



AUDIT DEPARTMENT

Audit Report

Business License
Information Technology
Infrastructure
Follow Up Audit

May 2012

Angela M. Darragh, CPA, CISA, CFE
Audit Director

AUDIT COMMITTEE:

Commissioner Steve Sisolak

Commissioner Chris Giunchigliani

Commissioner Lawrence Weekly



Audit Department

500 S Grand Central Pkwy Ste 5006 • PO Box 551120 • Las Vegas NV 89155-1120
(702) 455-3269 • Fax (702) 455-3893

Angela M. Darragh, CPA, CFE, CISA, Director



May 15, 2012

Mr. Don Burnette
Clark County Manager
500 South Grand Central Parkway, 6th Floor
Las Vegas, Nevada 89106

Dear Mr. Burnette:

Pursuant to Audit Department policy, we performed a follow-up audit of the Business License Information Technology Infrastructure audit dated February 27, 2010. The audit objective is to determine whether adequate corrective action has been taken on the findings addressed in the audit report. Our audit procedures were performed as of March 21, 2012. Our procedures included performing a preliminary survey, analyses, and test of transactions on a sample basis. Our audit was conducted in accordance with generally accepted government auditing standards.

It is the department/division management's responsibility to decide if any appropriate action should be taken in response to reported audit findings. It is also their responsibility to assume the risk by not correcting a reported condition because of cost or other consideration.

Business License, with coordinated efforts of the Information Technology Department, has taken adequate corrective action for all three findings reported in the original audit.

A draft report was provided to Business License. We appreciate the cooperation and assistance provided by Business License and Information Technology Departments during the course of this audit.

Sincerely,

/s/ Angela M. Darragh

Angel M. Darragh, CPA
Audit Director

TABLE OF CONTENTS

BACKGROUND.....	1
OBJECTIVES, SCOPE, AND METHODOLOGY.....	1
RESULTS OF FOLLOW UP AUDIT	2
Implementation Rate.....	2
DETAILED RESULTS OF PRIOR AUDIT FINDINGS	2
Software	2
Server Security Settings	3
Disaster Recovery	4

BACKGROUND Business License Department primary functions are to issue business, liquor and gaming, and regulated licenses; issue film permits; perform inspections; and facilitate negotiations, maintain agreements, and monitor compliance of franchise and other rights-of-way license agreements.

Business License information technology infrastructure is comparatively small to other county departments. It consists of 190 personal computers, four departmental servers, and three shared servers. These servers are housed in the County's Computer Operations Center and are considered to be physically secure. Most of the network systems administration functions are performed by the County Information Technology (IT) Department personnel. The department does have their own programming and technical support staff that has control over some administrative functions.

Original Audit - Clark County Audit Department Information Technology Division performed an audit of *Business License Information Technology Infrastructure*, dated February 17, 2010, for the period February 27, 2009, through March 27, 2009. The objective of the audit is as follows:

- *To determine if the controls implemented for the Business License Department Information Technology infrastructure assured that changes were both authorized and maintained in an accurate, timely manner and that access to all business related activities were properly controlled.*

The results of the original audit identified three areas that needed corrective action. The results in brief indicated the following concerns: server level security setting were not consistent; compliance with Administrative Directive 8 is not assured; non-business related software was installed on some departmental computers; and disaster recovery processes and procedures do not exist at the department level.

OBJECTIVES, SCOPE, AND METHODOLOGY The objective of the audit is determine whether corrective action has been taken on the three findings addressed in the *Business License Information Technology Infrastructure* audit report dated February 17, 2010.

Our procedures consisted of reviewing the original audit report and supporting documents, interviews with management and staff, observations, walkthroughs, examination of documentation, and performance of detailed tests and analyses. Excerpts from the original audit and management response were included in this report. The last day of fieldwork was March 21, 2012.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

**RESULTS OF FOLLOW UP
AUDIT**

Business License, with coordinated efforts of the IT Department, has taken adequate corrective action on all findings reported in the original audit. Security and software scanning reports are provided by the County's IT Department. There were no identified risks or non-standard programs reported in February 2012. IT also implemented security scanning software for maintenance of PCI compliance on pertinent servers and random scanning with global application of security issue corrections to all servers. Business License has also complied with submittal of the first phase Disaster Recovery document.

Implementation Rate

Status of Findings	Number of Findings	% of Total
Implemented	3	100%
Not Implemented	0	0
Other	0	0
Total	3	100%

**DETAILED RESULTS OF
PRIOR AUDIT FINDINGS**

Software

Prior Finding Reports that list non-standard software downloaded into an employee's computer contained every program installed and made it difficult to recognize inappropriate software products and compliance with Administrative Guideline Number 8. The size of the reports and lack of guidance made the reports unworkable. The lack of reports for at least 18 months went unnoticed. A report with only non-supported programs will now be provided by the County's IT management team.

Prior Recommendation	On a monthly basis, Management should review this [new] report and take any necessary corrective actions in order to comply with Administrative Guideline 8.
Management's Response to Prior Finding	<p>Machine Scans – Scan each machine using Microsoft Baseline Security Analyzer to ensure proper security settings. The department completed the initial machine scans as of February 1, 2010.</p> <p>IT Report – Lists all installed software on department computers as non-compliant. Upon completion of the machine scans and receipt of the monthly IT Software Report, the department will be able to establish a quality control mechanism, that going forward, will endure the department's compliance with Administrative Guideline Number 8.</p>
<i>Corrective Action Taken</i>	Business License receives reports from the County's IT Department identifying non-standard software installed on personal computers. The February 2012 report showed all personal computers did not have non-standard software installed.
<i>Corrective Action Status</i>	Implemented

Server Security Settings

Prior Finding	Risk of exposure to unauthorized access or modification in Shares, Guest Accounts, AutoRun, and Passwords were identified in some of the servers.
Prior Recommendation	Management should conduct a review of the Business License servers and ensure that corrective action is taken to correct both high risk and medium risk exposures identified by the security scanning software.
Management's Response to Prior Finding	The department will address these server issues in conjunction with the recommended individual at the IT Operations Center for appropriate corrective action. Future collaboration with the Operations Center concerning server security will ensure on-going compliance.
<i>Corrective Action Taken</i>	IT also implemented security scanning software for PCI compliance on required servers. IT scans County servers and globally corrects all servers for security issues identified on these scans. Network, workstation and server security is an ongoing effort with newly discovered security vulnerabilities continually providing challenges to the environment. To address this, IT has implemented processes of continual improvement to maintain a high level of protection and quick remediation of security issues.

Corrective Action Status Implemented

Disaster Recovery

Prior Finding Business License was involved in the IT Department's "COOP" project that was intended to address departmental disaster recovery efforts at a County-wide level. However, that project was cancelled, leaving Business License Department not properly prepared to address business continuity risks. A County-wide disaster recovery plan, sponsored by IT, is in its development phase.

Prior Recommendation The Business License Department management team should develop a written disaster recovery plan for their systems that can be absorbed by the IT Department once the Countywide disaster recovery plan is written.

**Management's Response to
Prior Finding** The department will forward any information that was developed from a previous disaster level recovery effort in conjunction with the COOP Initiative sponsored by Clark County IT in 2007. Business License is willing and eager to partner and cooperate with IT to achieve a disaster recovery plan that is of sufficient quality to sustain the critical mission and work of the department during a crisis.

Corrective Action Taken The Countywide COOP program is in the first phase. The purpose of the first phase is to identify essential services and document these in Business Impact Analysis (BIA) reports. Business License submitted the BIA reports that have been updated as of 2012. Currently, the COOP program has not progressed on a countywide level past the first phase due to the economic downturn.

Corrective Action Status Implemented

BUSINESS LICENSE IT INFRASTRUCTURE FOLLOW-UP AUDIT



AUDIT DEPARTMENT

Angela M. Darragh, CPA, CFE, CISA

Audit Director

**Findings, Recommendations, and Corrective Actions Status
As of March 21, 2012**

Original Report Issuance Date: February 27, 2010

Summary Audit Findings & Recommendations			Summary Management Response		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Actions Status	Implemented	Not Implemented	Other
1 Software							
	Reports that list non-standard software downloaded into an employee's computer contained every program installed and made it difficult to recognize inappropriate software products and compliance with Administrative Guideline Number 8. The size of the reports and lack of guidance made the reports unworkable. The lack of reports for at least 18 months went unnoticed. A report with only non-supported programs will now be provided by the County's IT management team.	On a monthly basis, Management should review this [new] report and take any necessary corrective actions in order to comply with Administrative Guideline 8.	Y	Business License receives reports from the County's IT Department identifying non-standard software installed on personal computers. The February 2012 report showed all personal computers did not have non-standard software installed.	✓		
2 Server Security Settings							
	Risk of exposure to unauthorized access or modification in Shares, Guest Accounts, AutoRun, and Passwords were identified in some of the servers.	Management should conduct a review of the Business License servers and ensure that corrective action is taken to correct both high risk and medium risk exposures identified by the security scanning software.	Y	IT also implemented security scanning software for PCI compliance on required servers. IT also randomly scans County servers and globally corrects all servers for security issues identified on the random scans. Security of servers is an ongoing process with security vulnerabilities continually providing challenges to maintain a secure environment. IT implemented these processes to continually address ongoing security vulnerability challenges with the understanding that at any one time these may exist.	✓		

Summary Audit Findings & Recommendations			Summary Management Response		Summary Status		
Ref	Finding	Recommendation(s)	Concurrence	Corrective Actions Status	Implemented	Not Implemented	Other
3	Disaster Recovery						
	Business License was involved in the IT Department's "COOP" project that was intended to address departmental disaster recovery efforts at a County-wide level. However, that project was cancelled, leaving Business License Department not properly prepared to address business continuity risks. A County-wide disaster recovery plan, sponsored by IT, is in its development phase.	The Business License Department management team should develop a written disaster recovery plan for their systems that can be absorbed by the IT department once the Countywide disaster recovery plan is written.	Y	The Countywide COOP program is in the first phase. The purpose of the first phase is to identify essential services and document these in Business Impact Analysis (BIA) reports. Business License submitted the BIA reports that have been updated as of 2012. Currently, the COOP program has not progressed on a countywide level past the first phase due to the economic downturn.	✓		