Stephon Bing 645-6993 Allen Evans 645-9002
2. Oracle General Ledger	IT Pundits Arvind Abraham (703) 371-4111 abraham_arvind@yahoo.com	Budget and Finance	Mike Brown 645-8085 Allen Evans 645-9002 Bill Robinson 645-8084
3. Agent Management	William Gray DCLB IT	Licensing and Charitable Games	Sarita Curtis 320-6533 Jeff Anderson 320-6519
4. Claim Processing	William Gray DCLB IT	Customer Services	Anne McPherson 671-2676 Cheryl Malone 671-2606

1.6.2 Coordination

This section contains a list of organizations that require coordination between the project and its specific support function (e.g., installation coordination, security, etc.). Include a schedule for coordination activities.

2.0 PROJECT AND SYSTEM DESCRIPTION

2.1 Summary

Following best-practices associated with the Facilitated Risk Analysis Process (FRAP), DCLB IT undertook this project to qualitatively access the risks to the following critical systems:

- Internal Control System
- Oracle General Ledger Application
- Agent Management System
- Automated Claims Processing System (in development)

Using standards and guidelines developed by the National Institute of Standards and Technology (NIST) for federal agency compliance with OMB mandates, Federal Information Processing Standards (FIPS) and Federal Information Security Management Act (FISMA) of 2002, the DCLB risk assessment team followed the NIST Risk Management Framework.

According to NIST, security controls are organized into *classes* and *families* for ease of use in the control selection and specification process. The matrix below summarizes the seventeen security control families identified by NIST.

	FAMILY	CLASS
1.	Access Control	Technical
2.	Awareness and Training	Operational
3.	Audit and Accountability	Technical
4.	Certification, Accreditation, and Security Assessments	Management
5.	Configuration Management	Operational
6.	Contingency Planning	Operational
7.	Identification and Authentication	Technical
8.	Incident Response	Operational
9.	Maintenance	Operational
10.	Media Protection	Operational
11.	Physical and Environmental Protection	Operational
12.	Planning	Management
13.	Personnel Security	Operational
14.	**Risk Assessment**	**Management**
15.	System and Services Acquisition	Management
16.	System and Communications Protection	Technical
17.	System and Information Integrity	Operational

2.1.1 Project Management Structure

The project was sponsored by the Director of the IT department and facilitated by the Auditor for the OCFO Office of Integrity and Oversight. While the project was completed in December 2008, this final document deliverable was not completed

2.2 Risk Management Structure

The DCLB IT department has taken the lead in organizing an Agency-wide Risk Management Structure modeled after the World Lottery Association's Information Security Management System (ISMS), which is a lottery-specific extension of the ISO 27001[1] security standard.

Moreover, the DCLB IT department adheres to the security policies and practices of the DC Office of Chief Technology Officer (OCTO), DC OCFO Chief Information Officer, and the Multi-State Lottery Association (MUSL), which DCLB is a member.

In addition, the DCLB IT ISMS follows the guidance of the US Office of Management and Budget (OMB), US General Accounting Office (GAO), and the National Institute of Standards and Technology (NIST), with regards to information security objectives and risk management practices.

2.3 Periodic Risk Assessment

Starting in August 2009, the DCLB IT department will annually re-evaluate this risk assessment efforts focusing primarily on (1) determining if controls were in place and operating as intended to reduce risk and (2) evaluating the effectiveness of the risk assessment in communicating policies, raising awareness levels, and reducing incidents.

2.4 Contingency Planning

The DCLB IT department has developed detailed continuity of operations planning (COOP) for the ICS system, which is critical to the lottery gaming operations. The Oracle General Ledger and Agent Management System do not have the availability requirements of ICS and have not been incorporated into the detailed COOP – however, the DCLB continuity of operations plan addresses the recovery of business functions, systems, platforms, application software, and business data installed and maintained by the DCLB staff, including the restoration of the DCLB LAN. This strategy is limited in that it will only assist DCLB's internal departments to prepare for disaster. While Lottery Technology Enterprises (LTE), located on the 1st floor at DCLB Headquarters will benefit from this strategy, they are responsible for the development of their own risk management and continuity of operations plans.

The DCLB COOP Plan provides a foundation for any disaster recovery effort within DCLB. It establishes a group of committees to oversee and improve upon the COOP Plan; describes the responsibilities of the disaster recovery leadership; and outlines the steps that will need to be taken should a disaster occur. While this document was developed to provide guidance when disaster happens, it does not promise all the answers to disaster recovery.

The COOP Plan is a living document, which needs to be constantly tested, reviewed, and revised to meet the ever-changing demands of DCLB. The responsibility of managing and administering the COOP Plan is distributed between several committees, which include the Steering Committee, Disaster Recovery Management Team, Damage Assessment Team, Specialists, and Disaster Recovery Technical Team.

[1] Its full name is *ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements* but it is commonly known as "ISO 27001".

3.0 ANALYSIS SCOPE

Based on the environment, scope, sensitivity of the data, and criticality of various DCLB information technology systems to their project sponsors and users, we decided to target the following systems within the scope of this risk analysis:

- Internal Control System
- Oracle General Ledger Application
- Agent Management System
- Automated Claims Processing System (in development)

In our analysis we assessed the security requirements and specifications necessary to safeguard each of the systems and their corresponding data, including such information as privacy requirements, estimated dollar value of assets, and contingency planning requirements (including the Business Resumption Plan).

3.1 Criteria of Risk Assessment

Information Assets Risks are divided in three criticality levels and the above systems are considered Level 1 applications.

Level 1: **Most Critical** – The information assets are classified with highest level of sensitivity. The data in the category can be labeled as "District Government Restricted" as guided in OCTO's Citywide IT Security Program's document "Data Sensitivity Policy"

Level 2: **Critical** – The information assets are classified with moderate level of sensitivity. The data in the category can be labeled as "District Government Internal Use Only" as guided in OCTO's "Data Sensitivity Policy" document.

Level 3: **Least Critical** – The information assets are classified with low level of sensitivity. The data in the category can be labeled as "District Government Nonpublic" as guided in OCTO's "Data Sensitivity Policy" document.

3.2 Security Categories

FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur. The potential impacts could jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

FIPS 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing Federal information and information systems for each of three stated security objectives (confidentiality, integrity, and availability).

As reflected in Table 1, FISMA and FIPS 199 define three security objectives for information and information systems.

Table 1: Information and Information System Security Objectives

Security Objectives	FISMA Definition [44 U.S.C., Sec. 3542]	FIPS 199 Definition
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"	A loss of confidentiality is the unauthorized disclosure of information.
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"	A loss of integrity is the unauthorized modification or destruction of information.
Availability	"Ensuring timely and reliable access to and use of information…"	A loss of availability is the disruption of access to or use of information or an information system.

3.2 Impact Assessment

FIPS 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest. Table 2 provides FIPS 199 potential impact definitions.

Table 2: Potential Impact Levels

Potential Impact	Definitions
Low	The potential impact is **low** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.7 A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The potential impact is **moderate** if—The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

High	The potential impact is **high** if—The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

In FIPS 199, the security category of an information type can be associated with both user information and system information8 and can be applicable to information in either electronic or non-electronic form. It is also used as input in considering the appropriate security category for a system. Establishing an appropriate security category for an information type simply requires determining the *potential impact* for each security objective associated with the particular information type. The generalized format for expressing the security category, or *SC*, of an information type is:

Security Category$_{\text{information type}}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)} where the acceptable values for potential *impact* are low, moderate, high, or not applicable.

4.0 RISKS AND SAFEGUARDS

This section highlights the Lottery's Information System Components that were identified by the project task-force as being mission-critical. The sub-sections below described the system component's risk categories being identified, the evaluated degrees of risk probability and impact, the related potential safeguards, and the corresponding risk mitigation implementation plan of action and milestone (POAM).

4.1 ICS – Risk Assessed: Operator Unavailable

4.1.1 Risk Category

Availability

4.1.2 Risk Impact/Probability

High/High

4.1.3 Potential Safeguard(s)

1. Operations Resource Management – *see 4.1.3.1*
2. Monthly Schedule – *an SOP has been developed and a fulltime Lead Operator position was filled in February 2009, which has responsibility for developing the Monthly Operations Schedule.*
3. Cross Departmental Training – *in December 2008, the IT Department accelerated it's cross-departmental training program, providing 4 additional backup operations staff persons from the Finance, Support Services, Draw and Resource Management business-units.*
4. Business Process Reengineering – *see 4.1.3.1*
5. Temp Agency – *further research indicated that MUSL security requirements do not allow temporary operators, and therefore, this is not a viable safeguard.*

4.1.3.1 Operations Resource Management

A review of operations procedures and needs analysis was completed. Cross departmental-training was conducted allowing for additional resources from other the Finance and Draw departments. Moreover, additional IT staff persons have been trained in the ICS operations and Draw closing procedures, and new operations staff were hired in early FY09. As of June 2009, the IT Department's operations unit has been fully staffed, which includes one (1) lead full-time operator, two (2) full-time operators, and three (3) part-time operators.

4.1.3.2 Business Process Reengineering

The ICS business process was reviewed and successfully modified to reduce task complexity and unnecessary report distribution. The BPR reduced the time to cross-train staff in ICS operations by 24 hours.

4.2 ICS – Risk Identified: Operator Error

4.2.1 Risk Category

Confidentiality, Integrity, Availability

4.2.2 Risk Impact/Probability

Low/High

4.2.3 Potential Safeguard(s)

1. Software Audit Policies – *an SOP will be developed by October 2009*
2. Automated Software Controls – *an SOP will be developed by October 2009*
3. Improve Operations SOP – *see 4.2.3.1*
4. Improved Training – *see 4.2.3.2*

4.2.3.1 Improved Operations SOP

ICS operations standard operating procedures are being reviewed and revised in regards to process improvements implemented per the Business Process Re-engineering.

4.2.3.2 Improved Operations Training

Training has been improved. However, there is a need for new operations training core curriculum to assist new hires in coming to speed in ICS processes. The IT department plans to develop a formalized new computer operators training program by the October 2009.

4.3 Oracle GL – Risk Identified: Loss of Vendor Support

4.3.1 Risk Category

Confidentiality, Integrity, Availability

4.3.2 Risk Impact/Probability

High/Medium

4.3.3 Potential Safeguard(s)

1. Documented Business Processes – *see 4.3.3.1*
2. Oracle Financials Administration Training – *see 4.3.3.2*
3. Documented Migration and Configuration Plan – *a plan will be developed by October 2009*

4.3.3.1 Documented Business Process

As part of the Oracle Financials upgrade and migration, and the Oracle GL Data Warehouse and Business Intelligence projects, the Oracle General Ledger component architecture is being thoroughly documented.

4.3.3.2 Oracle Financials Training

The IT department has purchased a Computer Based Training curriculum for Oracle 11i E-Business Suite for Oracle General Ledger. Several members of the department have completed the curriculum as well as vendors not currently providing Oracle GL support. Moreover, Finance department staff have taken Oracle 12i E-Business Suite (the next version in the migration path) classroom training, and have subsequently increased their product knowledge and self-support ability.

4.5 AMS - Risk Identified: Possibility of Unauthorized Disclosure of Privacy Data

The Agent Management System contains personal identifying information, in the form of addresses, phone numbers, birth dates, social security numbers and employer tax identifiers. Through analysis it was determined that access to this data was unrestricted, requiring **immediate risk mitigation**.

4.5.1 Risk Category

Confidentiality

4.5.2 Risk Impact/Probability

High/Medium

4.5.3 Potential Safeguard(s)

1. Programmatic changes to the application to isolate display of sensitive data
2. Redesign of the underlying Access tables to isolate and encrypt sensitive data
3. Enable Active Directory appropriate access level security to the Access database shared file

4.5.3.1 AMS Safeguards Implemented

All the above safeguards including data encryption have been implemented.

4.6 Claims Processing - Risk Identified: Possibility of Unauthorized Disclosure of Privacy Data

The Claims Processing application, under development, contains personal identifying information, in the form of addresses, phone numbers, birth dates, and social security numbers. Through analysis it was determined that access to this data would be unrestricted, and that data would be transmitted over the

DC-WAN, as well as the DCLB LAN. Due to our analysis, the security requirements for the application were enhanced during the development stage and prior to system roll-out.

4.6.1 Risk Category

Confidentiality

4.6.2 Risk Impact/Probability

High/Medium

4.6.3 Potential Safeguard(s)

1. Programmatic changes to the application to isolate display of sensitive data
2. Re-architect the underlying database to use Microsoft SQL-Sever 2005 instead of Microsoft Access, providing enterprise security and reliability
3. Implement secure database connectivity between Claim Center client workstations and the Lottery HQ database server

4.6.3.1 Database Re-Architecture

The back-end database has been switched to SQL-Server and the application redesign to incorporate enterprise security features for sensitive data.

4.6.3.2 Secure Network Connectivity

This potential safeguard needs to be verified and additional investigation conducted before system go-live sign-off. Prior to deployment of the claims processing application, DCLB IT will verify and validate the secure data transmission. In July 2009, unit testing and customer acceptance testing with non-sensitive data will be conducted.

4.7 Power Interruption – Risk Identified: Episodic Power Failures

Continued Uninterrupted Power Supply (UPS) problems forced this risk to the front burner. Through observation we determined that power fluctuations, related to LTE's diesel generator replacement and subsequent weekly testing, have caused episodic power failures on Sunday nights. When encountered, these events caused total system failure of all DCLB datacenter components, requiring **immediate risk mitigation**.

4.7.1 Risk Category

Integrity, Availability

4.7.2 Risk Impact/Probability

High/High

4.7.3 Potential Safeguard(s)

1. UPS Preventive Maintenance
2. UPS and UPS/Environmental Monitoring SOP
3. Replace UPS

4.7.3.1 UPS Preventive Maintenance

The UPS was substantial repaired and upgraded. New batteries, voltage regulators and circuit connectors were installed. Proactive monitoring of diagnostics and preventive maintenance reports was implemented. In addition, IT staff have been on stand-by during the Sunday generator test to observe UPS performance and prevent systems failure.

4.7.3.2 UPS and Environmental Monitoring

Procedures and environmental alerts have been implemented to proactively monitor the condition of the UPS room environment.

4.7.3.3 Replace UPS

The IT department conducted a needs analysis of the UPS and determined that replacement would be a preferred option. However, due to the substantial investment made in repairing and upgrading the current UPS, and to the competing priorities for network cabling upgrade investments, the IT Director made the strategic decision to pursue alternative solutions. (See 4.7.3.4)

4.7.3.4 Perform Comprehensive Electrical Circuitry Analysis

The IT department is preparing an acquisition plan for procurement of electrician services – this activity has been delayed while negotiations between the DC Office of Property Management and the Curtis Properties company continue. After the DC Office of Property Management makes a definitive determination of the extent of leaseholder improvements, the IT department can move forward with the comprehensive analysis.

APPENDIX 1

Appendix 1: Agency's Response - Two (2) pages

GOVERNMENT OF THE DISTRICT OF COLUMBIA
DC LOTTERY & CHARITABLE GAMES CONTROL BOARD

★ ★ ★

TO: Mohamad Yusuff, Interim Executive Director
Office of Integrity and Oversight (OIO)
Office of the Chief Financial Officer

FROM: Jeffrey A. Young
Executive Director

DATE: October 15, 2009

SUBJECT: Draft Report on the Facilitation of the Information Technology (IT) Department's Information Security/Internal Controls "Self Assessment" Process at the D.C. Lottery and Charitable Games Control Board (DCLB) (Report No. IA:DCLB:2804-C11)

Introduction

This memo is in response to OIO's Draft Report dated September 25, 2009 on the Facilitation of the Information Technology (IT) Department's Information Security/Internal Controls "Self Assessment" Process at the D.C. Lottery and Charitable Games Control Board (DCLB).

OIO Findings and Recommendations:

1. *Minutes of the Brainstorming Sessions were Unavailable and Caused Inefficiencies to the Overall "Self Assessment" Process.*

- Recommended Action: We recommend that the minutes be done and approved by the group at the next session of the 2009 DCLB IT "Self Assessment" process.

DCLB Response:

DCLB agrees. The IT Department has developed Standard Operating Procedures describing in detail the process for IT "Self Assessment". The SOP mandates that

meeting notes be completed within 3 business days and distributed prior to the next meeting for review and approval by the team participants.

OIO Findings and Recommendations

2. *The DCLB IT Risk Analysis Draft Report was not done until April 2009 and thus Loses Much of its Information Value.*

- Recommended Action: To preserve the information value of the "Self Assessment" process, we recommend that the report be produced soon after the brainstorming sessions are completed.

DCLB Response:

DCLB agrees. The IT Department has developed Standard Operating Procedures describing in detail the process for IT "Self Assessment". The SOP mandates that the Draft Report be completed within 30 days of the fourth Risk Assessment meeting, thus ensuring that the report is complete within 90 days of the IT Risk Self-Assessment Project start.

OIO Findings and Recommendations

3. *Lack of Referencing (or Cross-Walk) to NIST SP 800-53 Risk Assessment Procedures in the DCLB IT Risk Analysis Report*

- Recommended Action: We recommend that the 2009 Risk Analysis "Self Assessment" report cross-walk an updated IT Security Ranked Risks to the main results of the report and the IT Security Plan when it is completed

DCLB Response:

DCLB agrees. The IT Department has developed Standard Operating Procedures describing in detail the process for IT "Self Assessment". The SOP mandates that the Draft Report contain a traceability matrix which cross-walks the updated IT Security Ranked Risks to the IT Security Plan.