Indiana Bureau of Motor Vehicles

May 11, 2015

Table of Contents

Indiana Bureau of Motor Vehicles

Assessment

I. Background

The BMV became aware of transactional inaccuracies that had resulted in both undercharges and overcharges to Indiana residents. The Bureau of Motor Vehicles Commission **(**BMVC) engaged BKD in late 2014 to conduct an initial assessment with the objective of developing a proposed project scope for BMV managements' consideration. We were subsequently engaged for a second project, which entailed performing procedures to assess the processes and controls related to the assignment of fees and taxes. Our assessment supplements the ongoing procedures being performed by associates at the BMV and their outside legal counsel.

Indiana state law and administrative rules are the authority for the fees and taxes charged by the state of Indiana and collected by the BMV. The funds are then regularly distributed to county and local governments and foundations. Transactions are processed on the System Tracking and Record Support (STARS) application, which was partially implemented in 2004 and fully implemented in 2006.

The BMV is Indiana's second largest state agency. During our assessment, BKD identified over 5,500 lines on the Master Fee Table within the STARS system. The 5,500 lines represent approximately 1,200 unique fees and taxes, as well as 120 unique funds the BMV is responsible for administering.

In 2014, approximately $460 million in fees and $490 million in excise, wheel and surtaxes was collected and later distributed to other state agencies or organizations. The BMV serves Indiana residents in 132 branches within 92 counties. Examples of BMV annual transactional counts:

1. Approximately 12.5 million total transactions
2. 7.4 million vehicle registrations
3. 2.2 million license plates issued
4. 2.1 million vehicle titles

The Contact Center receives and processes over two million calls from residents annually. Driver education and safety programs, including driver education schools, motorcycle safety programs and various skills examinations, are also managed at the BMV's central office.

During the course of our assessment, we identified a number of issues, which are outlined further in the subsequent sections of this report. BMV personnel are proactively working to identify potential issues. Late in 2014, a new internal reporting process was implemented providing employees a method to report potential problems. Not only has this new process encouraged open communication throughout all levels of the BMV, it has also created an increased awareness by the employees. BMV management should be commended for encouraging open communication and transparency.

II. Executive Summary

Executive Summary of Key Findings and Recommendations

BKD presents the following summarized recommendations for consideration. Detailed observations are listed in Section IV of this document.

During the course of our review, BMV management was proactive in addressing issues, as they were communicated and prior to release of this report. Details of their actions are contained in the appendix, Section V, of this report. The corrective actions listed have not been validated by BKD for design or operating effectiveness.

- **Overly Complex and Ambiguous Legislative Authority for Fees and Taxes**

Currently, the BMV is responsible for administering approximately 1,200 fees and taxes as outlined in Indiana Code (Code). The language of the Code providing authority for the BMV's fee and tax schedule is ambiguous and very complex. This presents a risk of multiple legal interpretations and inconsistent application. The BMV should work with the Indiana Legislature to review, reduce and simplify the overall Code structure for fees and taxes.

- **Effectiveness of BMV Leadership Structure Should be Evaluated**

Given the complexity of their charge, the BMV should demonstrate a commitment to establishing a workforce capable of supporting their mission. An evaluation of the effectiveness and proficiency of key leadership positions should be performed. In order to promote increased accountability, the BMV should also review current reporting structures, authorities and responsibilities.

- **Lack of Governance and Responsibility for Ongoing Compliance with Legislation**

There is no centralized authority or oversight of ongoing compliance with legislative code. The BMV should establish a Project Management Office to oversee ongoing compliance holistically with laws and regulations, operational change management, issue tracking and resolution.

- **Lack of Adequate Change Management Processes in STARS**

Formalized Information Technology Change Management Policies and Procedures do not currently exist. Policies and procedures should contain adequate detail for controlling modifications to hardware, software, firmware, all in-house development of the STARS system queries and ancillary interface programming tasks. Processes used in the December 2014 System Build were less than adequately controlled.

- **Information System Design Does Not Adequately Support Business Processes**

Information systems should add measureable value to business operations and support business processes. The BMV's information system, STARS, does not meet the requirements of end users and operational leaders. As a result, processing in almost every operational area has become manually intensive, does not allow for consistency in processing activities and requires users to rely on workarounds or overrides. A comprehensive feasibility analysis should be conducted to determine if STARS is an adequate solution. This analysis should consider the cost/benefit of upgrading outdated infrastructure, creating technical documentation, improving functionality to meet user requirements, verifying system data processing and evaluating the remaining useful life of the application.

- **Lack of Independent Monitoring and Oversight**

Branch operations are independently audited on a consistent basis; however, the BMV's central office has not been independently audited for over five years. Implementation of an internal audit function would provide an independent and objective assessment of the adequacy and effectiveness of management's internal control system and related processes.

- **Lack of Adequate Master Fee Table Maintenance Procedures**

Fees, taxes, fund names, fund allocations and effective/end dates are some of the critical fields contained with the Master Fee Table within the STARS system. Accuracy of these data values is essential given the values contained in the table are the basis for calculations and amounts assigned during transactional processing. We noted errors and inconsistencies in these fields, which could impact processing accuracy.

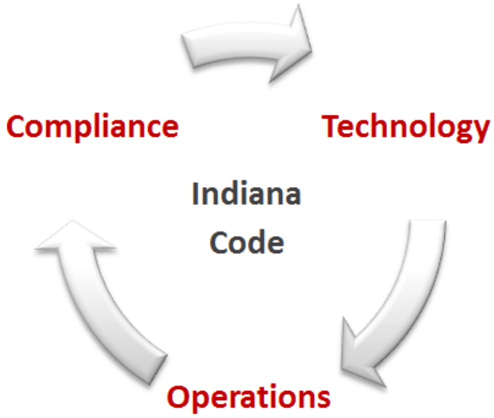
- **Lack of Formal System Development Lifecycle (SDLC) Policies and Procedures**

The BMV does not have a standardized set of documented guidelines and procedures for SDLC, including project management, and change management policies and procedures defined and documented. Without formal policies and procedures, the BMV cannot adequately control the processes used for making modifications to hardware, software, firmware and all in-house development of the STARS system, queries and ancillary interface programming tasks.

III. Scope and Procedures

Summary and Scope of Work Performed

Indiana Code is the authority for the amounts charged by the state of Indiana and collected by the BMV. BKD was engaged by the Indiana BMVC to conduct an assessment of the BMV's central office operations. Our scope did not include a review of the branch locations throughout the 92 Indiana counties. The objective of our engagement was to identify process and control deficiencies that could potentially affect the appropriate assignment of fees and taxes to transactions and to formulate recommendations for improvements. Our assessment was comprised of the following three functional and interrelated components: compliance, technology and operations.



Compliance

Technology

Indiana Code

Operations

BKD conducted interviews of personnel, performed process walk-throughs, reviewed the applicable legislative code and analyzed available documents and data. In performance of our assessment, we:

Compliance

- Obtained and reviewed Indiana Code related to fees and taxes
- Traced the fees and taxes from the Indiana Code to the Master Fee Table in BMV's system, STARS
- Interviewed key personnel

Operations

- Traced the fees and taxes from the Code to BMV forms and manuals
- Conducted walk-throughs and inquires of various operational areas
- Interviewed key personnel

Technology

- Reviewed and tested Change Management Controls used for updating the STARS system
- Reviewed and tested the security controls for user access related to the STARS system
- Interviewed key personnel

III. Scope and Procedures

BKD evaluated the BMV's central office operations by applying the 17 principles of effective internal controls as outlined in the Committee of Sponsoring Organizations' (COSO) updated *Internal Control – Integrated Framework* (see Appendix A). BKD focused on identifying and evaluating the following control components:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

An effectively designed internal control system contains a mix of preventive, detective or corrective controls and, when implemented properly, would effectively mitigate the risk of not meeting critical business objectives; such as, accuracy, timeliness and completeness. Within any control system, however, inherent limitations exist. Human judgment, technology and process complexity are examples of inherent limitations. All personnel play a role in an effective internal control system, but management is responsible for maintaining an effective control environment and ongoing monitoring.

The control gaps and deficiencies identified within the BMV's internal control systems permitted the condition for transactional errors to occur. This report should not be viewed as all-encompassing of every control weakness that may exist. Our assessment results should be used as a benchmark for purposes of measuring future improvements.

IV. Observations and Recommendations

BKD provides the following recommendations for consideration. To effectively mitigate the identified risks, BKD suggests a complete implementation of the recommendations in this document. Because systems and processes are interrelated, partial implementation would not adequately address the weaknesses identified in the BMV's internal control system.

Compliance Recommendations

To assess compliance with the Code, BKD attempted to trace and agree the amounts outlined in the Code to the Master Fee Table within the STARS system. To further assess compliance, we also attempted to trace and agree the same amounts to internal manuals, forms and other documents to identify instances of noncompliance.

Simultaneous to our review, updates were being made by BMV associates to the Master Fee Table without our knowledge. Upon our discovery, we were unable to adequately determine what fields had been updated or the extent of the changes due to poor information technology (IT) change management processes and controls. Therefore, our validation can only be relied upon for a point in time.

1. Overly Complex and Ambiguous Legislative Authority for Fees and Taxes

The BMV is responsible for administering approximately 1,200 unique master fee IDs that relate to fees and taxes as outlined in the Code. BKD attempted to trace and agree the amounts listed in the Code to the Master Fee Table within the STARS system to ensure fees and taxes were loaded accurately. While BKD was not engaged to make legal interpretations, we did note the current language is very complex and not always clear. The ambiguous and vague wording creates an increased risk of multiple interpretations and inconsistent application in transactional processing.

BKD noted that some fees have multiple definitions that cannot be reconciled. For example:

- The BMV charges fees for "amendment" or "replacement" transactions, but the applicable Code does not clearly define what is an amendment or a replacement (Sections 9-29-9-25 and 9-29-9-13).

- There are different fees for a "plate swap" vs. a "plate transfer" transaction. It is not clearly defined in the Code when one applies or when the other does or when a registration should be treated as a new registration.

- There are other ambiguous statutes, such as the excise tax collection service charge (IC 9-29-1-10) and how it is not clear whether it should be applied once or twice when the BMV performs a long registration.

The quantity of fees alone makes administration challenging. BKD performed a high-level analysis on transactional data covering an 18-month period to determine the frequency of occurrence of the 1,200 IDs. We noted the following:

- 38 percent of the IDs were used less than 100 times
- 18 percent of the IDs were used less than 10 times

To reduce the risk of inaccuracies and noncompliance, the BMV should work with the Indiana Legislature to review, reduce and simplify the overall Code structure for fees and taxes.

2. Lack of Governance and Oversight for Ongoing Compliance with Legislation

The BMV does not have a centralized authority accountable for ongoing compliance with legislative code. Compliance efforts are fragmented and disorganized with little to no proactive monitoring occurring. As laws change, business unit management is responsible for interpreting the impact of the changes to their areas and determining, on their own, what updates are needed to related forms, manuals and processes. There is no centralized oversight to ensure proper interpretation and comprehensive operational change management. A universal issue-tracking process does not exist, nor does a formal practice of assigning accountability and monitoring resolution. Without centralized oversight, the BMV has limited transparency into their level of compliance or the related efforts as a whole.

As an example, while performing our assessment, BKD noted a potential discrepancy between the amount listed in the Code and one of the BMV manuals. We met with the area manager to discuss the Code and inquire about the potential discrepancy. During the conversation, the manager updated the electronic manual and performed the edit without any additional interpretation, oversight or internal review for appropriateness.

Centralized oversight is essential to consistent guidance and accountability. The BMV should establish a suitable governance structure in the form of a Project Management Office (PMO) and program manager. A PMO would provide centralized oversight and promote standardization by developing a common set of policies, procedures and principles for managing operational changes and issue resolution. Responsibilities would include capturing requests, maintaining an inventory of projects underway, coordinating with the business units, measuring progress of improvements and tracking issues and resolution. To be effective, it is critical the PMO and program manager be engaged with the business units and be viewed as a partner in their compliance efforts. The PMO should be responsible for providing oversight and guidance only and should not be viewed as the owner of controls, which is the responsibility of management.

3. Lack of Independent and Objective Monitoring

The BMV's central office does not have an internal audit function. While the branch operations are independently audited on a consistent basis, the central office has not been subject to an internal audit for a number of years. An internal audit function would provide ongoing independent and objective assessments of the effectiveness and efficiency of business controls, regulatory compliance or financial activities. The current culture operates in a reactive mode versus proactively monitoring for instances of noncompliance or control failures. Without an internal audit function, there is limited assurance as to the adequacy and effectiveness of management's internal control system and related processes.

The BMV should consider establishing a formal internal audit department. An internal audit department would improve overall governance and risk awareness. If established, it is critical the function reports to a high-level official or state agency to ensure the appropriate status and authority. The function should not have any direct reporting relationships with departments or functions that could be subject to their audit processes. To ensure adequate coverage, the internal audit activity should consider every area within the BMV's central office, including information technology, in their risk assessment and scoping processes. They should have unrestricted access to personnel, documents, records and property.

4. Lack of Adequate Master Fee Table Maintenance Procedures

Fees, taxes, fund names, fund allocations and effective/end dates are some of the critical fields contained with the Master Fee Table within the STARS system. Accuracy of these data values is essential given the values contained in the table are the basis for calculations and amounts assigned during transactional processing. In performance of our procedures, we noted the following risks:

- Lack of historical traceability and version control of fees

  Each fee and tax is assigned a unique Master Fee ID. As legislation changes, the fees are updated within the Master Fee Table. As a result, STARS programming logic assigns a random, new master fee ID number and new record. For example, the Johnson County Surtax has two Unique Master Fee IDs of 309591 and 308769. Because the system assigns random numbering, the ability to trace historical data is greatly diminished. (For example, if a fee has a code of 10000, the updated ID should be 100001, allowing for the appropriate version controls and traceability.)

  BKD observed IT personnel writing a Structured Query Language (SQL) query for a specific fee. Because of the random numbering, IT associates are required to query by a word or name instead of using the fee IDs as a key search criteria. Fee names can change over time and should not be the primary basis for identifying historical transactions.

- Fee and fund names in the Master Fee Table do not match names in the Code

  In performing our procedures, BKD experienced difficulty when attempting to trace and agree the amounts in the Code to the appropriate record on the Master Fee Table. Fee and fund names did not always match the names in the Code, requiring judgment and creating a risk of error. For example, Code 9-29-5-24 is titled *Nonresident Transport Vehicle Decal*; however, in the Master Fee Table, it is titled *90 Day Agriculture Permit.*

As BMV personnel perform routine maintenance and updates, they would be subject to the same risk of error as BKD. Names in the Master Fee Table should be updated to more closely align with the Code. Alternatively, the BMV should consider adding a field to the Master Fee Table containing a reference to the applicable section in the Code that supports each record. Doing so would reduce the risk of errors and provide a quick reference for research purposes.

- Instances where effective dates are not accurate

  BKD noted instances where effective dates of fees and taxes were not accurate on the Master Fee Table, as they were often backdated. Through inquiry, we determined that backdating is a common BMV practice for purposes of testing. For example, if an existing fee is updated or a new fee added and, per the Code, has an effective date of 1/1/YY, BMV will backdate the value in the effective date field by a couple of weeks or months to correspond with the timing of their testing. It was explained to BKD that in order to test the functionality of the Code in a test environment, the effective date is backdated to match the date of testing. The effective date is not corrected to show 1/11/YY prior to being moved into production. If an updated fee is moved into production prior to the effective date (1/1/YY), then a risk exists that a code would have multiple unique fee IDs associated, creating an overlap in effective dates. The process is not ideal and creates an increased risk of error in transactional processing.

- Fund allocations listed as "remainders" are programmed as flat fees

  In tracing the fund allocations from the Code to the Master Fee Table, BKD noted instances where "remainder" amounts were hard coded into the Master Fee Table instead of being programmed to logically calculate and load the appropriate amount.

The values contained in the Master Fee Table are the basis for all fees and taxes used in transactional processing. The integrity and accuracy of the data is critical to ensuring the accuracy of processing. It is recommended the records in the table be reviewed and updated to more accurately reflect the nomenclature and effective dates contained within the Code.

IV. Observations and Recommendations

Operational Recommendations

The following recommendations were identified through inquiry, walk-throughs and observation. Testing of control design or effectiveness was not performed in the operational areas.

1. Effectiveness of BMV Leadership Structure Should be Reviewed

Given the complexity of their charge, the BMV should demonstrate a commitment to establish a workforce capable of supporting their mission. A sound control environment has processes in place to evaluate, attract, develop and retain individuals in key leadership positions. In order to promote increased accountability, the BMV should review current reporting structures, authorities and responsibilities. Further, management should evaluate the effectiveness and proficiency of key leadership positions and act as necessary to address shortcomings. A commitment to provide the mentoring and training needed to attract, develop and retain sufficient and competent personnel to support the achievement of objectives should be implemented.

2. No Centralized Document Repository and Ownership

In attempting to validate the accuracy of fees and taxes on printed documents, such as forms, letter templates and other documents, BKD requested a comprehensive inventory of the forms and documents used by the BMV. The BMV could not provide this information, and it was determined that each business unit is responsible for identifying and updating forms and documents used by their area.

We randomly located and assessed documents. We noted a lack of version controls on the majority of them. We also noted that employees would often use letter templates stored on their hard drives, which creates a risk of using an outdated letter template that could contain inaccurate fee amounts.

Good information governance involves centralized records management, which merges decentralized records and documents into a single digital repository for proper oversight. It is recommended the BMV establish a centralized document repository, a comprehensive inventory and accountability for oversight.

3. Use of Business System Analysts in Change Management Process

Business managers often have difficulty in adequately completing Service Request (SR) forms due to the technical nature of the information required and, as a result, the forms are not completed adequately. A Business System Analyst (BSA) functions as the liaison between the business units and IT. BSAs provide insight into operational expertise and system functionality. They also interact with the quality assurance (Q/A) teams to ensure testing scenarios are adequately designed, performed and documented, and provide a more global approach to the System Development Life Cycle (SDLC) processes.

BMV should consider adding BSA positions to assist in the change management processes by bridging the gap between the technical and operational areas.

4. Limited Reporting Capability

During performance of various operational walk-throughs, as well as discussions with the chief information officer (CIO), BKD determined the STARS system relies heavily on internally developed SQL queries, varying levels of manual processing and voluminous paper trails to provide reporting capabilities of transactional processing. Reporting functionality in the STARS system is generally nonexistent, no data dictionary exists, and a standard listing of all available SQL queries, with descriptions to the field level, at the specific point of processing, is unavailable. Without adequate reporting, management is limited in their monitoring capabilities and lacks operational transparency.

The Treasury Department is highly reliant on the STARS system to ensure that all of the refunds get processed appropriately. The Treasury Department processes refunds for excise and wheel taxes, when the branches are unable to process them through the STARS system. Refund transactions are batched and converted to text files in the STARS system for transmittal (via upload) to the State Auditor's PeopleSoft system.

Process walk-throughs with the Treasury Department management revealed that normal refunds have a two-week lag before they are batched and sent to the State Auditor's office for processing. During this two-week lag, these refunds are added as credits to customer accounts, which can be applied to charges incurred during that period. The State Auditor's office creates the refund checks and returns them to the Treasury Department for mailing. Currently, there is no reconciliation between the STARS and PeopleSoft systems.

The distributions/reconciliation manager (finance department) creates a file containing all issued check information and uploads it into the STARS system. Due to a lack of standardized reporting functionality, sufficient monitoring controls to ensure all refunds are appropriately issued are nonexistent, and manual verification of refund distributions is ineffective. Additionally, as noted in the ITGC comment section of the report, BKD determined that, although the STARS system interfaces with a number of governmental agencies, including the State Auditor, application interface diagrams and interface edit controls between the STARS system and the PeopleSoft system cannot be determined, documented or tested adequately.

The Build Committee and operational management should collaborate to determine, standardize and refine reporting needs and capabilities. These should be developed, documented and implemented for the major operational transactional processes and business units.

Procedures for monitoring of the STARS reports should be fully documented and implemented by the business units. These procedures should specify the designation of a primary and backup reviewer, the frequency of review, departmental contacts for violation types and documentation requirements for the review process.

5. Master Fee Table – Lack of Monitoring Access and Changes for Appropriateness

BKD determined that a number of people, including the former CIO, had access to edit values on the Master Fee Table. Because the data contained on the Master Fee Table is the basis for transactional process, access should be very limited to only a few individuals. BKD could not obtain a Master Fee Table File Maintenance report, demonstrating the logging of additions/deletions/revisions of all BMV fees. Without the logging of these events, BMV management cannot actively monitor changes for appropriateness.

A Master Fee Table File Maintenance report should be created and implemented for the STARS system. An independent review of the File Maintenance Report should also be implemented and monitored frequently. The independent reviewer should ensure that all changes reflected on the system are supported by approved SRs.

Further, monitoring controls should be developed, documented and implemented for reviews of the Information Technology Department (ITD)-developed queries and/or reporting detailing Master Fee Table parameter changes, security events, user changes and significant system modifications. Without these controls in place, unauthorized access and changes could occur and go undetected.

6. Data Warehouse – Not Fully Utilized or Standardized

During walk-throughs and discussions with management, BKD determined the STARS system and users rely heavily on ITD-developed SQL queries against production to provide reporting capabilities of transactional processing. Although the data warehouse decision support system (DSS) is supported by SQL 2012, the STARS system itself, which refreshes the data warehouse DSS daily, is currently operating on the SQL 2008 r2 SP2 platform, which is sunset, or end-of-life.

Custom SQL queries and report creation activities are coordinated centrally to the ITD team. Per discussion with the CIO, the ITD does not have documented query and report guidelines, standards and procedures. Documented standards, guidelines and/or procedures do not exist for the data warehouse DSS. Reports in the data warehouse DSS are based on: (1) requirements (from the user) to run the business; (2) ticketed time; and (3) time by channel. Data monitoring software is not used to provide information about: all databases, tables, columns, rows of data and profiles of data residing in the data warehouse DSS, as well as who is using the data and how often they use the data. During discussions with data warehouse DSS manager, BKD also determined that no manual procedures exist to document this data either. Running queries against production produces results that are inconsistent, depending on the timing of the query.

During discussions with the data warehouse DSS manager and a review of the data dictionary, BKD determined the data warehouse DSS is not being utilized enterprise wide. We recommend the build team, the data warehouse DSS manager, and the acting CIO collaborate with the business unit management to determine more effective, widespread utilization of the data warehouse DSS queries and reporting capabilities.

We recommend that executive management ensure data warehouse DSS standards, guidelines and procedures be designed, documented and implemented for the data warehouse DSS, in accordance with Best Practices guidelines. Standards should be documented and implemented that address data verification practices, naming conventions and provisions for updates following changes to database elements or system structure.

7. Lack of Automation in the Driver Education Department

In 2012, the BMV officially began administering the Driver Education application and licensing processes for schools and instructors. One program coordinator receives all application information, tracks all application information, approves all application packages and processes all licenses, which is effectively a segregation of duties issue.

The Driver Education application and licensing processes are manually intensive, and current BMV policies and procedures are not completely documented. Beginning December 25, 2014, electronic applications were no longer accepted. Online payments, via ACH, debit or credit cards, are not available. All applications (instructor and school) must be submitted to the driver education department via the USPS mail service, with a money order or check. Incomplete applications are manually tracked before they can be approved. All applications and supporting documentation are maintained in locked cabinets for one cycle, which comprises two years from receipt of the application package.

Executive management should consider fully automating the Driver Education application and licensing processes. Applications should be completed, submitted and paid for online. Applications should be rejected automatically by the online system when they are incomplete, in order to reduce administrative time in tracking open items manually. Management should consider using the STARS system for automatic license generation, instead of the current third-party processing arrangement, which can take from 7 to 14 business days. The FORTIS document management system is interfaced to the STARS core system, and all application documentation maintained in locked cabinets can be set up to be scanned into the FORTIS system using the KOFAX scanning tool. Management should add reporting functionality to the STARS system to enable users to track expiring schools and instructors, instead of the current manual process. The STARS system should be programmed to auto-expire schools/instructors when the expiration date is exceeded.

Regardless of the choice to automate these processes, the Driver Education application and licensing processes should be fully documented in policy and procedures.

IV. Observations and Recommendations

Information Technology General Controls (ITGC)

BKD performed an assessment of key IT controls to evaluate the effectiveness of the control environment in which transactional processing occurs. The objective was to ensure that processing is occurring in a controlled environment to support consistent processing, data integrity and security. Our assessment concentrated on the IT entity-level controls, IT governance, IT change management and logical access security processes on the operating system and application system.

1. Lack of IT Strategic Plan and Governance

The BMV does not have an IT strategic plan. Without a strategic plan, they do not have an effective methodology for managing IT costs, allocating IT resources or planning for future investments. A strategic plan should cover all aspects of technology management, including cost management, resource management, infrastructure planning and management, application management and vendor management.

The BMV would derive more value by proactively planning as opposed to being reactive. Executing an IT strategy should include collaboration between all areas of IT and operational leadership. The foundation of the strategic plan should be driven by business requirements and the goal of operational excellence. The BMV should create an IT strategic plan with an outlook of one-, three- and five-year periods.

2. STARS Infrastructure No Longer Supported (SQL 2008 r2)

During our assessment, we noted the core BMV STARS application is currently running on SQL 2008 r2 servers. Mainstream support for the SQL 2008 r2 product, released July 20, 2010, ended on January 14, 2014, with the end of extended support scheduled for January 8, 2019. BKD inquired about a timeline and formal plan to upgrade. We were told a formal plan did not exist. It is recommended the BMV migrate from the sunset SQL 2008 r2 product to the more robust SQL 2012, or current SQL 2014 product. This should be included in the IT strategic planning document.

3. Standardization of STARS Application Configuration Parameters

Initialization parameters are set at install, as defaults, as part of the SQL server build. The STARS application uses standard configuration parameters, which have not been documented in the install documentation. We recommend that all configuration parameters for the core STARS application be consistently documented, for all versions, in order to provide assurance the same parameters are consistently applied across the operating environment. Documentation of system specification and parameter changes should be standardized to consistently evidence the following, as applicable: description of the change; requesting manager/department and date; data entry employee and date; and change reviewer and date. Such information can then be compared to system reports, by operational staff and supervisors.

4. BMV Microsoft Windows and Active Directory Migration Plan

The Microsoft Windows/Active Directory platform provides a central location for network administration and delegation of administrative authority. Use of the Active Directory operating system allows access to objects representing all network users, devices, and resources, and the ability to group objects for ease of management and application of logical security and group policy. Active Directory provides information security and single sign-on for user access to network resources, including shared directories.

During discussions with the Indiana Office of Technology (IOT) team supporting the BMV's Windows and Active Directory platform, BKD determined the BMV network environment is comprised of one Windows 2003 AD forest with 13 child domains (Windows 2008 r2).

Mainstream support for the current BMV platform supported by the IOT, Microsoft Windows Server 2003 r2 with Service Pack 2, ended on July 13, 2010. Support ends 24 months after the next Service Pack releases or at the end of the product's support lifecycle, whichever comes first. Extended support for the Microsoft Windows Server 2003 r2 with Service Pack 2 ends on July 14, 2015. Migration to Windows Server 2015 is scheduled for Summer 2015.

We recommend the BMV document an effective Microsoft Windows/Active Directory platform migration strategy, including a review of all access in all shared directory structures, in an adequate strategic plan, with appropriate considerations for vendor support of current versions of the network operating system, in coordination with the IOT's strategic direction and implementation plans.

5. Lack of Formal System Development Lifecycle (SDLC) Policies and Procedures

Section 5.14 of the Information Security Policy (ISP), revision 0, effective date February 4, 2014, states:

> *"The BMV's Chief Information Officer (CIO) is responsible for the implementation and maintenance of normal software development processes based on industry standards and/or best practices."*

During several meetings with the former CIO, application development managers, members of the Build Committee, the database administrator (DBA), and members of the Q/A team, BKD determined the BMV does not have a standardized set of documented guidelines and procedures for SDLC, including project management and change management policies and procedures defined and documented. Without formal policies and procedures, the BMV cannot adequately control the processes used for making modifications to hardware, software, firmware and all in-house development of the STARS system, queries and ancillary interface programming tasks.

Enterprise-level policies are concise statements of "how" an organization is expected to conduct its actions and processes. Change management policies should define what constitutes a "change" and establish minimum standards governing the change process. Provisions for requesting, approving, implementing, testing, verifying, accepting and documenting all changes should be clearly stated, including the specific teams/departments/individuals responsible for each stage of the process. Procedures should describe how each policy will be put into action. Each procedure should outline steps to be taken, forms to use, approvals required and exception handling.

BKD recommends that formal SDLC policies and procedures be documented and published. During a review of the December 2014 Build Document (the Build) and subsequent discussions with the CIO and his deputy director, BKD determined that a SR ID #966 had been included in the Build, entitled "PCI Remediation 121813." Although the SR references PCI Remediation, it in fact details a far more structured SDLC methodology than the currently undocumented processes described in the ISP. We recommend that SR ID #966 be reviewed and revised to accurately encompass all build processes, *e.g.*, SDLC, project management and change management methodologies. It should be noted that observations # 6 - 10 in the ITGC section are either related to, or the result of, not having formally documented policies and procedures.

6. <u>STARS Build Process – Lack of Adequate Risk Assessment and Prioritization Criteria</u>

The BMV conducts semi-annual "Builds" or updates to the STARS system each June and December. The Build is comprised of a number of SRs, which are standardized and sequentially-numbered forms. Each SR contains the following sections describing, at a minimum:

- Statement of work description
- Original service request description
- Notes and applicable business rules
- Risk assessment

Documented standards, guidelines and procedures have not been created and implemented for the SR process. Although a Build Committee is comprised of several members of various business units and IT employees, the decisions and priorities regarding SRs are decentralized to the business unit level. Because of this, the requested change may not be evaluated with consideration to the entire BMV operating environment.

To assess the current prioritization processes and controls, BKD reviewed 100 percent of the SRs (165) and supporting documentation constituting the most recent Build (December 2014). We noted the following:

- The risk assessment table of the SR form, which provides insight into the impact of each change and is a means for prioritization, had not been filled out on 157 of the 165

(95 percent) SRs. Without complete information on the SR forms, the BMV risks excluding higher-risk items in their semi-annual system updates.

- BKD noted that ranking criteria and scoring was not regularly used in the December 2014 Build. Two of the SRs had been prioritized as level '1' on the Team Foundation Server (TFS) Log, while the remaining supplied TFS Logs contained the default level '2' for each SR.

The Build Committee should establish documented standards, guidelines and procedures specifying the standard Build documentation required for all SRs, and ensure all documentation is appropriately filled out prior to authorizing individual SRs and the semi-annual Builds, in order to provide traceability from the development phase to the Q/A phase, through the parallel testing phase and ultimately into the production environment. Additionally, guidelines for integrating the efforts of both the ITD and IOT teams, in the development process should be documented and communicated to both teams to ensure there are no lapses in documentation standards for all SRs.

Management should implement a standard requirement that the embedded Risk Assessment table of each SR be filled out, in order for the change(s) to be authorized for development and implementation into the production environment. Clear statements of the applications, end users, network segments, systems and/or business functions should be documented, if necessary, on a separate document, with all supporting documentation, in order for the Build Committee to perform its impact analysis of the SR on the BMV operating environment. Additionally, if the SR requires process, transaction, menu, screen and/or form changes in user procedures, these changes should be documented, user training documentation should be created and attached to the SR, including any BMV manual revisions, and the branch operations department should be notified of the proposed changes. If the changes do not require process, transaction, menu, screen and/or form changes in user procedures, this statement should be documented in the appropriate section of the Risk Assessment table in the SR form. Prior to its implementation into the BMV production environment, the Build Committee should perform a final review of all SR Risk Assessment tables, and document an overall Build Risk Assessment for each semi-annual Build of the STARS system.

We further recommend the BMV implement a more structured approach to prioritizing requests. Selection criteria should be developed, defined and weighted. Doing so would provide consistency and a common terminology for discussions. Per discussions with the prior CIO, a ranking feature is available in the embedded priority feature in the SR system. BMV management should consider using this feature as part of their improved change management processes.

7. <u>Lack of Controls For Emergency System Changes (Hotfixes)</u>

In certain circumstances, when critical processing services are down or not operating correctly, emergency changes (hotfixes) may be required to be completed before they can be routed for approval by management. Typically, the prior CIO had the authority to approve hotfixes, as necessary. All documentation, *e.g.*, SR form, test matrices and supporting documentation, Build Committee Meeting Minutes, and User Testing Meeting Agenda, should be completed as soon as possible after the hotfix is implemented into the production environment. The individuals approving the emergency change(s) should evaluate appropriate testing, backup/back out procedures, and notifications to all locations/employees/customers, as the situation allows.

During the February 2, 2015, meeting with BKD, the Build Committee assured BKD that all emergency fixes associated with the December 2014 Build followed the same guidelines as normal SRs. BKD obtained documentation for the 42 hotfixes performed during a 6-month time period. Of those, we noted the following:

- 7 (16.7 percent) had no supporting documentation

- 27 (64.3 percent) of the supplied documentation had not been filled out completely

- 12 (28.6 percent) had no test matrices

- 27 (64.3 percent) had no Build Committee Meeting Minutes

- 18 (42.9 percent) had no User Testing Meeting Agendas

- 12 (28.6 percent) documentation was not supplied timely (until February 24, 2015, 20 days after the initial receipt of documentation for the December 2014 Build)

- 6 (14.3 percent) had no SR documented

Of the 23 hotfixes performed prior to January 1, 2015, and included in the December 2014 Build, we noted the following:

- 22 (95.6 percent) of the supplied documentation had not been filled out completely
- 18 (78.3 percent) had no Build Committee Meeting Minutes
- 3 (13 percent) of the supplied documentation had not been filled out completely
- 2 (8.6 percent) had no User Testing Meeting Agendas
- 1 (4.3 percent) did not have an SR documented.

Although the Risk Assessment Table embedded in the SR form poses the following question as #13, “What is the back-out strategy to reverse a change, *e.g.*, archive logs for database changes?” this table is rarely filled out and, when filled out, the answer to this question is typically “Yes,” but the back-out strategy itself is not attached, or included as verbiage in this form, or in this table. Back-out procedures should be required documentation for all SRs, including at a minimum, the answer(s) to the following questions: What is the back-out strategy should the proposed change fail; how will failure be determined and when will the determination to back out a change be made?

Management should develop and publish policies and procedures related to emergency fixes. Further, a process for tracking outstanding approvals and documentation for emergency fixes should be implemented and monitored on a regular basis.

8. No Inventory of Stored Procedures

The STARS system relies heavily on stored procedures for transactional processing. Stored procedures perform very basic operations, such as data transformation or calculations within the database tables. The BMV could not provide BKD with an inventory of STARS-stored procedures; though we were told by the former CIO that approximately 10,400 stored procedures exist. As changes are made to the database schema and system, consideration needs to be given to the impact on the existing stored procedures and calculations. Without a documented inventory, changes made to the database could result in an unintentional negative impact, such as data integrity issues, inaccurate calculations or incorrect reporting. All stored procedures used in the STARS system should be documented, by name, with a definition of the purpose(s) for each.

9. Lack of Standardization of Testing Documentation

Updates to the system are tested in a separate test environment prior to being migrated to the production environment. In reviewing the documentation from the December 2014 Build, we noted the BMV does not utilize a standard Test Matrix form. During BKD’s review of the 165 SRs comprising the December 2014 Build, we determined that:

- 3 of the 165 test matrices (1.8 percent) were filled out completely

- 79 of the 165 SRs, (47.8 percent) did not have a supporting Test Matrix form or one could not be supplied

- 143 of the test matrices, or 87 percent, were incompletely filled out in the Test Results and Comments fields

- 12 of the 165 (7 percent) test matrices could not be supplied to BKD in a timely manner; they were provided 20 days after our initial receipt of supporting documentation

To ensure consistency and rigor in testing procedures, each test matrix should document a detailed test plan, the expected results for each step, the actual results of testing and any comments regarding the effects of the change itself. A lack of consistency in test documentation creates a risk of nonconformity in applying the change management policies and procedures. The Build Committee should assess the anticipated impact of the change(s) documented in each SR, based on the embedded risk assessment in the form. The level and rigor of testing should be planned based on this assessment.

10. IT Project Management – Lacking a Go/No-Go Live Decision Checklist

The December 2014 Build project document for the BMV STARS system does not contain a Project Go/No-Go Decision Checklist. Going live into the BMV production environment without everything in place may result in:

- Unresolved defects
- Inadequate testing
- Insufficient training
- Business processes not understood
- Procedures not written
- Stakeholders missed
- Lack of communications
- Data migration failure
- Interfaces not working
- System administration and support not in place
- Inadequate system security
- Unclear responsibilities, accountabilities and ownership
- Inadequate implementation strategy
- System/application failure
- Impact to the business/organization
- Project/Build failure

In order to ensure adequate implementation planning, appropriate communication to all key stakeholders and sufficient due diligence has been performed, a Project Go/No-Go Checklist should be created for each semi-annual Build of the STARS system, covering, at a minimum, the following 12 areas of concern:

(1) Have the needs and concerns of all key stakeholders been considered and resolved?

(2) Does the Build have an overall approved mission statement defining the scope, schedule and resources/budget?

(3) Has the relative flexibility among scope, schedule, resources and budget been determined?

(4) Have all Build deliverables been identified and described in detail, with unambiguous completion criteria?

(5) Are all roles and responsibilities defined and agreed upon for all Build team members?

(6) Has an appropriately detailed work breakdown structure (WBS) been created with input from key team members?

(7) Has a credible schedule with identifiable critical path and late schedule been developed from the WBS and optimized within the project constraints?

(8) Have milestones been included in the schedule to track major events, completed phases and/or deliverables and external dependencies?

(9) Have workload commitments been identifiable for each week of the Build and agreed to by team members and their managers?

(10) Have response plans been developed for the most significant threats to the Build's success?

(11) Has a change management process been defined and agreed to by all key stakeholders?

(12) Has the governance structure for the Build been established with an agreed sponsorship role and expectations set for review frequency and format?

The Build Committee can use the Project Go/No-Go Decision Checklist to consider the bigger picture and include other factors, such as regulatory compliance and other external pressures; urgency to proceed; appetite for risk; consequences of delays, etc. If significant gaps are identified, it is usually better for all concerned to delay implementation until these gaps have been addressed/mitigated.

In the case of non-negotiable implementation dates, *i.e.*, a response to legislation changes that have to be in by a certain date, the gaps on the checklist should be prioritized and addressed in order of importance and ability to resolve. In this case, by going-live, the Build Committee would essentially be accepting the risks identified in the assessment, on the basis that meeting the implementation date is more important than mitigating the risks and having a smooth go-live. When applicable, this chain of events should be documented and included, as a caveat, in the Project Build document.

11. Overall Logical Access Security Processes and Controls Need Improvement

In order to understand, test and document the logical security access controls in the BMV operating environment, BKD conducted a series of interviews with the IOT manager responsible for providing security administration on the PeopleSoft and Active Directory platforms, and with the BMV ITD functioning as security administrators on the STARS application, the SQL platform, the data warehouse DSS, FORTIS and KOFAX document management tools.

IV. Observations and Recommendations

BKD determined the process of assigning, changing and removing employee access to the BMV logical system resources is accomplished as follows:

- The Human Resources (HR) department works with the IOT help desk to establish a PeopleSoft role description for all employees to track time and benefits.

- Direct supervisors access the BMV intranet (Main Street) site to fill out a Computer Access form for new hires, rehires, transfers, promotions and demotions. A separate Computer Access Removal Request form is filled out for terminated employees, including retirements.

- Direct supervisors notify the IOT help desk of employees' need for access to BMV system via an email, attaching either a Computer Access form or a Computer Access Removal Request form, as applicable.

- The IOT team initiates a help desk ticket in the VSM system to document all activity related to any changes requested.

BKD evaluated the logical access communication and documentation processes, as referenced above, for a three-year period (March 1, 2012 through March 1, 2015), with an overall sample of 30 percent of new hires, rehires, transfers, promotions, demotions, terminations and retirements. BKD was notified the sample would take several weeks to pull together, and resized the sample accordingly, in order to complete all testing to meet the report deadline.

During this period, the BMV hired or rehired 53 employees, and BKD requested a sample of 16, resized to 15. Transfers, promotions and demotions for this period totaled 167, and BKD requested a sample of 50, resized to 9. Terminations and retirements totaled 101 for the period under review, and BKD requested a sample of 30, resized to 23.

During this period, the BMVC (branches) hired or rehired 573 employees, and BKD requested a sample of 57, resized to 24. Transfers, promotions and demotions for this period totaled 737, and BKD requested a sample of 74, resized to 16. Terminations and retirements totaled 707 for the period under review, and BKD requested a sample of 71, resized to 24. The following exceptions to the communication and documentation processes were noted, for a total sample of 111:

- No email from supervisor requesting access was provided for 26 employees

- No Computer Access Request form or Computer Access Removal Request form was provided for 26 employees.

- Email provided by the manager was dated 14 days after employee was terminated for 1 employee.

- No Computer Access Removal form provided, indicating the need to temporarily disable accounts for leaves of absence for eight employees.

- Computer Access Removal form provided 14 days after employee was terminated (along with email request from manager) for one employee.

- Although employee's termination date was February 7, 2013, the Computer Access Removal form listed the effective date as February 7, 2016, and the Effective Time was listed as "immediately" for one employee.

- Although the employee was transferring from the BMV to the BMVC (branch), the Computer Access form provided did not indicate the last working day at the BMV for one employee.

- No VSM ticket was provided demonstrating that active directory network access was reviewed to determine whether the employee change required change/removal in active directory network access or shared directories/folders for 26 employees

- For one employee, the VSM ticket resolved after the start date specified on Email/ Computer Access Request form (for New Hire).

- For one employee, the VSM ticket was completed six days after employee was terminated (same day as vmware Call Report).

- For one employee, the VSM ticket was completed four days after the employee retired.

We recommend the HR department and the IOT help desk, in conjunction with the internal BMV security coordinators and BMV ITD security administrators, establish solid communication and documentation guidelines, procedures and appropriate Service Level Agreements (SLAs) to accurately and effectively handle all requests for access to and removal from the BMV logical security access resources. Additionally, we recommend that quarterly reviews of all employee access to all BMV logical security access resources be performed by the BMV ISO and his team to ensure that only valid current employees and contractors have access to these resources. Finally, due to the nature of their responsibilities, we recommend that all ITD terminated or retired employees should be removed from all BMV logical access resources, on the same day as their termination instead of the next day following their departure from the BMV.

12. SQL Logical Access Security Processes and Controls Need Improvement at Both Infrastructure and Database (or STARS Application) Levels

As noted earlier in this report, the core BMV STARS application is currently running on an SQL 2008 operating system. BKD reviewed the logical access security on the SQL platform on two distinct levels, infrastructure access (by the IOT support team and ITD security administrators) and at the database (or STARS application) level (by the ITD developers, database administrators and Q/A personnel).

Infrastructure Level:

The STARS production database is currently four TB (terabytes). The IOT runs a trace log nightly for the BMV ITD, which monitors the production servers and databases for the STARS SQL platform. The ITD also performs trace logs on their test servers supporting the STARS system. The trace log captures CPU reads and writes to ensure effective performance of all processes nightly.

The IOT notifies the ITD DBA of long-running query performance issues. IOT is currently piloting the McAfee Database Security Suite for Database, which may be used for all Indiana state agencies, including the BMV. We recommend the IOT database services team continues to research the functionality provided by the McAfee Datacenter Security Suite for Database tool, and determine whether it is feasible to use to monitor the BMV and its productions servers and databases for the STARS SQL platform.

At the infrastructure level, in order to ensure the SQL server platform environment is configured and activated to record and report security events, *e.g.*, security violation reports, unauthorized attempts to access information resources, BKD requested a listing of all SQL server folder permissions, on all servers supporting STARS, from the IOT.

After attempting to satisfy this request for nine days (from March 11, 2015 through March 20, 2015), the IOT server administrator team was unable to produce this listing, using the Security Explorer Version 8 (8.0.0.157) tool. We recommend the BMV ISO collaborate with the IOT ISO to formulate a strategy detailing, at a minimum: (1) the BMV's platforms supported by the IOT; (2) the IOT teams supporting those platforms; (3) the tool(s) required to provide effective information security monitoring controls over those platforms; (4) the report(s) available to demonstrate those controls are operating effectively; (5) detailed procedures documenting the handling of any exceptions noted during review of those reports; and (6) a schedule of how often those reports can be produced for review.

Periodic SQL server security reviews are performed on migration, but these reviews are not documented. Standard processes for the BMV SQL server security reviews, performed by the IOT, are not documented. There is a lack of IOT SQL server security review standards and documented reviews. We recommend the IOT ISO collaborate with the BMV ISO to determine how to establish and document appropriate review and monitoring controls over the BMV SQL server environment, which serves as the base operating system for the STARS application.

Database (or STARS application) Level:

In order to ensure that adequate monitoring is being performed on all critical STARS SQL databases, BKD requested the server/database/objects audits for December 2014, January 2015 and February 2015. The ITD DBA informed BKD that he does not perform server/database/objects audits on the SQL production environment. Best practices recommend that a SQL server security review be part of the DBA's regularly scheduled activity. We recommend that, for critical databases only, the following audits be performed monthly, at a minimum, completely or partially automated, using server-level DDL triggers, alerts, third-party tools, etc.: (1) Audit Add DB User Event; (2) Audit Add Role Event; (3) Audit Add Login to Server Role; (4) Audit Add Login Event; (5) Audit Add Member to DB Role; (6) Audit Application Role Change Password; (7) Audit Change Audit; (8) Audit Change Database Owner; (9) Audit Database Scope GDR; (10) Audit Database Operation; (11) Audit Database Object Management; (12) Audit Database Principal Impersonation; (13) Audit Database Principal

Management; (14) Audit Database Scope GDR; (15) Audit Login Change Password; (16) Audit Login Change Property; (17) Audit Login GDR Event; (18) Audit Object Derived Permission Event; (19) Audit Schema Object GDR; (20) Audit Schema Object Management; (21) Audit Schema Object Take Ownership; (22) Audit Server Alter Trace; (23) Audit Server Object GDR; (24) Audit Server Object Management; (25) Audit Server Object Take Ownership; (26) Audit Server Operation; (27) Audit Server Principal Impersonation; (28) Audit Server Principal Management; (29) Audit Server Scope GDR; (30) Audit Database Object Take Ownership.

In order to verify adequate monitoring controls exist over the SQL platform, BKD requested a copy of the most current documented review of all SQL database users, and the ITD DBA provided a spreadsheet, which he had documented a few years ago (2012/2013). Best practices recommend that information security tools over the new and modified application systems, data structures, network and communication software, and systems software be configured and activated to record and report security events, *e.g.*, security violation, unauthorized access attempts, as defined in information security policies; reports generated should be regularly reviewed and necessary action taken during the configuration process.

We recommend the ISO collaborate with both the ITD database manager and the data warehouse DSS manager to devise appropriate, automated, effective reviews of all SQL database platform users in the ITD and Q/A areas. Monitoring controls, and the testing and verification of the appropriateness of these controls, should be coordinated with the internal audit department, in order to ensure an independent review of all access is performed and documented.

Best practices recommends that roles and responsibilities related to administrative access to new and modified application systems, data structures, network and communication software, and systems software (users with the ability to make modifications to overall system security parameters, security roles or security configuration) should be limited to appropriate personnel. During a review of all users and processes named to the following fixed database roles: db-owner, db-securityadmin, db-accessadmin, db-backupoperator, db-ddladmin, db-datareader, db-denydatareader, and db-denydatawriter, BKD determined that an excessive number (seven) of the users have db-datawriter access to the production database for the STARS application, which means these users could modify the data in the Master Fee Table.

Numbered among these users are the CIO and an application development senior, both of whom also function as security administrators for the SQL platform. We recommend that management review and document the business need(s) for so many ITD employees, at so many varying levels of expertise and responsibility, to have access to modify the data in the Master Fee Table, as well as all other SQL tables utilized in the production STARS application environment.

Stored procedures allow modular programming, meaning they are created once, precompiled, stored in a database, then called several times during processing, enabling faster execution than SQL queries. In order to verify that permission to execute all stored procedures, views and functions is restricted only to those employees who require this access in order to perform their assigned job duties, BKD requested a listing of all permissions via the SQL GRANT statement, from the CIO and the ITD DBA, and determined five employees have been granted permission to all stored procedures, views and functions, via their db_executeall DBRole and the application-level STARS_data_access role. These five employees include the CIO, the deputy director/IT project manager, the application system administrator/program manager, the application system administrator/program supervisor, an application developer-senior, and an additional IT project manager. Additionally, BKD determined that one terminated employee, a former application systems analyst/program supervisor, still has access to the user acceptance testing environment of the SQL platform. Best practices recommend this level of access be appropriately restricted to those employees requiring this permission to perform their job duties.

We recommend the CIO, the deputy director/IT project manager and any other IT project managers be removed from the list of employees with db_executeall and STARS_data_access roles, in order to provide adequate segregation of duties between those employees who perform development activities and levels of management who review work performed by those employees performing development activities. We also recommend that semi-annual reviews of all employee access to the SQL platform be performed by an independent party, for all three environments, *e.g.*, production, development and user acceptance testing.

In order to verify that access to the SQL platform logical resources is appropriately controlled, BKD requested documentation of all account creation, changes, and terminations/deletions, from March 1, 2012 through March 1, 2015, for all SQL-related databases, applications, tools, etc., from the CIO and the ITD DBA. Documentation was not provided; however, the DBA stated that, "Access is requested by email from supervisor or individual (with supervisor as cc), requesting access to the database environment (dev, qa, parallel)." The process of requesting, approving and assigning logical access to the BMV environment was tested during the review; however, the Computer Access Request and Computer Access Removal Request forms, sent by supervisors via email, do not specify requested access to the SQL platform environment. Best practices recommends that all access requests for all users of all platforms, applications, databases, tools, etc., be specifically documented for all users, in particular developers, programmers, Q/A analysts, etc., in an environment in which development activities are performed. We recommend a form be designed for all IT employees, Q/A employees and contractors with access to the SQL platform, applications, databases, tools, etc., requesting additions, changes and removal of all access. This access should be reviewed by an independent individual, *e.g.*, the ISO, the internal audit department, semi-annually, at a minimum, to determine that all employees and contractors retain the minimum access required to perform their assigned duties.

13. <u>STARS Logical Access Security Processes and Controls Need Improvement</u>

BKD reviewed a listing of all access to the STARS system, as of March 17, 2015, and determined that 1,577 individuals have access to the production STARS environment, of which 111 individuals are employees of other state agencies.

BKD performed a comparison of the 1,466 BMV and BMVC employees to a listing of active employees from 2012 through 2015. We identified the following:

- 27 terminated employees (1.8 percent) were identified as still active.
- 13 individuals (.08 percent) could not be identified as BMV or BMVC employees. They could be active employees, either hired after March 1, 2015, from another state agency, or a contractor. They could be active employees either hired after March 1, 2015, from another state agency or a contractor.

BKD could not determine, from the documentation provided, whether or not the employees listed were assigned appropriate or inappropriate access levels on the STARS system. We recommend that STARS role template descriptions be documented, detailed down to the field level, all data in all menu options, queries, screens, tables and rows.

Additionally, we recommend the BMV ISO and his team coordinate a quarterly review of all employees with access to the STARS system, with all business unit management. Each business unit management should be presented with listings of all direct reports and access level descriptions and be required to return confirmation of that access, or required changes to that access. Eventually, the internal audit department should be required to validate performance of the review and coordinate all changes with the ISO. Finally, all external individuals with access to the STARS application platform should be subject to quarterly access reviews, to verify that their access to the core BMV system is still required.

14. PeopleSoft Logical Access Security Processes and Controls Need Improvement

IOT is responsible for provisioning access to PeopleSoft. Through inquiry with IOT personnel, BKD determined that a gap in communication exists regarding BMV employee transfers, demotions and promotions, which may impact the employee's assigned role description (logical access) level(s) on the PeopleSoft platform.

BKD requested a sample listing of current PeopleSoft roles for BMV and BMVC employees (as of March 25, 2015). BKD received a listing that contained 192 employees, which we compared to a listing of current employees (as of March 1, 2015). The following exceptions were noted:

- Six terminated employees were listed as current employees in PeopleSoft Role Descriptions maintained by the IOT
- BKD could not identify 13 employees listed on PeopleSoft Role Descriptions report (March 25, 2015) as an employee (from March 1, 2012 – March 1, 2015)

We recommend the HR department coordinate all requests for employee access with the IOT help desk, including name changes, all transfers, demotions and promotions. We further recommend the BMV HR department institute a process of notifying the IOT manager, applications (PeopleSoft) of all employee transfers, demotions and promotions, in order to ensure the PeopleSoft application access provided to BMV employees is justified in light of each employee's location and position responsibilities.

15. <u>FORTIS and KOFAX Logical Access Security Processes and Controls Need Improvement</u>

BKD discussed the security administration controls over the FORTIS and KOFAX systems with ITD and IOT team members and determined that access to the FORTIS document management system is requested by managers via email. These BMV and BMVC managers' email addresses are maintained on an email distribution listing for the FORTIS system, which BKD requested and compared with a listing of employees from March 1, 2012 through March 1, 2015.

- Of the 33 users listed, 1 user was terminated in 2013, and 1 user retired in August 2014, but both users were still recorded as being a valid email address to request FORTIS system add/change/remove access.

We recommend the FORTIS document management system be reviewed quarterly, by the ISO and his team, to determine if those email addresses listed as valid still belong to active employees who should be allowed to request logical access to BMV systems.

16. <u>Segregation of Duties Monitoring</u>

Subsection 5.2 of the BMVC Information Security Policy addresses Segregation of Duties controls and requires that:

> *"The area supervisor or designated account manager must review, on a 2-year cycle basis, the access privileges granted to all their assigned staff and/or system accounts that they manage."*

The ISO is responsible for overseeing and coordinating this review process. BKD requested evidence of the review for validation purposes. No evidence of the ISP's directive for a cycled two-year business unit management review of all staff and system accounts could be produced for review by BKD, on the following:

- Windows/Active Directory network, SQL, STARS, PeopleSoft or data warehouse DSS platforms

In order to ensure user access rights are restricted appropriately, representing an adequate segregation of duties, the BMV's user provisioning processes on all platforms should be aligned with the controls stated in subsection 5.2 of the current BMVC ISP. Best practice suggests that period reviews should be performed ***quarterly*** to review current employees' access rights, contractor rights and external agency rights. If the frequency is modified, the ISP should be updated to reflect the change.

17. Master Fee Table – Lack of Monitoring Access and Changes for Appropriateness

BKD determined that a number of people, including the former CIO, had access to edit values on the Master Fee Table. Because the data contained on the Master Fee Table is the basis for transactional process, access should be very limited to only a few individuals. BKD could not obtain a Master Fee Table File Maintenance report, demonstrating the logging of additions/deletions/revisions of all BMV fees. Without the logging of these events, BMV management cannot actively monitor changes for appropriateness.

A Master Fee Table File Maintenance report should be created and implemented for the STARS system. An independent review of the File Maintenance Report should also be implemented and monitored frequently. The independent reviewer should ensure that all changes reflected on the system are supported by approved SRs.

Further, monitoring controls should be developed, documented and implemented for reviews of the ITD-developed queries and/or reporting detailing Master Fee Table parameter changes, security events, user changes and significant system modifications. Without these controls in place, unauthorized access and changes could occur and go undetected.

18. Lack of Data Dictionary or Metadata Management

The BMV core STARS system is written in Visual Basic (VB), using SQL tables and queries, and a data warehouse DSS is refreshed daily. Thousands of tables, accessing untold volumes of metadata, comprise the STARS system and 40 tables utilize the Master Fee Table fields. In order to facilitate development, database structures and produce accurate queries, an understanding of those fields that are used in all transactions must be clearly defined, using a data dictionary. In structured programming and metadata management practices, a data dictionary is built in the initial Build processes for a VB system, maintained and revised in conjunction with successive Builds, queries and hotfixes.

The ITD data warehouse DSS manager provided the data warehouse DSS data dictionary, which comprises a listing of specific query reports, described to the field level, of output. The data warehouse DSS data dictionary does not comprise a standard data dictionary, which should contain detailed transaction-level processing descriptions of all core STARS system data, referencing all databases, tables, rows and data fields.

We recommend that executive management perform an analysis of the data warehouse DSS, to determine whether it should be re-architected internally, outsourced, or whether an automated third-party solution should be purchased and implemented. The design and implementation of the following automated controls should be considered as a component of this analysis: (1) reconcile and validate information before it enters the data warehouse DSS; (2) validate information before, during, and after Extract, Translate and Load (ETL) processes and customer feeder programs; (3) verify and reconcile sources to warehouse, data marts to warehouse, data marts to sources, etc.; (4) non-intrusively validate information in the data warehouse DSS against other external information—even if a source is unrelated to the data warehouse DSS or several steps removed from the warehouse; (5) ensure that information is not lost or erroneously duplicated; (6) reconcile report contents against the warehouse; (7) perform reasonableness tests to detect potential problems; and (8) compute statistical tests to feed other controls or determine if expected thresholds are exceeded.

19. Feasibility Study – STARS Lifecycle Management

During the course of our assessment, BKD determined the STARS system, designed in VB on a SQL 2008 platform, is largely undocumented, with semi-annual Builds encompassing regulatory updates, user-defined development requirements and hotfixes to patch processing errors encountered during use. Communications and documentation between various business units were evaluated and determined to be largely unstructured, ill-timed and subject to poor change management practices and poor logical access controls. Further, STARS SQL 2008 r2 servers are no longer eligible for mainstream support.

Through inquiry and performance of operational walk-throughs, BKD noted the current system configuration often does not align with the needs of business users in meeting their objectives: standardized and consistent processing, application controls to ensure data integrity and processing accuracy. We observed numerous instances where processing is manually intensive and often requires workarounds to complete a transaction.

Given all of the identified weaknesses, BKD recommends performance of a comprehensive analysis to determine if STARS is the appropriate solution going forward. The BMV should assess the cost/benefit of upgrading the STARS application to a vendor-supported SQL platform and document the system accurately and effectively, as noted in several recommendations in this report, or to consider migrating the current VB application to a more efficient, effective, third-party, fully documented application, on a vendor-supported platform.

The proposed feasibility study should clearly define the boundaries of systems development or purchased software implementation, and provide supporting cost/benefit analysis to justify the decision, as well as to provide a strategic plan indicating how the development should be completed. At a minimum, the feasibility study should include the following elements: (1) evaluate the current STARS system, all automated and manual controls; (2) define critical success factors; (3) evaluate systems development options; (4) define costs and benefits of most suitable options; and (5) recommend suitable alternative systems, vendors and internal restructuring options. Information systems should add measureable value to business operations and adequately support business processes.

20. Network Architectural Diagrams

KD reviewed Service Request #1377 (Create Visio of our Server Environment [STARS, MT, IKON]), included in the December 2014 Build. Many of the 11 flowcharts and technical specification documents have been created by MorphoTrust USA, an external service provider, who partners with many state and federal agencies. MorphoTrust USA provides front and back office identity solutions and services to state motor vehicle agencies, including the BMV.

The following documentation components do not contain version controls: (1) BMV STARS system; (2) DMS servers and process flow for Q/A; (3) Intellectual Technologies Incorporated Indiana DR Topology; (4) Morpho Trust Auto-Test BMV Solution Architecture SOW; (5) Morpho Trust Auto-Test BMV HW Solution Architecture; (6) Morpho Trust Auto-Test Distributed Architecture Funct Spec; (7) Morpho Trust Auto-Test Workflow Funct Spec; (8) Morpho Trust DDL Servers Visio; (9) MT DDL Servers Visio v092413; and (10) Ricoh Document Management System servers and process flow. One of the documents, IN CIPF Upgrade Network Architecture Document v.1.06, is dated November 10, 2012, and may be very outdated.

We recommend that management contact all external vendors who supply architectural documentation supporting their provided services, to determine if current flowcharts and technical specifications can be obtained. All documentation provided by third-party service providers should be reviewed by the Build Committee, with the assistance of IOT team members with expertise in network architectural documentation, to ensure its quality and validity. Any internally-developed network and/or STARS core application diagrams should also be subjected to the same level of review and approval processes. Finally, in compliance with best practices guidelines, all system and network documentation should contain versioning information embedded in the document itself. This versioning information should include, but not be limited to, the following: date of creation; most recent revision date; approval date of revisions; committee/individual name/initials of approver(s).

21. <u>Data Flow Diagram</u>

BKD determined, during several interviews with the former CIO, his deputy director, application development managers, the DBA and Q/A team members, the STARS application has thousands of undocumented tables, and over 40 of these tables handle fee calculations. The Master Fee Table drives the fee calculations, and the DBA stated that no other databases feed into the Master Fee Table.

Although requested at various points during the review, BKD was unable to obtain any application diagrams or data flow diagrams, to support the DBA's statements. To help overcome the communication challenges between developers, Q/A team members, and users, data flow diagrams serve as working documents to record an understanding of needs requirements and serve as the base for the core system structure. We recommend that management create data flow diagrams for the STARS application, documenting, at a minimum: (1) procedures/ processes with supporting logic specifications; (2) data at rest; (3) data in motion; (4) outside sources and sinks of data flow; (5) events triggering processes; and (6) rules for processing sequences.

22. Lack of Third-Party Vendor Inventory

In lieu of an application diagram, BKD requested an inventory of the third-party vendors who access the STARS or FORTIS systems, provided any form of input to STARS or FORTIS processing cycles, and/or who are the recipients of any output from either the STARS or FORTIS systems. While not readily accessible, the BMV team provided BKD with a listing of 47 vendors.

In our attempt to validate the completeness and accuracy of the listing, it was determined that a number of the 47 vendors listed no longer interface with the BMV STARS or FORTIS systems. Because we could not confirm the validity of the third-party vendor inventory, BKD could not test the existence and effectiveness of the following controls:

- Whether the selection of vendors for outsourced services is performed in accordance with the BMV's vendor management policy

- Whether the criteria and business case used for selection of third-party service providers includes: consideration of the third-party's financial stability; skill and knowledge of the systems under management; controls over security and availability and processing integrity

- Whether third-party service contracts include controls to support security, availability and processing integrity, in accordance with the BMV's policies and procedures

- Whether third-party service contracts include: definition of services to be performed; responsibilities for the controls over supported systems have been defined; third party's acceptable compliance with the BMV's security policies and procedures; contracts were reviewed and signed by appropriate parties before work commenced; controls over supported systems and subsystems, described in the contract, agree with those required by the BMV

- Whether third-party service providers perform independent reviews of security, availability and processing integrity (*e.g.*, service auditor reports (SOC1, SOC2, etc.).

Without a current and comprehensive listing, the BMV cannot adequately monitor or control the information shared with third parties. We recommend that a definitive listing of all current third parties accessing the BMV system resources be compiled, and the method(s) of access, *e.g.*, web interface, VPN, manual, be documented, maintained and monitored. The types of data shared with each vendor should be documented and managed accordingly based upon level of risk.

23. Lack of Interface Inventory and Diagrams (internal and external)

The STARS system interfaces with a number of governmental agencies (*e.g.*, the governor; the secretary of state [dealers services]; the Department of Revenue [commercial]; the Department of Natural Resources [watercraft]; the State Board of Accounts [review/audit]; the State Budget Agency [budgeting]; the Auditor of State [payments/funds]; the Treasurer of State investments); external entities *(i.e.*, the Department of Motor Vehicles [DMV.com]); Indiana counties; and internal departmental teams *(i.e.*, the Indiana Office of Technology [IOT]).

Application interface diagrams demonstrating the extent of input to the STARS and ancillary feeder_systems, *e.g*. FORTIS, KOFAX, PeopleSoft, and output from the STARS system and feeder systems (*e.g*., FORTIS, KOFAX, PeopleSoft), do not exist. Without this documentation, BMV management cannot adequately manage interfaces and the associate risks in a controlled manner.

System documentation should be developed and maintained, to be published internally along with the semi-annual Build.

V. Appendix

Appendix A

Internal Control Component	**Principles**
Control environment	1. Demonstrate commitment to integrity and ethical values 2. Ensure that board exercises oversight responsibility 3. Establish structures, reporting lines, authorities and responsibilities 4. Demonstrate commitment to a competent workforce 5. Hold people accountable
Risk assessment	6. Specify appropriate objectives 7. Identify and analyze risks 8. Evaluate fraud risks 9. Identify and analyze changes that could significantly affect internal controls
Control activities	10. Select and develop control activities that mitigate risks 11. Select and develop technology controls 12. Deploy control activities through policies and procedures
Information and communication	13. Use relevant, quality information to support the internal control function 14. Communicate internal control information internally 15. Communicate internal control information externally
Monitoring	16. Perform ongoing or periodic evaluations of internal controls (or a combination of the two) 17. Communicate internal control deficiencies

V. Appendix

Below is a listing of corrective actions implemented by BMV management during the course of our assessment. BKD has not performed validation procedures on the design or operational effectiveness.

- Created overcharge and undercharge survey
  - Any BMVC employee may report knowledge of an overcharge or undercharge to management, effective **October 2014**
  - These survey entries are reviewed by the business areas and SRs are entered to correct system issues and/or create refunds
  - Seven requests for refunds from the Overcharge/Undercharge Survey have been completed to date, **February 2015**
  - An additional 16 requests for refunds from the Overcharge/Undercharge Survey have been prioritized and are being worked for the June Build, **June 2015**
- Creation of Build committee, **January 2015**
  - Committee consists of executive management in areas of operations, legal, finance and information technology
  - Committee approves/denies requests for a particular Build after deadline
  - Committee approves/denies requests with Master Fee Table changes within STARS
- Hotfixed a number of fee and tax issues in December and January
- Retained Barnes & Thornburg to assist with legal review related to fees and taxes interpretations
- Started procedure that requires BMV legal department to review Main Street communications before posted
- Locked down Master Fee Code Table, **March 2015**
  - One person, IT Director, has access through STARS system
  - Nine people, IT system administrators, have access through SQL
- Identified 159 Service Requests to make system processes in compliance with law, **October 2014**
  - Completed five compliance requests from December 2014 through today, **April 2015**

  - Working 108 compliance requests for June Build, **June 2015**
  - Will continue to work remaining 46 compliance requests for December Build, **December 2015**

- Additional fields have been added to the build documentation template to facilitate work outside IT, **March 2015.** Examples include:
  - Communication—Who needs to know about this system change?
  - Form updates—Which forms need to be updated due to this system change?
  - Notices—Which notices need to be updated due to this system change?
  - SOP/Policies—Which SOP/policies need to be updated due to this system change?
  - Vendors—Which vendors have responsibilities in this system change?
- Creation of, or significant updates to, several manuals used throughout agency
  - Revised Title Manual – 5/2013
  - Revised Registration Manual – 7/2013
  - Creation of Sport & Leisure Manual (Replaced Watercraft Manual) – 8/2013
  - Revised Credential Manual – 12/2014 and 4/2015
  - Creation of Finance Manual – 1/2015
- Several smaller reorganizations within the agency reassigning some departmental duties in an effort to align departments with agency core functions – 1/2015
- Upgraded VIN validation software – project began 1/2015
  - MDCs – 1/2015
  - Passenger vehicles, trucks and MCs – 6/2015
  - Trailers and RVs – TBD
- Significant reorganization of records management department – 1/2014
  - Replaced entire management and supervisory staff
  - Reduced large document backlogs through creation of metrics and department procedures

    - Focused on relationship repair with external stakeholders
    - Began documentation of daily processes
- Various rules promulgated for driver education, commercial and driver training schools – 12/2014

BKD LLP
CPAs & Advisors

201 N. Illinois Street, Suite 700 // P.O. Box 44998 // Indianapolis, IN 46244-0998
317.383.4000 // fax 317.383.4200 // bkd.com

Consultant's Report

Mr. Kent W. Abernathy, Commissioner
Indiana Bureau of Motor Vehicles
100 North Senate Avenue, N400
Indianapolis, IN 46204

We are pleased to provide our report on the Indiana Bureau of Motor Vehicles (BMV) operations performed by **BKD, LLP** (BKD). We want to thank the BMV's management and staff members who contributed positively to our efforts.

We have performed the procedures enumerated in Section III of this report, which were agreed to by you pursuant to our engagement letter, dated February 13, 2015, to review and provide recommendations for improving BMV's internal controls associated with transactional processing of fees and taxes. This engagement was an assessment and was not designed to provide assurance over the prevention or discovery of errors, misrepresentations, fraud or illegal acts. Inherent limitations in any internal control structure are that errors, fraud, illegal acts or instances of noncompliance may occur and not be detected. Controls may become inadequate because of changes in conditions or deterioration in design or operation. Two or more people may also circumvent controls or management may override the system.

We were not engaged to provide an opinion with respect to the effectiveness of your controls or degree of compliance with your policies and procedures or applicable laws and/or regulations. Accordingly, we do not express such an opinion. The majority of our procedures were performed on an inquiry basis with limited testing conducted and cannot be relied upon to detect all errors or violations of laws, regulations or internal policy. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

Our report is intended for use only by management of the BMV solely for reporting findings with respect to the procedures performed by us. This report is not intended to be, and should not be, used by anyone other than the specified parties.

BKD, LLP

BKD, LLP

May 11, 2015