STATE OF VERMONT

Auditors’ Report on Internal Control Over Financial Reporting and on Compliance
and Other Matters Based on an Audit of Financial Statements Performed
in Accordance with *Government Auditing* Standards

Year ended June 30, 2012

KPMG LLP
Suite 400
356 Mountain View Drive
Colchester, VT 05446

Independent Auditors' Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance With *Government Auditing Standards*

Speaker of the House of the Representatives
President Pro-Tempore of the Senate
Governor of the State of Vermont
General Assembly, State of Vermont
State House
Montpelier, Vermont:

We have audited the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the State of Vermont (the State), as of and for the year ended June 30, 2012, which collectively comprise the State's basic financial statements, and have issued our report thereon dated December 27, 2012. Our report was modified to include a reference to other auditors. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Other auditors audited the financial statements and related disclosures of certain discretely presented component units identified in note 1A of the State's basic financial statements, the Vermont Lottery Commission, the Special Environmental Revolving Fund, the Vermont Energy Efficiency Utility Fund, the Vermont Universal Service Fund, the Vermont Information Technology Leaders, Inc. and the Tri-State Lotto Commission as described in our report on the State's financial statements. This report does not include the results of the other auditors' testing of internal control over financial reporting or compliance and other matters that are reported on separately by those auditors.

For purposes of this report, our consideration of internal control over financial reporting and our tests of compliance with certain provisions of laws, regulations, contracts and grant agreements, and other matters did not include the University of Vermont, or the Vermont Economic Development Authority which are discretely presented component units. We have issued separate reports on our consideration of internal control over financial reporting and on tests of compliance with certain provisions of laws, regulations, contracts and grant agreements, and other matters for these entities. The findings, if any, included in those reports are not included herein.

Internal Control over Financial Reporting

Management of the State is responsible for establishing and maintaining effective internal control over financial reporting. In planning and performing our audit, we considered the State's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the State's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses and therefore, there can be no assurance that all deficiencies, significant deficiencies, or material weaknesses have been identified. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider to be material weaknesses and other deficiencies that we consider to be significant deficiencies.

A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. We consider the deficiencies in the State's internal control over financial reporting described in the accompanying schedule of findings and questioned costs as findings FS2012-01 and FS2012-02 to be material weaknesses.

A significant deficiency is a deficiency, or combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiency described in the accompanying schedule of findings and questioned costs as finding FS2012-03 to be a significant deficiency in internal control over financial reporting.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the State's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

We noted certain matters that we reported to management of the State in a separate letter dated December 27, 2012.

The State's responses to the findings identified in our audit are described in the accompanying schedule of findings and questioned costs. We did not audit the State's responses and, accordingly, we express no opinion on them.

This report is intended solely for the information and use of the Speaker of the House of Representatives, the President Pro-Tempore of the Senate, the Governor, the General Assembly, management, the cognizant federal agency, the Office of the Inspector General, and federal awarding agencies and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

December 27, 2012

Vt. Reg. No. 92-0000241

Findings Relating to the Financial Statements Reported in Accordance with *Government Auditing Standards*

Over the past several years, the State has improved its financial accounting and reporting capabilities. As the State moves forward, however, maintaining focus on accountability, transparency and accuracy will continue to be difficult as state financial resources become scarce and key personnel retire. The State needs to be diligent about optimizing its current revenue streams, controlling costs, avoiding the temptation to use one-time revenues and ensuring key personnel close to retirement are identified and leveraged properly to ensure a smooth transition to the successor. The comments we identified as a result of the 2012 audit are presented below:

FS2012-01 – Review and Analysis of Financial Data

Background

The State's accounting process is very decentralized and relies heavily on the individual departments and agencies to properly and accurately record activity on a timely basis in the State's VISION accounting system as well as to provide year-end closing information to the Department of Finance and Management (Finance) in the form of the year end closing packages. Finance provides the individual departments and agencies with annual guidance on generally accepted accounting principles and the form and content of the information that is required in the year end closing packages; but relies on the individual departments and agencies to completely and accurately compile the data.

Finding

Finance has been working with individual departments and agencies for several years to improve the financial reporting process and reduce the number of data errors and adjustments. Although improvements have been made in this area, adjustments to the financial statements continue to be identified through the external audit. The cause of these adjustments is in part due to personnel changes in the individual departments and agencies, a lack of financial reporting knowledge in the individual departments and agencies, and departments and agencies not having adequate control procedures over the recording of financial data. The adjustments identified during the fiscal 2012 audit are as follows:

a. Federal Revenue Fund:

   - $36 million reclassification to reduce deferred revenue and increase federal grant revenue as a result of the Department of Finance and Management not recording federal revenue in accordance with the proper accounting basis.

     Governmental fund financial statements are reported using the current financial resources measurement focus and the modified accrual basis of accounting. Revenues are recognized as soon as they are both measurable and available. Revenues are considered to be available when they are collectible within the current period or soon enough thereafter to pay liabilities of the current period. For this purpose, the State generally considers revenues to be available if they are collected within 60 days of year-end. However, federal receivables are treated differently within the governmental funds as federal receivables are amounts due from the federal government to reimburse the State's expenditures incurred pursuant to federally funded programs. Therefore, federal grant revenues are generally accrued for when the qualifying expenditure is incurred.

We noted that the Department of Finance and Management was not accruing federal revenue when the qualifying expenditure was incurred, but rather if the federal funds were received within July and August, which is inconsistent with the State's accounting policy as stated in the footnotes to the financial statements.

- Increase receivables by $2.9 million and revenue by $5.9 million and corresponding decrease of $3 million to payables. While we were reviewing the reconciling draw for the Global Commitment waiver it was determined that the Department of Finance and Management was using a draft report from the Agency of Human Services and not the final year end data which resulted in the above entry.

b. Transportation Fund: $5.9 million reclassification to reduce deferred revenue and increase federal grant revenue as a result of the Department of Finance and Management not recording federal revenue in accordance with the proper accounting basis. See Federal Revenue Fund item a above for additional details.

c. Special Fund: Decrease cash and revenue by $15,000, due to a correcting entry being recorded without reversing the original entry. The Catamount Heath Fund receipts are managed by the Department of Labor (DOL), who didn't notice that after the correcting entry was made the original entry was not reversed. The Office of the State Treasurer performs cash account reconciliations and we noted that this $15,000 was listed as a reconciling item and was not corrected during their reconciliation process.

d. Unemployment Compensation Trust Fund: Increase receivables and revenue by $481,243, due to data inadvertently being excluded from a spreadsheet calculation. This adjustment was the result of a new Program Integrity Chief within Unemployment performing the allowance for uncollectible taxes calculation at the Department of Labor and the lack of review over this calculation.

e. Workers Compensation (Internal Service) Fund: Decrease claims expense and claims payable by $223,518 as a result of incorrectly calculating the Incurred But Not Reported (IBNR) amount. This adjustment is the result of the Office of Workers' Compensation and Prevention within the Department of Buildings and General Services (BGS) not calculating the IBNR liability correctly and the lack of review over this calculation.

While Finance is primarily responsible for the preparation of the State's financial statements, responsibility for the underlying data and activity resides in the departments and agencies. These adjustments indicate the continued need for further training for business officers throughout the State on topics including financial accounting and reporting as well as internal controls and data analysis concepts.

Recommendation

Finance should continue to provide training to and work with State departments and agencies to provide them with the knowledge and guidance relating to financial accounting and reporting concepts, including internal controls, to help ensure that the State's financial statements are complete and accurate. Finance should also evaluate its procedures for spot-checking year end closing packages and for analyzing data for completeness.

Management's Response

The Department of Finance and Management has made significant progress in working with the individual departments and agencies on properly recording activity during the year and providing accurate information for closing at year-end, but we recognize we can continue to make improvements in this area. We plan to make the following changes to our procedures:

- Finance will review our year-end closing package to make sure that we are clear about the information that we are requesting and to provide more guidance on the accounting and reporting concepts that are applied to the various items we are asking departments and agencies to report.
- Finance will review the significant adjustments that were made during the last audit and review those changes with the responsible department to determine how they plan to improve their procedures to ensure similar adjustments are not required in the future.
- Finance will review the status of responsible personnel in each of the departments and agencies to determine which personnel might need additional assistance or training due to staff changes, and reach out to those personnel to ensure they better understand the needs of our department.
- Finance will be more proactive during our processes by performing more reviews of the information that has been submitted to our department; paying particular attention to areas of concern in the prior year audit or accounting and to reporting concepts that are new to a particular department or agency; and requesting supporting information and calculations for more significant items.

FS2012-02 – Liquor Control Fund - Inventory

Background

The Liquor Control Fund (the Fund) is a major enterprise fund reported in the State's financial statements. The financial activity for this fund is managed by the Department of Liquor Control (the DLC).

The DLC stocks inventory in a central warehouse in Montpelier, Vermont and throughout the State in the Agency retail locations. The majority of the inventory in the Montpelier warehouse is not State-owned, but rather held in bailment. The inventory shown on the financial statements consists of a small portion residing at the warehouse that is owned by the State, while the majority of the inventory is located across the state at the various Agency locations. At June 30, 2012, the State owned $5.2 million of liquor inventory.

Finding

We noted that the DLC does not appear to have sufficient internal knowledge relating to inventory accounting or any documented policies and/or procedures for the handling of its inventory, including annual physical inventory counts and year end cut off. Throughout the course of the audit, we received incomplete and contradictory information from various personnel at the DLC in response to our questions and requests for information. Specifically, the following matters related to inventory were noted:

a. The DLC does not maintain formal agreements with their vendors outlining the terms of ownership, but indicated that the terms are specified on quote sheets. These sheets contain boxes including State stock, bailment or special purchase, and the vendor checks the corresponding box to indicate the ownership.

   - During our testwork we observed the ownership designations on the quote sheets were not consistent with the ownership designations reported from DLC's accounting system. Specifically, of the 50 items selected in our counts, 21 (or 42%) had conflicting ownership designations.
   - The DLC does not appear to have any documentation beyond the price quotes to outline the terms of the custody of the bailment inventory. Any financial penalty due to losses from natural causes is ambiguous within the terms of the existing support.
   - We further noted that the effective date on several of the quote sheets appeared to be very old, some dating back to 2008 and before.

b. During our inventory count of the warehouse on June 21, 2012, we noted differences between the inventory system report and the actual inventory counted. The differences primarily related to inventory that was loaded onto delivery trucks. We noted that the DLC leaves unattended inventory in these delivery vehicles overnight for deliveries to various agencies the following day. Due to the lack of formal vendor agreements outlining the bailment terms and when ownership transfers to the State, it is unclear if the inventory residing in the delivery trucks should be considered State-owned or vendor-owned. This also proposes a potential cut-off issue at year end, due to the fact that if this is considered to be State-owned inventory, there is a manual process for confirming the inventory within the DLC's inventory system (RIMS) to add it as State inventory and if not confirmed in the system on the day it is loaded on the truck, the inventory will be understated. During our warehouse inventory count, the inventory loaded onto the delivery trucks was not properly confirmed within the DLC's inventory system, which caused the majority of the differences noted between the DLC accounting system and the actual counts taken.

To ensure that year-end inventory was properly stated, KPMG requested that the DLC review its cut off procedures and verify that inventory loaded on the trucks was confirmed in the system and included in the June 30, 2012 balance. During this process KPMG received conflicting information from agency personnel on whether the inventory loaded on the delivery trucks, valued at $163,819 had been included in the year-end balance. KPMG notes that the DLC was not able to determine if the inventory on the trucks had been recorded in fiscal year 2012 and was not able to provide supporting documentation for the inventory.

c. We obtained a rollforward of the inventory balance from the prior year end to June 30, 2012. Included in this rollforward were adjustments valued at $275,365. The DLC management provided the following explanations for these adjustments:

- $176,000 from losses due to fire, flood and theft. We noted the DLC submitted a claim for the loss of inventory but has not booked a receivable for the amount of the claim.
- $26,000 in warehouse breakage. The DLC was unable to provide sufficient documentation to support the amount of breakage. Based on the average cost of a bottle of liquor, this represents approximately 1,000 broken bottles over the 12-month period.
- $71,000 in warehouse over and shorts. Per discussion with DLC personnel, they indicated that it was a common occurrence for there to be disagreements between what is shipped per vendor records and what was received per the Department, including disagreements on entire pallets of inventory. DLC was unable to provide sufficient documentation on how these disputes were handled and whether the State paid for inventory they did not receive.
- $18,000 variance from adjustments in the inventory system to adjustments in VISION. The DLC was unable to provide sufficient documentation to support the difference from VISION to RIMS.

d. We noted there were many variances between the inventory system and VISION, the State's accounting system. During our review of the reconciliation of differences prepared by the Department of Liquor Control, we noted there were multiple accounts for over and short adjustments as well as other adjustment accounts. Per discussion with management these accounts refer to over and shorts and breakage at Agency locations. We noted that there is insufficient supporting documentation to determine what is considered breakage, which the State assumes as the cost of doing business, and over and short items that must be reimbursed by the Agency. In addition there appears to be a lack of differentiation in the accounting system for the unsellable inventory resulting from breakage versus from over and shorts.

Recommendation

We recommend that the Department of Liquor Control review its internal control procedures over inventory including the safeguarding of those assets. We also recommend that the DLC update its policies and procedures documentation for the handling of its inventory, including annual physical inventory counts and year end cut off. Finally we recommend that the State set up formal vendor agreements, update the terms and conditions, and specifically define the 'bailment', which will help ensure that the transfer of ownership is clearly defined.

Management Response

a. DLC is currently in the process of generating agreements that will specify ownership with its vendors. DLC plans to have these agreements in place by the end of FY2013.

   - DLC uses quote sheets to obtain quote information on products and for no other reason. Ownership designations listed on the quote sheet are irrelevant. DLC is unsure what this finding is specifically addressing since quote sheets are not used for ownership designation.
   - DLC is currently in the process of generating agreements that will specify ownership with its vendors. DLC plans to have these agreements in place by the end of FY2013.
   - There is current availability in the warehouse to house six trucks. The trucks are not locked; however, they are housed in a locked building armed with a security system. It is extremely rare that DLC will have more than six trucks loaded, but if needed, trucks can also be loaded and stored outside the warehouse. If this happens, the trailer is padlocked.

b. Inventory is confirmed on the day of shipment, which indicates ownership of the inventory in DLC's current process. Per KPMG's request, an adjustment was made to include the inventory held on the truck in DLC's financials.

c. DLC has resolved this issue in FY2013.

   - A receivable was not booked due to the recovery not deemed realizable.
   - Supporting documentation was provided on December 21, 2012.
   - DLC has since resolved this issue and is documenting the process that relates to "overs and shorts" in the warehouse.
   - DLC has resolved this issue in FY2013

d. DLC provided breakage reports for one agency and the warehouse on December 21, 2012. These were examples of what could be generated to provide support for breakage. No further requests were made for reports. On December 20, 2012, DLC also provided an explanation of how Agencies are held responsible for their over and shorts.

FS2012-03 –Information Technology Controls

Background

The State relies heavily on its information technology (IT) systems to process, account for and report on its financial activities. The State's VISION system services as the State's principal financial system and is used to prepare the State's financial statements. Although the VISION system is the State's principal financial system, many of the actual financial activities are originated in other departmental managed systems. During the previous two fiscal year audits IT general controls (ITGC) reviews were performed over certain critical IT systems. The purpose of a review of IT controls is to gain an understanding of the controls that are in place and to the test the design and operating effectiveness of those controls. During the ITGC review the following control objectives were reviewed: access to programs and data; program changes; program development; and computer operations. These ITGC reviews indicated numerous control deficiencies of varying severity.

As part of the fiscal year 2012 audit the prior year findings were followed up on to ascertain if the identified control deficiencies had been corrected. The following computer systems were part of this follow up:

	Findings and Recommendations
1.	**Application Name**: State Network & Data Center **Responsible Agency**: Department of Innovation and Information (DII) **Purpose**: State-wide local area network.
	a. The initial control deficiency related to the fact that the complexity for password parameters was disabled. Weak password constructs increase the risk that computer application access will be compromised leading to a misuse or misappropriation of confidential and sensitive information. As of fiscal year 2012 they increased the minimum length to 8 alpha-numeric characters for all clients except the Agency of Human Services' ACCESS system. Currently the minimum password length is set to 8 alpha-numeric characters for all clients except for AHS ACCESS. We recommend that DII continue to work towards enabling the complexity for the RACF password parameters. b. The Agency/Department notifies DII when user access is to be removed. DII has written procedures requiring the DII RACF Administrator to acquire and review the HR termination list to determine if any access has inappropriately been retained. DII reviews a lock-out report for anomalies, such as hacking attempts, but does not distribute it to departmental RACF Administrators because it is not user friendly. A program has been written to address this problem, but it has not yet been implemented. Absence or lack of prompt communication to responsible IT staff regarding employee terminations could result in the continuance of unauthorized gateways into key systems or application and may lead to the compromise of

Findings and Recommendations

key systems, application and data assets by unauthorized persons.

We recommend that DII establish a review process, and determine a process to begin the lock out report process.

c. The initial control deficiency related to the fact that backup restoration testing is periodically performed; however, no formal backup or restoration policy existed. Without appropriate and periodic restoration tests, assurance cannot be placed on the reliability of backup media to recover key systems, applications and data assets in the event of an emergency. As of fiscal year 2012 a disaster recovery plan was in draft form, but had not been finalized, and no disaster recovery was performed to ensure the recoverability of the data.

We recommend that DII create and implement a policy for backup restoration testing that includes the timing of restoration tests, the scope of the restoration, and the retention of the results of the restoration test.

Management Response

a. RACF Complex Password - Complex Password is planned for implementation after a few critical software upgrades. Target Date: 12/1/2013

b. RACF Report - We are in the process of implementing a new reporting system. Target Date: 04/30/2013

c. We have replaced the IBM Tape Backup System with an IBM Virtual Tape Library. We are updating our Backup/Restore & Disaster Recovery procedures. Target Date: 09/30/2013

2. **Application Name**: VISION Financials

Responsible Agency: Department of Finance and Management

Purpose: State-wide accounting system

a. The initial control deficiency related to a variety of segregation of duties issues, including:

- users have superuser_no_sec, vendor processing, and manager roles that allow them to add a vendor, enter a voucher, and approve a voucher.
- users have superuser_no_sec and manager roles.
- users have been granted the manager role that allows them to enter a voucher and approve a voucher.

In addition, there is no edit in VISION that would preclude a user from entering a voucher and approving this same voucher. This is particularly important since State employees are commonly listed as vendors in VISION in order to receive certain reimbursements. Ineffective segregation of duties may permit inappropriate access that leads to the creation and approval by a single individual of fraudulent transactions that compromise the financial

Findings and Recommendations

integrity of the system.

We recommend that Finance, in conjunction with DII, establish and enforce a segregation of duties policy that restricts developers from having added and change access to data. If this policy allows for limited or emergency access, then such access should be monitored. Finance, in conjunction with DII, should reduce the access of certain staff that can perform each of the roles of adding a vendor, entering a voucher, and approving a voucher. Finance, in conjunction with DII, should expeditiously implement a control in VISION to preclude a user from both entering and approving the same voucher. Finance, in conjunction with DII, should evaluate the current role structure in VISION to ensure that the system enforces segregation of duties.

b. The initial control deficiency related to the fact that a comprehensive change management policy for the VISION environment did not exist. Moreover, the VISION change management process is not fully documented. The lack of a change management policy with appropriate outlines of approval increase the risk that unauthorized and inappropriate software changes could be put into production leading to the compromise of key applications and data assets. As of the end of fiscal year 2012, a policy was in draft form and Finance & Management was working with DII to implement an overarching change management process with DII.

We recommend that Finance, in conjunction with DII, expeditiously document its VISION change management policy and process.

Management Response

DII along with Finance have created a comprehensive Change Management process that will be finalized and fully operational by June, 2013.

The Department of Finance and Management strongly agrees that segregation of duties is a powerful tool against fraudulent transactions. We have made segregation of duties a key element of our accounts payable and internal control guidance, emphasizing the importance of separating key functions within that process. We also have incorporated this concept into our annual self-assessment of internal controls survey. Although the current configuration of PeopleSoft security has the entry and approval process imbedded in the same role, we have always encouraged manual approval and sign off of invoices be someone different than the person that does the data entry. Additionally, within VISION, entering and approving a voucher does not make that voucher available for payment. To have a voucher move from an approved status to a payable status it still needs to be budget check. This is the process that actually commits the funds for payment. We strongly encourage that this final step also be performed by someone other than the person that enters and approves. Additionally, there are several accounts payable management reports that are available to departments and widely used that provide insight to payment being made and to whom. Monitoring through reports is a great way to identify fraudulent payments as well.

Within the next several months we will be embarking on an upgrade of the VISION Financials

Findings and Recommendations

Application from version 8.8 to 9.2. During that upgrade we will review our security roles with an eye toward separating the function of data entry and approval within the same security level. We will also be reviewing the enhanced workflow functionality.

Over the past several months we have also been in the process of implementing a new employee expense reimbursement module. We are expected to go live with this new module during May 2013. This module will allow us to remove all employees from our master vendor file and pay them as employees through our expense module, not the accounts payables module. This will eliminate the opportunity for employees to process checks to themselves or to co-workers through the account payable module

3 **Application Name**: ETM

Responsible Agency: Department of Taxes

Purpose: State Tax System.

a. The State of Vermont's IT Security Policy has not been updated since May 2009. An updated or reviewed IT Security Policy provides the end user with comprehensive and up to date information related to IT policies and procedures in place. Lack of an updated policy could result in outdated information being provided to end users and consequently increase risk to security.

We recommend that the IT Security policies and procedures be reviewed and updated at least on an annual basis to address all relevant systems and applications and to address new security threats.

b. No formal user access review by the business owners of the ETM application is conducted to identify potential separation of duties conflicts. However, on a quarterly basis, Department of Tax reviews the inactive network accounts to determine that access to ETM was appropriately deactivated. The absence of periodic management reviews of the key application user access increases the risk that active staff may retain processing capability that exceeds their job requirements and undermines a prudent separation-of-duties.

We recommend that Department of Taxation management:

- Develop, publish and enforce a policy to require business application owners to limit staff access privileges to those necessary to perform their jobs and to ensure an appropriate separation of duties.
- Review user access privileges on a periodic basis and take steps to identify and remove unnecessary or inappropriate application functionality or privileges.

c. No formal change management policy/procedure exists for the ETM application environment. A generic change management policy for Department of Taxation exists that was last updated on September 13, 2007. The lack of a formal and enforced Change Management Policy that documents steps to be followed, approvals required, testing to be conducted and acceptance

Findings and Recommendations

sign-offs to be required for changes to ETM, increases the risk that unauthorized and/or inappropriate software changes could be intentionally or accidentally be placed into production.

We recommend that an ETM specific Change Management policy and procedure be documented that describes the software change management process from initiation through migration to production and documents the roles and responsibilities of all parties including the business owners for development, testing and migration.

d. While one (1) user has been designated as the primary migrator of software changes, currently ten (10) users have “SYSADM” level access that grants them access to develop and migrate changes to production. Of these 10 users, 2 are vendors from CGI/Oracle. Based on our discussion with the Department of Taxation, we noted that no mitigating or compensating controls exist that could be used to prevent or detect unauthorized changes being made to production. The risk of the introduction of inappropriate software changes is commensurate to the number of persons with the access privileges that support this activity.

We recommend that Department of Taxation IT management review current support access and:

- Limit privileged support access to the minimum needed to support the application in production.
- Enforce an appropriate separation of duties between software development staff and those migrating software into.

We further recommend that periodic reviews of changes moved to production be conducted to discourage and to identify any unauthorized changes.

e. The initial control deficiency related to the fact that no restorations from tape have been conducted for ETM since it went live in August 2010. The lack of periodic restoration of data from backup tapes increases the risk that when needed critical data may not be available to restore business operations. During fiscal year 2012 the Tax Department stopped using tape backups for ETM and the systems are now backed up via Net Bankup to two data domains. A procedure document has been put in place detailing the steps and processes to follow for restoring data files from Net Backup and three restorations were done during FY 2012, however no documentation was provided evidencing that the restorations took place.

We recommend that Taxation Department IT periodically test restoration of data from tape to ensure the integrity and completeness of the data and that the backup process and equipment is working as expected.

f. ETM currently has no formal, documented or tested Disaster Recovery or Business Continuity Plan. The lack of a comprehensive and tested Disaster Recovery Plan (DRP) and complementary Business Continuity Plan (BCP) increases the risk that in the event of a serious environmental event affecting ETM’s operations could be disrupted for an extended period of time.

Findings and Recommendations

We recommend that Department of Taxation business and IT management take appropriate steps to bring the DRP up to date and augment it with an appropriate BCP and provide resources to ensure an appropriate recovery capability. We further recommend that the DRP and its associated BCP be treated as a living document subject to ongoing revision and that it be tested at least annually.

g. No daily operations log/checklist is maintained to capture information on daily production such as job processing, backups taken, abends and issues noted. Depending on the specific job schedule, a text message is sent to the Operations group and Department of Taxation notifying if a job ran successfully or not. If error/issues occurred, support personnel are required to follow up and may be required to raise a support ticket if necessary. A formal daily computer operations log/checklist provides evidence that all appropriate processes were completed and if error or abends occurred they were followed up and resolved in an appropriate manner. An appropriate log can also serve as the basis for conducting root cause analysis when dealing with reoccurring issues.

We recommend that a documented log/checklist of daily computer operations be introduced. The log should be retained to provide evidence that batch jobs and backups processed to completion and also as a means to identify recurring issues.

Management Response

In order to manage the system and promote to production there are different components requiring different ID's that need to be accessed. There is basically one ID for each component used for these purposes and known by a select few for the tasks they need to accomplish. Even fewer know how to migrate anything to production. We have not gotten to the point of setting up individual users ID's with all the combinations of roles needed.

The partition wall between DII and National Life was opened while National Life Technical people were removing equipment from their racks. The finding was to add camera while the duration of partition wall was open.

Action taken:

The partition wall was closed. Cameras were installed looking down the cold and hot aisles where the Tax racks are located.

Pursuant to the SAO / KPMG ETM Review and subsequent Audit Finding, DII will install an additional security camera in the National Life Data Center by February 29, 2012. The new security camera will be positioned in Row 1 where the ETM production server is located in order to monitor activity in the vicinity of the ETM production server as recommended below by KPMG.

a. VDT agrees. Will endeavor to review annually and update as needed and will distribute annually as well.

Findings and Recommendations

b. VDT will establish a process to review user access of ETM on a quarterly basis.

c. VDT will review and update our current change management policy and within it call out any specific differences regarding ETM vs Advantage Revenue.

d. VDT will review access and adjust access to those required to support the application.

VDT will take separation of duties between software development staff and those migrating software under advisement for future implementation however given current resource constraints this separation is not feasible at this time.

VDT agrees that periodic reviews of production changes is a good practice and will look into the feasibility of implementing this recommendation.

e. VDT will strive to implement this recommendation however please note that multiple DB refreshes have been conducted from backups since ETM go live.

f. VDT will review and update the business continuance plan within the next 12 months.

g. VDT will take this under advisement to augment our current operational batch processing logs.

4. **Application Name**: STARS

Responsible Agency: Agency of Transportations

Purpose: Project Cost Accounting System for Transportation Construction Projects

a. The initial control deficiency related to the fact that assets from backup media are only restored when required for Operational reasons and there was no documented Disaster Recovery Plan or activity to restore systems to test recovery procedures. Restoration tests of off-site data backups are performed on a regular basis to determine the usability and integrity of the files. Documentation of the testing results is retained. During fiscal year 2012 AOT performed restorations from the main site using backup tapes successfully; however restores from the backup media at the disaster recovery site have not yet been performed successfully.

We recommend that AOT continue to work towards successfully restoring the backup media at the disaster recovery site.

Management Response

The Agency does have a completed Disaster Recovery Plan that is available in both electronic and hard copy formats. The document is comprehensive and therefore rather large so I have not included it here but we can make it available upon request. With regards to the restoration tests of backup data at the DR facility this is something we have wanted but with DII's change from traditional tape to the VTL that has not occurred. On May 9, 2013, DII will be giving us access to the DR site in Barre. We will be performing a series of tests to determine if we are able to successfully restore our databases from backup media. We will also be testing STARS

	Findings and Recommendations
	functionality, both online and batch. In addition, we will be testing to ensure we are able to promote code through our environments. Given the May 9th testing is successful we should be able to satisfy this finding.
5.	**Application Name**: FARS, VABS and CATS **Responsible Agency**: Department of Labor (DOL) **Purpose:** FARS is the Department's financial accounting system; VABS is the Unemployment Insurance Benefit and Eligibility System; and CATS is the Employer Contribution Tax System.
	FARS: a. Reliance is placed on the policies established by the State of VT DII and no specific policies exist for DOL in regard to the FARS application and support. Lack of established information security function reduces focus on information security and results in inconsistencies with execution of statewide policies and processes. We recommend that the DOL develop a security policy in relation to the FARS application and support which is consistent with DII statewide policy. b. The initial control deficiency related to the fact that access to the computer room required knowledge of the key punch code to open either of the two doors. We observed that the door was left open by the admin desk for people to come and go instead of using the key punch access, as multiple people come into the room to pick up reports during the day and are not IT staff. Additionally, one of the two doors key punch lock was not functioning during our initial visit. Absence of controls over privileged access, powerful utilities and system manager facilities increases the risk of compromise to key IT systems, applications and data assets. As of the 2012 fiscal year end, we observed that the door was shut to access the computer room and clocked by slots that hold reports for employees and the other door requires a key to access. However the door was not open it was unlocked during working hours and a person could climb over the 3 foots cubicle wall. We recommend that the DOL ensure that the door is locked at all times and that key codes are restricted to appropriate personnel. c. Reviews of the access to the computer room are performed by the Manager of IT or their delegate and are completed on a quarterly basis, however this review is not documented. We recommend that DOL IT Management request and review on a quarterly basis a list of people/contractors with access to the computer room. d. No policy exists stating that a periodic review of FARS access should be performed and no periodic review is performed by Business on active users and their privileges. Currently, an ad hoc review is done as new employee or contractor is added or an existing person is changed. The absence of periodic reviews of system or application access by appropriate Business and/or IT management increases the risk that unauthorized individuals may retain

Findings and Recommendations

inappropriate access to key systems, applications and data assets.

We recommend business management and IT management develop and implement a policy requiring a regular access review to the FARS application at a minimum of an annual basis.

e. The initial control deficiency related to the lack of policies for changes to the infrastructure or the operating system as well as an emergency change management policy for the FARS Application, which has not been vendor supported since 1991 and updates are performed by Roger Lowe. The absence of authorization over the change management of application software changes may result in the intentional or unintentional migration of invalid application changes into production that lead to the compromise of key systems, applications and data assets. As of 2012 fiscal year end, the Change Management Policy is in draft form and is applicable for Emergency Changes as well as covering infrastructure and operating system changes. This policy is pending updated data and additional input from the Configuration and Change Management Board.

We recommend that the DOL develop, introduce and monitor a comprehensive change management policy that include emergency changes and that is consistent with the statewide DII policy.

f. Changes to the system are not consistently made until after an appropriate level of testing is performed and approved, which is not always in writing. An absence of formal testing and appropriate sign-off by both information systems and user personnel increases the risk that unauthorized or untested changes may be migrated into production.

We recommend that the DOL develop, introduce and monitor a comprehensive change management policy that is consistent with the statewide DII policy.

g. No segregation of duties exists for the FARS application as Roger Lowe and Joe Lucia have access to development and production. A lack of control over who has the ability to migrate software changes into production increases the risk that inappropriate and unauthorized changes could be made to software, moved undetected into production.

We recommend that the DOL implement a process to segregate the migration of changes to production that would alternate between Roger Lowe and Joe Lucia. This would accomplish the segregation without adding another resource.

h. Restoration of backup data is performed on an as needed basis; however, no regular tests or policy exists. Without appropriate and periodic restoration tests, assurance cannot be placed on the reliability of backup media to recover key systems, application and data assets in the event of an emergency.

We recommend that the DOL develop and document the process to test on a regular basis restoral of data from tapes. The regularity of the test should be documented and maintained for the State’s retention period.

VABS and CATS:

i. DOL applications (VABS and CATS) had weak password syntax with a minimum of 3 and

Findings and Recommendations

maximum of 6 character required. Weak password parameters create weaknesses that can be exploited to gain unauthorized access leading to the compromise of key systems, applications and data assets.

The current VSE/ESA system limits passwords from 3 to 6 characters in length.

We recommend that the DOL IT upgrade to a newer version of IBM o/s that supports longer passwords.

j. The initial control deficiency related to the fact that reviews of Access Lists indicated that there was no regular, periodic review of DOL user access rights to the IBM systems supporting VABS and CATS. The absence of periodic reviews of system or application access by appropriate Business and/or IT management increases the risk that unauthorized individuals may retain inappropriate access to key systems, applications and data assets. As of the 2012 fiscal year end, the DOL rescinds user access as their status changes daily through the Helpstar tracking system and reviews are performed quarterly. However, we were unable to obtain evidence to substantiate that quarterly reviews are performed for VABS/CATS.

We recommend the DOL IBM Support Group (with input from DOL HR) conduct a quarterly review of VDOL staff with access to VDOL’s IBM mainframe and deactivate inactive users pending further review with HR and should remove access from accounts for terminated employees and maintain documentation of this review.

k. The initial control deficiency related to the fact that there was no periodic review of the DOL user access rights to the DOL network. The absence of periodic reviews of system or application access by appropriate Business and/or IT management increases the risk that unauthorized individuals may retain inappropriate access to key systems, applications and data assets. As of the 2012 fiscal year end, the DOL rescinds user access as their status changes daily through the Helpstar tracking system and reviews are performed quarterly. However, we were unable to obtain evidence to substantiate that quarterly reviews are performed for VABS/CATS.

We recommend the DOL Network group (with input from HR) conduct a quarterly review of DOL staff with access to DOL’s network assets and deactivate inactive users pending further review and should remove access from accounts for terminated employees and maintain documentation of this review.

l. The initial control deficiency related to the fact that there is no periodic review by business management of functional VDOL user access to the VABS & CATS applications. The lack of a periodic review of functional access to applications by Business Management may result in the continued and inappropriate access to application functionality by individuals and increases the risk that inappropriate transactions can be processed. As of the 2012 fiscal year end, the DOL rescinds user access as their status changes daily through the Helpstar tracking system and reviews are performed quarterly. However, we were unable to obtain evidence to substantiate that quarterly reviews are performed for VABS/CATS.

We recommend the DOL IT develop and generate every quarter a detailed report by User-ID

Findings and Recommendations

that lists Functional capability within both the VABS & CATS applications. We further recommend that the DOL UI Business Management review the report every quarter to ensure that user access is current and appropriate and the DOL IT take immediate steps to remove application access no longer authorized by UI Management. Documentation of the review by UI Business Management should be maintained.

m. The initial control deficiency related to the fact that requests for VABS and/or CATS changes are informal and IT staff receive verbal requests and e-mails detailing small changes; however more complex requests may be discussed at staff meetings. The absence of authorization over the change management of application software changes may result in the intentional or unintentional migration of invalid application changes into production that lead to the compromise of key systems, applications and data assets. As of 2012 fiscal year end, the process for program changes has been documented within the Change Management Policy. However this policy is in draft form and is pending updated data and additional input from the Configuration and Change Management Board.

We recommend that the DOL introduce a formal Change Request document that requires information on the change required and Management approval before work can be started.

n. The initial control deficiency related to the fact that software development, modification or error correction changes were informally managed. While testing of changes was undertaken in a test environment by development staff, unless the changes are complex, there was generally no business user participation in testing. Business user/management sign-off was not required or solicited by IT development. Due to a lack of an IT manager, IT sign-off was not formally conducted. The absence of authorization over the change management of application software changes may result in the intentional or unintentional migration of invalid application changes into production that lead to the compromise of key systems, applications and data assets. As of 2012 fiscal year end, the process for program changes has been documented within the Change Management Policy. However this policy is in draft form and is pending updated data and additional input from the Configuration and Change Management Board.

We recommend that one business signoff be required on an appropriately initiated Change Request form to confirm that testing was appropriate and successfully completed. We further recommend that the software change not be put into Production (by appropriate IT Operations staff) unless there is Business approval and sign-off.

o. The initial control deficiency related to the fact that there was no DOL policy or procedure detailing with VABS and CATS Change Management. A lack of control over who has the ability to migrate software changes into production increases the risk that inappropriate and unauthorized changes could be made to software, moved undetected into production. As of 2012 fiscal year end, the Change Management Policy has been documented for the DOL. However this policy is in draft form and is pending updated data and additional input from the Configuration and Change Management Board.

We recommend that the DOL develop, introduce, and monitor a comprehensive DOL Change

Findings and Recommendations

Management Policy for application software which is consistent with any statewide DII policy on Change Management.

p. Due to the small size of the DOL's IT staff, developers are permitted to migrate software into production. An ability of IT development staff to migrate application software into production risks the introduction of inappropriate code changes.

We recommend that access to and migration of software into the production environment should be restricted to Production Control/Operations staff only.

q. Business management is rarely involved in testing or authorizing of application changes including configuration changes. All VABS and CATS application configuration changes are tested by application development staff but are not required to be validated by the business. An absence of appropriate testing and approvals by IT and Business personnel over application configuration changes may lead to the introduction into production of inappropriate and unauthorized changes that could adversely affect the results of financial application processing.

We recommend that all changes to production software including configuration changes should be formally approved and authorized by appropriate Business owners.

r. There is no policy or procedure to handle Emergency Changes**.** A lack of emergency change procedures that document changes made to production applications and jobs makes follow-up and future avoidance difficult and increases the risk that inappropriate or incorrect changes go undetected. Written policies and procedures also provide for continuity of operation during times of staff transition.

We recommend that the DOL develop, introduce, and monitor a comprehensive DOL Emergency Change Policy which is consistent with any statewide DII policy on Change Management. It is further recommended that a statewide policy on dealing with Emergency Production changes be written and introduced by DII.

s. Notification of emergency changes to Management is informal and not mandatory. There is no requirement for retrospective review and authorization. The absence of management reviews of emergency changes risks that inappropriate or incorrect modifications to applications could be introduced and remain undetected.

We recommend that all emergency changes to batch runs should be documented and notified to Business and appropriate IT management in a timely fashion.

t. Assets from backup media are restored when required for Operational reasons. There is no documented Disaster Recovery Plan or activity to restore systems to test recovery procedures. Without appropriate and periodic restoration tests, assurance cannot be placed on the reliability of backup media to recover key systems, applications and data assets in the event of an emergency.

We recommend that VDOL IT should immediately develop and document a Disaster Recovery Plan for recovering its IBM and related applications in the event of a data center

Findings and Recommendations

disaster.

Management Response

a. DOL is in the process of creating a VABS/FARS/CATS specific security policy upon existing DII policy. Should have document and approvals by end 3rd QTR 2013.

b. DOL Central Office is card access entry on. Non employees are escorted when they are admitted. The access door to the data center with key punch is now working, has been reinforced with a magnetic lock mechanism. The unlocked door allowing staff access to pick up print outs is protected by the fact that the building is locked down and that non-employees are escorted. Defeating those two barriers an intruder could then if still undetected climb over the 3 foot barrier wall created behind the open door. Key codes to the key pad door are restricted and periodically reviewed and the door to print outs will remain unlocked to staff during normal working hours.

c. Quarterly review by DOL Director of Admin Service and sign off is now documented.

d. Will be referenced in VABS/CATS/FARS policy, see 5a response

e. Change Management Policy will address this issue

f. Change Management Policy will address this issue.

g. Change Management Policy will address this, but regardless of the role currently played by programmers Lowe or Lucia, production sign off resides with IT Manager Patrick McCabe.

h. DOL is developing this process and will have a formal policy.

i. DOL follows the State of Vermont password policy network access <u>and</u> maintains in house AD settings that exceed that requirement. You can't get to VABS/CATS password screen without first complying with these standards.

j. DOL runs a quarterly job for UI Director that prints as a 21 page green bar print out. It contains all employee names and lists their VABS/CATS access by category. We NOW require a sign off on this listing quarterly. We provided this file physically to KPMP in December 2012 at their request.

k. DOL removes individual users access as they leave the department. Physical access cards are recovered or deactivated, domain access is removed, any dept equipment is recovered through the office of the Director of Admin Services working with DHR. We consider the quarterly review by UI Director as back up to this process for VABS/CATS.

l. See response 5j., the quarterly review process and sign off serves this purpose. The list is provided by IT Administration to UI Business Management, signed off and returned.

m. Change Management Policy in draft form as noted and will resolve the concern in this finding.

n. Change Management Policy in draft form as noted and will resolve the concern in this finding.

	Findings and Recommendations
	o. Change Management Policy in draft form as noted and will resolve the concern in this finding. p. Change Management Policy in draft form as noted and will resolve the concern in this finding. q. DOL would argue that Business management is always involved but their involvement is not documented, we will correct that in Management Change Policy. r. DOL will review and consider Emergency Production Change policies when they are available. At this time, all emergency production changes are approved and documented by IT Manager Patrick McCabe. s. Management Change Policy will address notice to Business and IT Admin. t. IT Disaster contingency Review began in Sept 2012 and documentation letter from BerryDunn was provided to KPMG December 13, 2012. We intend to follow up with an annual review after December 2013.
6.	**Application Name:** Management System (WMS), Point of Sale (POS), and Sequoia **Responsible Agency:** Division of Liquor Control **Purpose:** Manages warehousing, inventory, purchasing, AP, tracking of sales/revenues, commission, licensing and GL. In addition, Point of Sale terminals which are owned by the State and are installed in each store.
	a. The Programmer and Developer have access to both the development and production environment for Sequoia and POS. A lack of control over who has the ability to migrate software changes into production increases the risk that inappropriate and unauthorized changes could be made to software, moved undetected into production. We recommend a clear separation of access be created to restrict developers from having production access. This can be implemented with different resources, or with a work around that logs changes made by a developer that require a Manager's review and approval. ***Management Response*** As noted in our IT Change Management Policy (Version 1.0) instituted in October 2012 in response to previous auditor recommendations, these procedures are already in effect. In each of the two systems for which in-house development is still possible, the developer does not put changes into production. Due to limitations in staff, the specific role depends on the system. For Sequoia, the Systems Developer does development; putting changes into production is done by the IT Systems Administrator. For Point of Sale, development is done by the IT Systems Administrator; putting changes into production is done by the Systems Developer. In addition, in both cases, changes are logged in the Help Desk for review and a permanent record. All change logs are visible to all DLC staff members, including both IT and other staff up to and including the Commissioner.

	Findings and Recommendations
	Development is not possible in the Warehouse Management System (WMS) since it is a commercial software package developed by a third party, so there is no development to manage or restrict. (Even there, the Help Desk is used to log issues, although those issues are resolved with calls to the software provider, since the Help Desk is used to log all IT activities, not just development).
7.	**Application Name:** BFIS **Responsible Agency:** Agency of Human Services (AHS) **Purpose:** A system for Human Services Child Care Subsidy Payments.
	a. Password parameters are weak with complexity disabled. We recommend that the Agency enable complexity of pass word parameters. b. No formalized policy or process exists to determine users who no longer require access to the application due to termination. We recommend that the Agency implement a process to utilize the State of VT HR listing on a scheduled basis (monthly/quarterly) to verify users that should be removed from BFIS. c. Although ad hoc reviews of user access were performed; the review is not formally documented or occurrence defined. We recommend that the Agency create and implement a formal process for a review of access rights to the application and appropriate sign off retention of the performance of the review should be retained. d. Without standard scheduled partial and full backups, data may be lost and not available for restoration should an event occur and data is lost. The Agency relies on DII to perform and store backup data; however, the Agency was not aware of what the backup schedules are. We recommend that the Agency document the backup schedule and periodically review to ensure that all data sets are being backed-up appropriately. e. The Agency does not have a formalized restoration process and testing schedule for ensuring that data from backups can be restored completely and accurately. We recommend that the Agency document the process and a standard testing cycle for restoral of data from backup tapes. f. No formalized process is defined or utilized to respond to problems and issues by receipt of an email or a helpdesk ticket. We recommend that the Agency develop and utilize a tool that allows them to identify and track all problems and issues for the application.

	Findings and Recommendations
	Management Response a. There is a BFIS Upgrades project currently underway that includes this as a requirement. This project is scheduled to be completed in spring 2013. b. Quarterly BFIS Users Account is reviewed by BFIS Help Desk. A tracking sheet has been developed to document this activity. Ref: BFIS User Account Management Tracking Checklist. Ref: BFIS Monitoring User Protocol, All BFIS Users are reminded about Users responsibilities. c. This has been implemented and is a current work in progress. Quarterly BFIS Users Account is reviewed by BFIS Help Desk. A tracking sheet has been developed to document this activity. Ref: BFIS User Account Management Tracking Checklist. d. There is documentation as of December 2012, and includes review of all data sets. e. With the new backup system, developers can now schedule regular restore/backup on servers. Documentation of this process and standard testing cycle will be developed and in place by December 2013. f. A tool is currently being researched (potentially JIRA) and will be set up to track issues and resolutions. This will be in place by December 2013.
8.	**Application Name:** SSMIS **Responsible Agency:** Agency of Human Services (AHS) **Purpose:** A benefit and eligibility system for Foster Care, Adoption Assistance and Social Services Block Grant Programs.
	a. Password parameters are weak with no policies other than recommendations of data dictionary words that should not be used. We recommend that the Agency create and implement a set of standard password parameters. b. SSMIS perform ad hoc reviews of user access; however, the review is not formally documented or occurrence defined. We recommend that the Agency create and implement a formal process for a review of access rights to the application and appropriate sign off retention of the performance of the review should be retained. c. The Agency does not have formalized change management policy that outlines the requirements for making changes, obtaining approvals and the retention of the documents. We recommend that the Agency create a change management policy should be developed and issued for SSMIS and communicated to the organization. d. There is no formalized change management policy that requires that testing and approvals are

Findings and Recommendations

obtained prior to migrating a change into production.

We recommend that the Agency create a change management policy should be developed that defines the requirements for appropriate testing and approvals of testing prior to changes being migrated into production.

e. SSMIS do not have a formalized restoration process and testing schedule for ensuring that data from backups can be restored completely and accurately.

We recommend that the Agency document the process and a standard testing cycle for restoral of data from backup tapes.

f. SSMIS respond to problems and issues by receipt of an email or a helpdesk ticket. No formalized process is defined or utilized.

We recommend that the Agency develop and utilize a tool that allows them to identify and track all problems and issues for the application.

Management Response

a. Standard password parameters are being implemented as part of the SSMIS Upgrade project. This project is underway and is set for implementation in the Spring of 2013.

b. A formal process for reviewing access rights to the application and appropriate sign off retention of the performance of the review is being created as part of the SSMIS Upgrade project. This project is underway and is set for implementation in the Spring of 2013.

c. Currently, JIRA is being used as the Change Request mechanism. A formal change management policy will be created by the DCF ISD Standards Committee. Completion of this policy is planned for December 2013.

d. A change management policy that defines the requirements for appropriate testing and approvals of testing prior to changes being migrated into production will be created by the DCF ISD Standards Committee. Completion of this policy is planned for December 2013.

e. We do not use tape in our environment any longer, having recently converted to a solution that does replicated, versioning disk to disk (offsite) backups. We need to create new documentation of procedures and standard testing – this will be completed by December 2013.

f. A tool is currently being researched (potentially JIRA) and will be set up to track issues and resolutions. This will be in place by December 2013.

9. **Application Name:** ACCESS

Responsible Agency: Agency of Human Services (AHS)

Purpose: Benefit and Eligibility System for Human Service Cash Assistance Programs.

Findings and Recommendations

a. We noted that appropriate IT Security Policy exists and is communicated to employees via intranet. However, no evidence was provided to substantiate that the policies are reviewed periodically and updated by management. We noted that several of the policies have not been revised since more than a year.

We recommend that IT Security Policies be reviewed on an annual basis to ensure compliance with new regulations as well as to address potential security threats.

b. DII network Domain Administrator access should be appropriately restricted. KPMG was unable to obtain screens for the DII Domain Administrators. However, KPMG obtained and inspected the State of Vermont, Agency Department of Information and Innovation Organization chart to identify the Network and System Administrators. Without appropriate restrictions to the Domain Administrators group, applications and supporting infrastructure may be exposed to unauthorized access.

We recommend that appropriate documentation is provided to identify the Domain Administrators for the ACCESS application and verify the job roles and responsibilities of the Domain Administrators to assure appropriateness of their access.

c. Super User level access to the application should be limited to appropriate personnel and monitored to detect inappropriate activity. System access to add/change/delete user accounts should be limited to Security Administrators.

KPMG noted that developers have Super User access to the production system. In addition, DBAs are allowed to create, edit and delete users and can grant roles. KPMG noted that a vacant account "D14" has both the "SSS" role and the "DBA" role which gives DBA an ability to add, modify or delete a user account or grant user role in the production system. KPMG also noted that there are 3 additional vacant accounts (D20, D70 and D80). No monitoring is in place over the use of these ids. KPMG was informed that if a worker tries to login with a RACF ID that is not associated with their user ID they cannot get into the system. However it was noted in the case of two (D14 and D80) out of the four vacant roles noted above, the RACF ID was tied to user ID

We recommend that vacant accounts be removed to reduce the chance that the ID is misused. In addition, a monitoring process should be in place to assure against misuse of the super user capability.

d. On a periodic basis, business management reviews user access rights to the application to verify that access is appropriately aligned with users' job responsibilities and that terminated employees have not retained access. We were unable to substantiate periodic access review to assure that access is not retained for terminated employees and that access is appropriate for current users based on their job responsibilities.

We recommend that management perform periodic review of user access for the ACCESS

(Continued)

Findings and Recommendations

application. This will enable removal of inappropriate/inactive IDs in a timely manner and will reduce the possibility of malicious activity by unauthorized users. This review should be formally documented and evidence should be retained for audit purposes.

e. A change management document was not provided for review. KPMG was notified that DCF ISD has formed a Standards Committee which will be working on the development of a formal written policy and procedure. These documents are to be completed by the end of calendar year 2013.

We recommend that AHS develops processes and mechanisms to implement these policies as well.

f. AHS does not have appropriate segregation of duties. Personnel who have development responsibilities currently have access to migrate changes to the production environment. KPMG was informed that AHS is currently going to a reorganization that will address the segregation of duties requirements.

We recommend that conflicts of interest and concentration of power with any role be evaluated as part of the reorganization.

g. No evidence was provided to substantiate that adequate backups were performed. Without appropriate backups, there is a risk that financially significant information may be lost in case of a disaster or hardware failure.

We recommend that the Agency document the data backup and retention process and work with DII to monitor the effectiveness of backups. AHS should document the process and establish a standard testing cycle for restoral of data from backup tapes.

h. We noted that no ticketing system is used to track issues. The current process is manual and the mainframe group keeps track of issues via a spreadsheet. In addition, there is no formally documented process for logging issues and tracking them to resolution. Without a formally documented process for logging issues as well as appropriate controls in place to ensure that all issues are logged and tracked through resolution, there is a risk that all issue may not be tracked or resolved in a timely manner.

We recommend that the Agency utilize a ticketing system to manage the documentation of issues and problems to ensure proper management and resolution. A ticketing system provides appropriate structure and control to ensure that all problems are managed to resolution. Furthermore a formally documented policies and procedures should be in place to include process of tracking, categorizing and resolving issues in a timely manner.

i. We noted that the ACCESS system is not capable of enforcing the password complexity requirements as required by AHS Security Plan and System/Service Password Policy. Even though complexity is not enabled, the multi layer authentication process mitigates some of the risk associated with not having strong password parameters. In addition, password lockout is

Findings and Recommendations

enabled.

We recommend that the Agency investigate the possibility of enabling password complexity or a policy exception form should be obtained to document non-compliance with the AHS Security Policy requirements.

Management Response

a. Currently the position of AHS Security Director is vacant. Once this position is filled the task of reviewing security policies on an annual basis will be implemented by that position.

b. The ACCESS system is a mainframe application. Authentication is not handled by Active Directory; therefore, no Domain Administrators would have any access to the mainframe. There is full separation of duties and access between the Network/Active Directory environment and DII’s hosted mainframe environment.

c. It is true that a RACF ID must be associated with an ACCESS ID. For a user to get into the ACCESS system there is a further level of security with the password being removed/scrambled and the user access is revoked at both the RACF and ACCESS level. In ISD when a person leaves, we revoke access and scramble the passwords until such time as the position is either filled or a decision is made not to fill the position. If the position is not filled, then deletes are done and positions are marked vacant.

d. The periodic review of user access for the ACCESS application will be conducted by the business. ESD is creating a Business Application Support Unit (BASU) and will have responsibility for creating and managing procedures for account review. This unit and the procedures will be in place by December 31, 2013.

e. The DCF ISD Standards Committee will be developing a change management policy for the Department. As part of this work, processes and mechanisms for implementing the policy will also be developed. This will include management and oversight by the newly implemented Business Application Support Unit (BASU) within ESD. All work has a planned implementation date of December 31, 2013.

f. Within our teams we strive to have separation of duties. A developer who has made changes to programming does not migrate those changes to production without another developer reviewing the code. This is not a formal process however, as our current staffing levels prevent us from having the level of separation that we would like. As we continue to improve or internal work processes we will strive to improve in this area and will evaluate conflicts of interest and concentration of power with any role as part of our continuous efforts toward improvement.

g. In the ACCESS system we have a full stand alone backup that is created every Sunday. In addition we have 3 parallel backups that run on Monday, Wednesday, and Friday nights. We also have running what is called ‘protection logging’. All modifications to the database are logged in a separate file. This combination allows us to restore our databases back to any given point in time for the last week and to any backup time for a number of months in the

	Findings and Recommendations
	past. This restore capability is routinely used and tested in our test environments. The mainframe application also has a disaster site where the mainframe disc files are mirrored on a real time basis. In the event of a disaster at our main facility, we can immediately move to the disaster site where a complete and usable copy of our mainframe system is maintained. We also keep another copy of most of our data that is copied to a SQL database on a real time basis. This SQL database is used to feed a number of satellite applications such as data warehouses, voice response units, and web applications. This will be documented and monitored, per a Service Level Agreement with DII. h. A tool is currently being researched (potentially JIRA) and will be set up to track issues and resolutions. This will be in place by December 2013. i. Because the ACCESS application is not capable of providing the level of complexity required for passwords by our own policy, we will add to the existing AHS policy that the ACCESS application is exempt from this requirement. As efforts are underway to eventually move all programs off the ACCESS application in the next 5-10 years, requirements for password complexity will be considered on any new platforms the Agency may use.

Management Response

Responses are embedded in the above table.

FS2012-04 – Succession Planning

Background

Goal 8.4.1 of the Vermont Statewide Strategic Plan 2012, Version 4, December 2012, states "Develop and implement a comprehensive approach to workforce recruitment, hiring, retention, and planning resulting in a diverse, effective and efficient workforce to meet the present and future needs of Vermont State Government."

The State is a multi-billion dollar enterprise that has many diverse and complex business functions and decentralized operations. The State also operates in a dynamic environment and is exposed to many different risks and challenges. The average age of the State's workforce, like many other governments in the Country, continues to age and move towards retirement.

Finding

The issue of the pending retirement of the baby boomer generation has come to the forefront for businesses, including state government, as the first of the "boomers" have reached retirement age. Over the next decade, as more state employees reach retirement age, the State will be faced with a tremendous loss of institutional knowledge and possibly significant deficiencies in highly specialized areas and functions. The effects of this are already starting to be seen as evidenced by the types of financial statement

and compliance findings noted for the current audit. The lack of critical resources highlights the need to immediately implement an appropriate personnel succession plan throughout the State.

In order to ensure continuity of service and minimize the loss of institutional knowledge, it is essential that the State develop and execute a succession plan that will address this inevitable challenge.

Recommendation

We recommend that the Department of Human Resources continue to work with individual agencies and departments to ensure that formal succession plans are developed for all key functional areas; that the plans are current; and that the plans are appropriately communicated and acted upon.

Management Response

DHR will conduct training in calendar year 2013 for members of the Governor's extended cabinet that will highlight the need for succession planning, given the pending retirement of the baby boom generation. At this training, DHR will provide tools and guidance to senior leaders to help them prepare formal succession plans for their Agencies and Departments. In addition, the Secretary of Administration will also review the need for and efforts made to date on succession planning, as part of the annual reporting process on each Agency and Department's strategic plan.