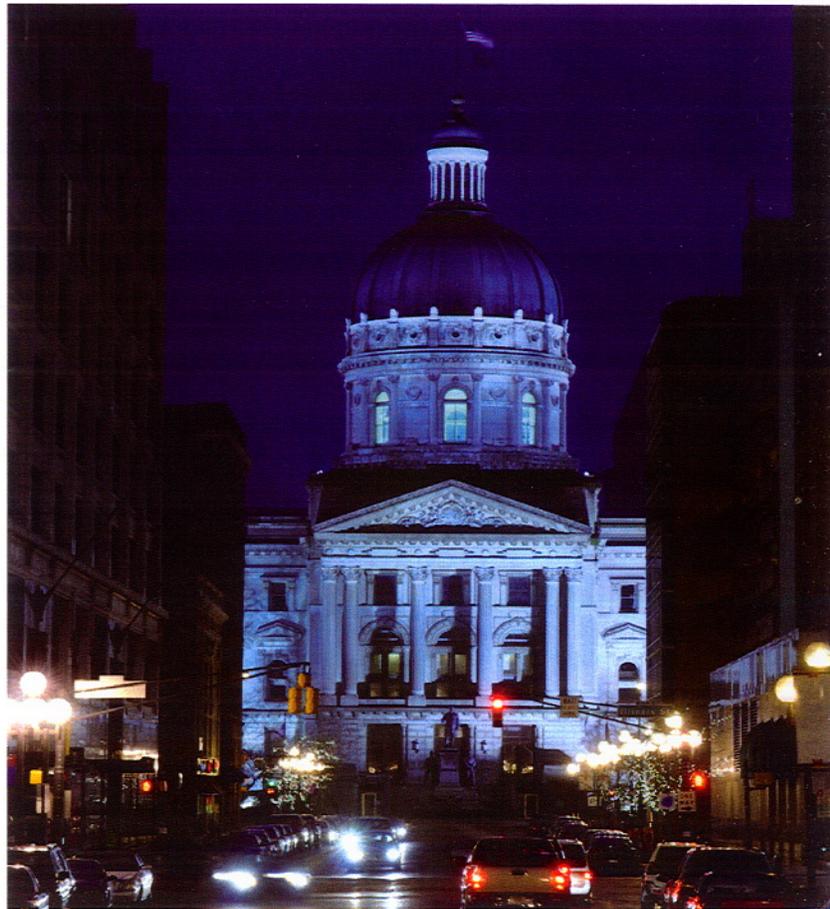




Indiana Office of Management & Budget



**Financial Operations Risk Assessment of the
Indiana Department of Revenue**

August 2012

This report is intended solely for the information and use of OMB, DOR and the State Budget Committee and is not intended to be, and should not be, used by any other party, with the exception of oversight agencies for the performance of their oversight responsibilities.

August 31, 2012

Mr. Adam Horst
Director
Office of Management & Budget
200 West Washington Street, Room 212
Indianapolis, IN 46204

Dear Director Horst:

Deloitte & Touche LLP (“Deloitte & Touche”) has completed the financial operations risk assessment of the Indiana Department of Revenue’s (“DOR” or the “Organization”) information technology (“IT”) and financial operations. The purpose of this report is to communicate the results of the risk assessment, which includes a summarization of the key risks identified within DOR and recommendations for the areas upon which the controls and performance audit of the Organization should be focused.

In accordance with the June 21, 2012 services agreement between the Indiana Office of Management & Budget (“OMB”) and Deloitte & Touche, an understanding of DOR’s key business processes was gained, which was used to establish the controls and performance audit universe to be considered for the controls and performance audit; a risk model was developed, which helped to identify current risks facing DOR; and subsequently identified risks were assessed and prioritized areas were included in the proposed controls and performance audit plan included in this report.

Our services were performed in accordance with the Statement on Standards for Consulting Services issued by the American Institute of Certified Public Accountants (AICPA).

This report is intended solely for the information and use of OMB, DOR and the State Budget Committee and is not intended to be, and should not be, used by any other party, with the exception of oversight agencies for the performance of their oversight responsibilities.

We appreciate the cooperation received from management and staff of OMB and DOR during the performance of the risk assessment phase of our services.

Yours truly,



Partner
Deloitte & Touche LLP

Contents

Background	1
Executive Summary	3
The Importance of Risk Management	3
Overview of Procedures Performed	3
Common Risk Themes	4
Summary of Proposed Controls and Performance Audit Plan Areas.....	6
Scope and Methodology	8
Financial Operations Risk Assessment.....	8
Stage I: Understand DOR's key business processes.....	8
Stage II: Develop the risk model.....	8
Stage III: Assess and prioritize risks.....	9
Stages IV: Develop a draft risk-based controls and performance audit plan	10
Professional Standards	10
Controls and Performance Audit Universe.....	11
Risk Assessment Results.....	12
Process-Level Risk Map.....	12
Operational-Level Risk Map	13
Infrastructure-Level Risk Map.....	14
Key Business Process Risks.....	15
Operational Business Process Risks	15
Infrastructure Business Process Risks.....	20
Controls and Performance Audit Plan.....	24
Areas to Be Audited.....	24
Controls and Performance Audit Approach.....	25
Controls and Performance Audit Timeline.....	27

Background

In May 2012, the Indiana Office of Management & Budget (“OMB”) issued a Request for Information (“RFI”) soliciting proposals for an independent risk assessment and internal controls and performance audit of the Indiana Department of Revenue (“DOR”). The RFI was in response to concerns that arose over the Organization’s information technology (IT) systems and financial operations after two large financial errors were identified.

DOR is the state organization that collects and accounts for the majority of general fund tax revenues for the State of Indiana (the “State”). DOR is responsible for assessing and collecting the taxes and transferring them into their proper funds so that they may be utilized by the State and, when required, local governments as prescribed by statute. It is also responsible for managing taxpayer accounts and for generating the reports that are utilized to distribute certain local revenues, such as local option income taxes (“LOITs”), food and beverage, auto rental, professional sports development areas, etc., back to local governments.

DOR has enjoyed a reputation as an organization that was focused on its customer, the Indiana taxpayer. In recent years, they undertook efforts to streamline most of the operational areas, which resulted in more efficient returns processing and an enhanced taxpayer experience. Since 2008, DOR has significantly reduced the time frame for processing paper returns while also cutting the cost per return for processing. Conversely, support areas such as information systems management and financial accounting and reporting appear to have been a lower priority without the same degree of focus, and as such, the control environment and importance of financial and IT controls may not have been as rigorous in detecting errors within the financial accounting systems. A comprehensive set of policies, procedures, and system documentation governing these areas does not appear to have existed, and there was a concern that staff turnover resulted in some control processes no longer being performed. Additionally, there was some concern that information systems may not be producing complete and accurate information to support the Organization.

Within the past year, DOR suffered two significant errors regarding corporate tax and LOIT distributions. Specifically, DOR discovered that \$320M of corporate tax e-file payments were not transferred from a holding account, thereby overstating the account balance of one account while understating the balance of another. Additionally, DOR identified that \$206M in LOITs were not distributed to local governments because new legislative rules were not thoroughly tested within the system and the allocation method for the funds was not correctly updated. DOR has acknowledged these errors and is taking proactive measures to reclaim the trust of the taxpayers and the legislature.

As a result of DOR’s challenges, a new Revenue Commissioner and Chief Financial Officer were brought on board in May 2012, soon followed by a new Chief Information Officer and two Deputy Controllers. Additionally, some supervisory and management staff have also turned over, with new individuals being placed into those positions. The new management team is focused on evaluating and correcting the identified errors while identifying other risks requiring remediation.

OMB issued the above-mentioned RFI to obtain an independent and objective risk assessment and conduct a controls and performance audit of DOR to review the circumstances and corrective actions of the identified errors and aid in identification of additional risks and concerns that may exist in DOR. OMB stated in the RFI its expectation that the final controls and performance audit report will also provide recommendations for improving IT and financial controls and other recommendations deemed appropriate to include replacement of IT system(s), organizational/structural changes, legislative changes, etc.

Deloitte & Touche was contracted on June 21, 2012, to perform the requested services. The results of the risk assessment and the proposed areas upon which the controls and performance audit of DOR should be focused are presented within this report.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Executive Summary

The Importance of Risk Management

Elements of risk are found within every organization, including government organizations, and, therefore, an organization should calculate its risks and understand that risk management needs to be built into the core infrastructure of the organization. Risk is broadly defined as “what can go wrong.” It is the possibility of an event occurring that will have an impact on the achievement of objectives. “Risk” is not synonymous with “problem,” and the risks that are identified in this report are a combination of risks that exist at DOR and risks that are inherent in state revenue agencies. These inherent risks may or may not cause loss exposure to DOR and are not a statement that a problem exists.

To maintain alignment between risk exposures and organizational objectives, a risk intelligent organization draws on the coordinated efforts of three levels of risk management responsibility:

- Risk governance, including strategic decision-making and risk oversight, led by executive management
- Risk infrastructure and management, including designing, implementing, and maintaining an effective risk management program, led by executive management
- Risk ownership, including identifying, measuring, monitoring, and reporting on specific risks, led by the business areas

The more clearly an organization can state its mission and priorities, as well as understand its strengths and capabilities, the more directly it can navigate to identify key risk areas to develop mitigation plans. Recent events, including the distribution errors, have placed DOR in a unique position to evaluate its strategies, key business processes, supporting technology, people, and their related elements of risks.

Overview of Procedures Performed

Deloitte & Touche began the risk assessment at DOR by gaining an understanding of DOR’s key business processes through interviews with key DOR personnel and review of relevant policies, procedures, and business process-related documentation. Key personnel from other organizations who work with or depend upon DOR’s support to accomplish their mission were also interviewed. The information was used to develop a pictorial map of DOR’s key business processes, which were categorized as follows:

- Operational processes, which are those related to DOR’s key mission of collecting and accounting for taxes (returns processing, collections, enforcement, taxpayer advocacy, etc.)
- Infrastructure processes, which are those that relate to the support and management of DOR (information systems, financial reporting, human resources, etc.)

Each process was broken down into the various subprocesses or activities that naturally occur within the process. This collection of processes and subprocesses established the controls and

performance audit universe from which the risk assessment could be performed. (See page 12 for details about DOR's controls and performance audit universe.)

Once an understanding of DOR's key business processes was gained, Deloitte & Touche then identified DOR-specific risks that were collected through the interviews and combined those with the inherent risks that are pervasive within revenue agencies and similar governmental organizations. For each subprocess, Deloitte & Touche established a ranking of the vulnerability of DOR to the various risks within the subprocess and the significance of the impact the risk could have on the Organization. An overall ranking of high, medium, or low risk was then assessed for each subprocess. These risk rankings were then captured on the controls and performance audit universe by color-coding each subprocess with its overall risk score. High-risk subprocesses were color-coded red, medium-risk subprocesses color-coded yellow, and low-risk subprocesses color-coded green; these risks were then captured on the controls and performance audit universe. (See page 12 for details about DOR's controls and performance audit universe.)

Utilizing the risk-ranked controls and performance audit universe, a proposed controls and performance audit plan was developed that focused more attention on the areas of high to medium risk within the Organization. As such, areas with high to medium risk will be included in the controls and performance audit plan for testing and review. Areas with predominately low risk will be included in the controls and performance audit plan but will receive a lower level of review than the higher-risk areas. DOR leadership has begun to implement mitigation plans for certain risks that have been identified and these plans will be reviewed as part of the controls and performance audit.

Common Risk Themes

The controls and performance audit universe identified above consists of 18 key business processes and 140 individual subprocesses that drive the daily operations of DOR. Both DOR specific and inherent risks were identified for each process, and its corresponding subprocesses, and are articulated more fully in the Key Business Process Risks section of this report. As a result of the risk assessment procedures performed, several general risk themes became apparent. These themes generally relate to one of the following fundamental questions:

- Does the Organization have the right **strategy** and **governance** mechanisms in place to achieve its mission?
- Does the Organization have the right **processes** and **technologies** in place to support its strategies?
- Does the Organization have the right **people** in place to execute the processes and technologies in accordance with the Organization's expectations?

Specific observations related to each of these areas are as follows:

- **Strategy/Governance** — DOR's strategy has been heavily focused on its customer, the Indiana taxpayer, and many of the initiatives undertaken by DOR focused on streamlining tax operations to result in more efficient returns processing and an enhanced taxpayer experience. Much success appears to have been achieved in this area, as DOR's front-end processing area could be considered leading national practice based on the reduced time and cost required to transfer paper returns into electronic format and the quality with which returns are prepared for tax administration processing. With that being said, support areas do not appear to have been emphasized to the same degree and, as such, the following observations are noted:
 - There may be a lack of recognition of the importance of a strong system of governance and internal controls

- There may be a lack of a risk identification process and mitigation of those risks
 - There may be a lack of understanding, responsibility, or appreciation for the key accounts DOR is responsible for in the Auditor of State’s chart of accounts
 - There may be a lack of awareness of the importance behind producing accurate and complete information that can be relied upon by other State agencies
 - There may be a lack of an overall governing strategy that guides the Organization to achieve its goals
 - There may be a lack of business analysts or experienced personnel who are responsible for understanding operating procedures by tax type, including analyzing, trending, forecasting, and reporting on the revenue
- **Process** — There does not appear to be a comprehensive set of documented processes in place to adequately guide the day-to-day operations of the Organization. DOR processes may not be well defined and may lack internal controls; as a result, errors may occur and go undetected if the following issues are not addressed:
 - A robust repository of process documentation, including policies and procedures, may not be clearly defined and utilized for consistency within the Organization
 - As a result of turnover, it is unclear whether key activities within the processes are being performed or that they are being applied consistently
 - Many processes are manual and may require duplicative and intensive data entry
 - Reconciliations may not be consistently performed by staff and reviewed by management
 - Analytics to review balances and identify trends in data may not be performed
 - **Technology** — DOR’s strategy, mission, and direction related to IT systems may not be clearly defined to meet the current and future needs of the business and aligned with the strategy of the Organization. Below are key risk areas associated with IT for DOR that need to be further examined:
 - There may be a lack of an IT governance model, including an IT strategy that is aligned with business needs and leadership priorities
 - There may be a lack of defined key technology processes, such as, the system development life cycle (SDLC) process, the change control process, IT policies, system documentation, and technology procedures
 - The technologies for many key business applications appear to be outdated and inflexible
 - There may not be an effective disaster recovery and business continuity plan for key DOR business applications
 - Core systems may not support automated interfaces, which can cause manual entry or data summarization errors and limit the ability to reconcile accounts and age collections, distributions, and payments by tax type
 - System and data audit logging, monitoring for changes, and maintaining system history for tax-processing information may not be occurring
 - Application and data security access to the system and sensitive information may not be properly secured or monitored according to business and compliance requirements

- The Organization may not have personnel or business analysts who are knowledgeable in both IT and business processes necessary to develop business requirements to correspond with IT changes
- **People** — DOR may not have a sufficient resource strategy to support the Organization's needs and its responsibilities to the State. DOR may not be appropriately focused on managing organizational design as outlined in the following risks:
 - The organizational plan does not seem sufficient, and the structure may not be aligned to meet needs
 - Staffing of personnel may not be focused on placing personnel with the proper level of knowledge, skills, and abilities necessary to effectively accomplish their jobs
 - Key roles and responsibilities may not be adequately defined and communicated
 - Succession plans may not be in place to plan for and manage turnover in key positions
 - Positions may not exist for those areas that may not historically have been a focus, such as financial reporting, accounting, and business and revenue analysis
 - The Organization may lack experienced personnel with knowledge of the operating procedures specific to tax types
 - Revenue stream reporting may not exist due to the lack of experienced personnel who understand the end to end business by tax type in order to perform appropriate analysis
 - There may not be a robust change management process to implement and communicate changes consistently across the Organization

Summary of Proposed Controls and Performance Audit Plan Areas

As a result of the risk identification process and ranking procedures performed for DOR specific risks and inherent risks, 18 key business processes were identified to be the Organization's performance audit universe. Of these 18 processes, 9 have been identified as high risk, 8 have been identified as medium risk, and 1 has been identified as low risk. The audit plan and procedures focus testing efforts on the 17 areas of high risk and medium risk as identified below:

- High Risk (In alphabetical order)
 - Manage Financial Accounting and Reporting
 - Manage Organizational Design
 - Manage Information Technology
 - Manage Revenue Accounting and Distributions
 - Perform Collection Activities (Past-Due Items)
 - Perform Internal Audit
 - Perform Tax Administration and Analysis
 - Plan for and Manage the Organization
 - Report Administration

A higher level of audit procedures will be performed for key business processes identified within the audit universe as "high risk," including policy and procedure review, identification of key reporting aspects, and testing of integral activities within the process.

- Medium Risk (In alphabetical order)
 - Issue Refunds or Credits
 - Legal
 - Perform Billing Activities
 - Perform Enforcement Activities
 - Perform Front-End Processing
 - Process Receipts (Post Payments to Taxpayer Account)
 - Process Tax Return Data
 - Taxpayer Registration and Education

A moderate level of audit procedures will be performed for key business processes identified within the audit universe as “medium risk,” including policy and procedure review, identification of key reporting aspects, and testing of integral activities within the process.

- Low Risk
 - Provide Taxpayer Assistance

A minimal level of audit procedures will be performed for key business processes identified within the audit universe as “low risk,” including policy and procedure review.

- Special Attention Area

As a result of the reported errors noted in this report, special attention will be given as part of Phase 2 to review the known errors that occurred in corporate tax and LOIT areas. Analysis of the identified distribution errors, including a walk-through of the processes to identify the past procedural breakdowns, accounting transaction review of the correcting entries and support, as well as the evaluation of management’s remediation plans to identify whether risks have been properly mitigated will be performed.

Scope and Methodology

Financial Operations Risk Assessment

Deloitte & Touche completed a financial operations risk assessment of DOR's IT and financial operations, specifically as follows:

- Internal IT and financial controls
- Current IT systems, policies, and procedures
- Current financial policies and procedures
- IT, financial, and auditing organizational structure

The risk assessment incorporated the various aspects of risk, including, but not limited to, size (both dollars and number of transactions), complexity of operations, control weaknesses, and propensity for human error. The aspects of risk are found within every organization and can be broadly defined as "what can go wrong." "Risk" is not synonymous with "problem," and the risks that are identified in this report are a combination of risks that exist at DOR and risks that are inherent in state revenue agencies. Identified risks were grouped into categories aligned with DOR processes and given high, medium, or low values based on the effects a realized risk would have on the Organization and the extent to which the Organization may be unprotected from the risk. Deloitte & Touche utilized the following four-stage approach in performing the risk assessment:



Stage I: Understand DOR's key business processes

During Stage I of the approach, Deloitte & Touche gained an understanding of DOR's control environment and key business processes. Documentation and information obtained from DOR included business objectives and goals, strategic plans, key performance metrics, budgets, policies and procedures, management reports, prior controls and performance audit reports, financial statements, internal and external audit reports, process and systems flows and related documentation, and relevant reconciliations and analyses performed to date.

Deloitte & Touche mapped key business processes and systems to the Organization's objectives, strategies, and goals. These activities resulted in the controls and performance audit universe considered in the risk assessment.

Stage II: Develop the risk model

Utilizing the identified controls and performance audit universe from Stage I, Deloitte & Touche identified the most salient risk categories, grouped identified risks into the categories, and

customized financial operational risk definitions for each risk. Deloitte & Touche's proprietary Risk Intelligence Map and Risk and Control Knowledgebase were leveraged, in addition to external resources.

The risk model utilized two criteria for ranking and prioritizing risks. These criteria were impact and vulnerability. Impact is an estimate of the severity of adverse effects, the magnitude of a loss, or the potential opportunity cost should a risk be realized. Impact can be thought of as gross inherent risk. Vulnerability is the extent to which the functional area may be exposed or unprotected in relation to various risk factors after existing controls have been taken into account. In other words, vulnerability is the susceptibility of the Organization to the risk.

Using the information gathered in Stages I and II, Deloitte & Touche identified the current risks facing the Organization for inclusion in the assessment and prioritization process. The customized risk model was then used in Stage III to provide a common understanding for the assessment and prioritization of risks.

Stage III: Assess and prioritize risks

In Stage III, Deloitte & Touche worked to define the risk assessment approach and process for completing the assessment (e.g., conducted one-on-one interviews, facilitated workshops). Executives, management, and process owners were identified to participate in the risk assessment. The results of the risk assessment interviews and workshops with the representatives from the following offices were compiled and risks identified for assessment and prioritization.

State agencies and offices included in the interviews

- Department of Revenue
- Office of Management & Budget
- Auditor of State
- Treasurer of State
- State Budget Agency (SBA)
- Department of Local Government Finance
- Indiana State Board of Accounts (SBOA)
- Indiana Office of Technology (IOT)

Two types of risks identified and assembled into the customized DOR risk assessment were as follows:

- **DOR-Specific Risks** — Risks that have been identified through the interview process and are specific to the Organization.
- **Inherent Risks** — Risks that naturally exist in the Organization's business processes and that are pervasive within governmental organizations and revenue agencies

In evaluating the impact and vulnerability of the risks, both quantitative and qualitative factors were considered. These factors included, but were not limited to, financial impact, reputational impact, taxpayer impact, likelihood of the risk consequences, prior experience with the risk, complexity of operations, and organizational structure. The risks were then assigned a ranking of high, medium, or

low according to the risk impact and vulnerability as defined in Stage II. The corresponding color ranking, shown below, is used throughout this report to identify the risk level of each key business process.

- **Red** — High-risk area with multiple significant DOR-specific and/or inherent risks identified
- **Yellow** — Medium-risk area with moderate DOR-specific and/or inherent risks identified
- **Green** — Low-risk area with low DOR-specific risks identified and/or low inherent risks identified

The results of the risk assessment provided a point-in-time assessment of the impact of the risks on the Organization and the vulnerability of the Organization to said risks. Management has begun to implement remediation plans in various areas which will be reviewed as a part of the controls and performance audit.

Stages IV: Develop a risk-based controls and performance audit plan

These prioritized risks will be the focus of the controls and performance audit. The risk assessment results are the primary driver for developing the controls and performance audit approach. Not every risk and area identified in the prior stages is “auditable.” The results of the risk assessment process and the other factors described yield risks and concerns that may not be effectively addressed by a controls and performance audit. Rather, these areas may be better addressed by management initiatives, programs, or other mechanisms.

The preliminary risk-based controls and performance audit plan is presented in this document. Tailoring of the controls and performance audit to execute the controls and performance audit assessment will be conducted in Stage I of the controls and performance audit.

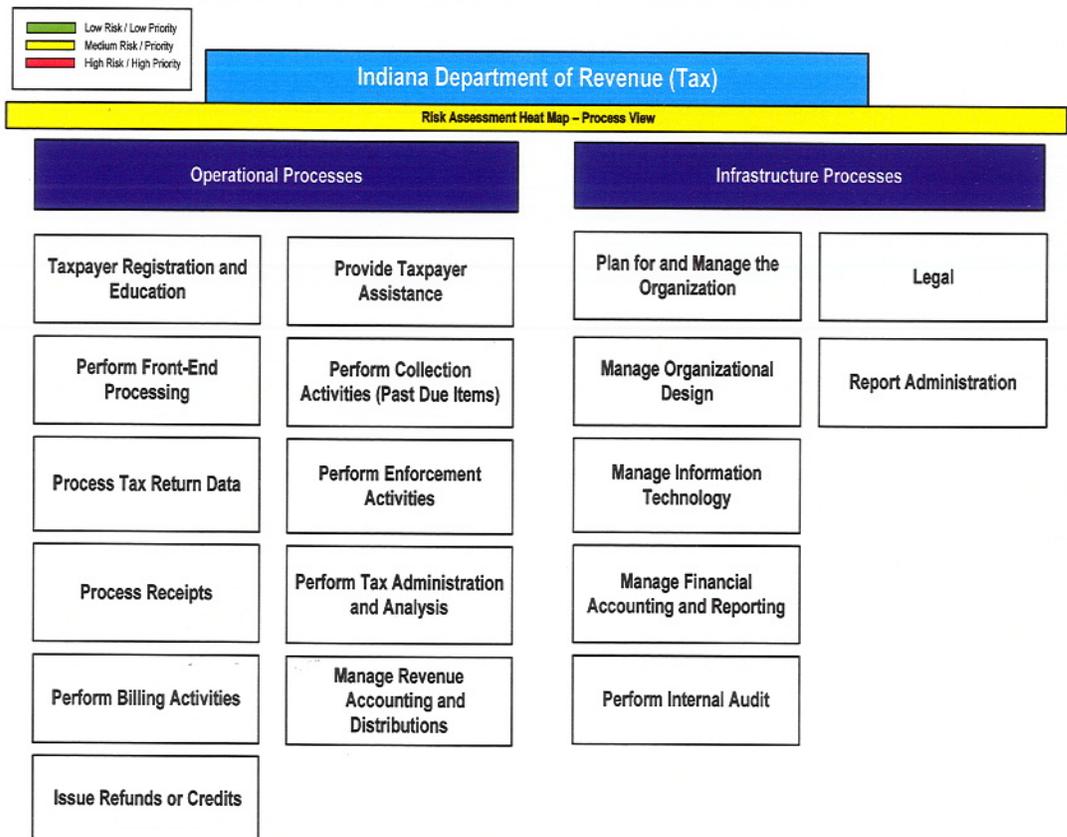
Professional Standards

Our services were performed in accordance with the Statement on Standards for Consulting Services issued by the AICPA. These services did not constitute an engagement to provide audit, compilation, review, or attestation services as described in the pronouncements on professional standards issued by the AICPA, and, therefore, no opinion will be expressed or other form of assurance with respect to the services. In addition, the services did not constitute an examination or compilation of prospective financial information in accordance with standards established by the AICPA. No legal advice regarding our services was provided; the responsibility for legal issues with respect to these matters is OMB's and DOR's. It is further understood that OMB and DOR management is responsible for, among other things, identifying and complying with laws and regulations applicable to OMB and DOR activities.

Controls and Performance Audit Universe

Risk Assessment Process Overview

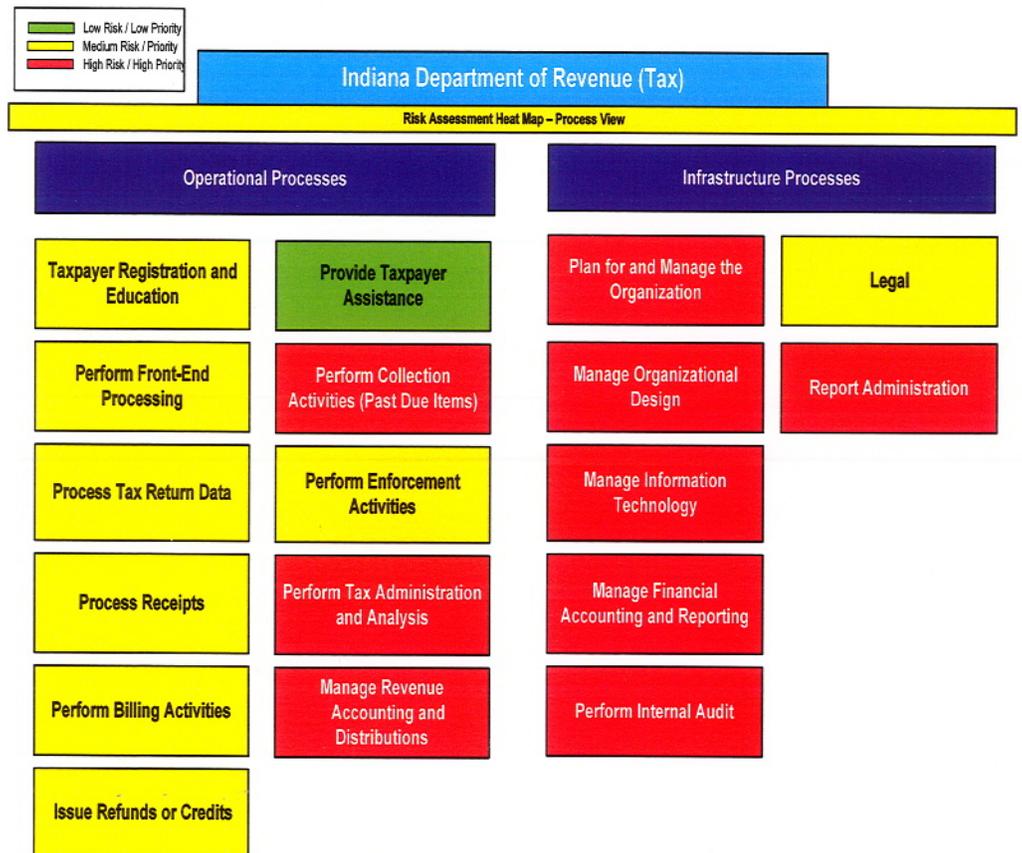
As mentioned in the executive summary, a pictorial map of DOR's key business processes was separated into two categories: operational processes and infrastructure processes. Operational processes, as used here, are those areas that run the day-to-day business of the Organization and support the key mission of collecting and accounting for taxes. Infrastructure processes, as used here, are those areas that are the foundation of the Organization and run in the background to support the day-to-day functions. These processes and the naturally occurring subprocesses collectively make up the controls and performance audit universe from which the risk assessment was performed.



Risk Assessment Results

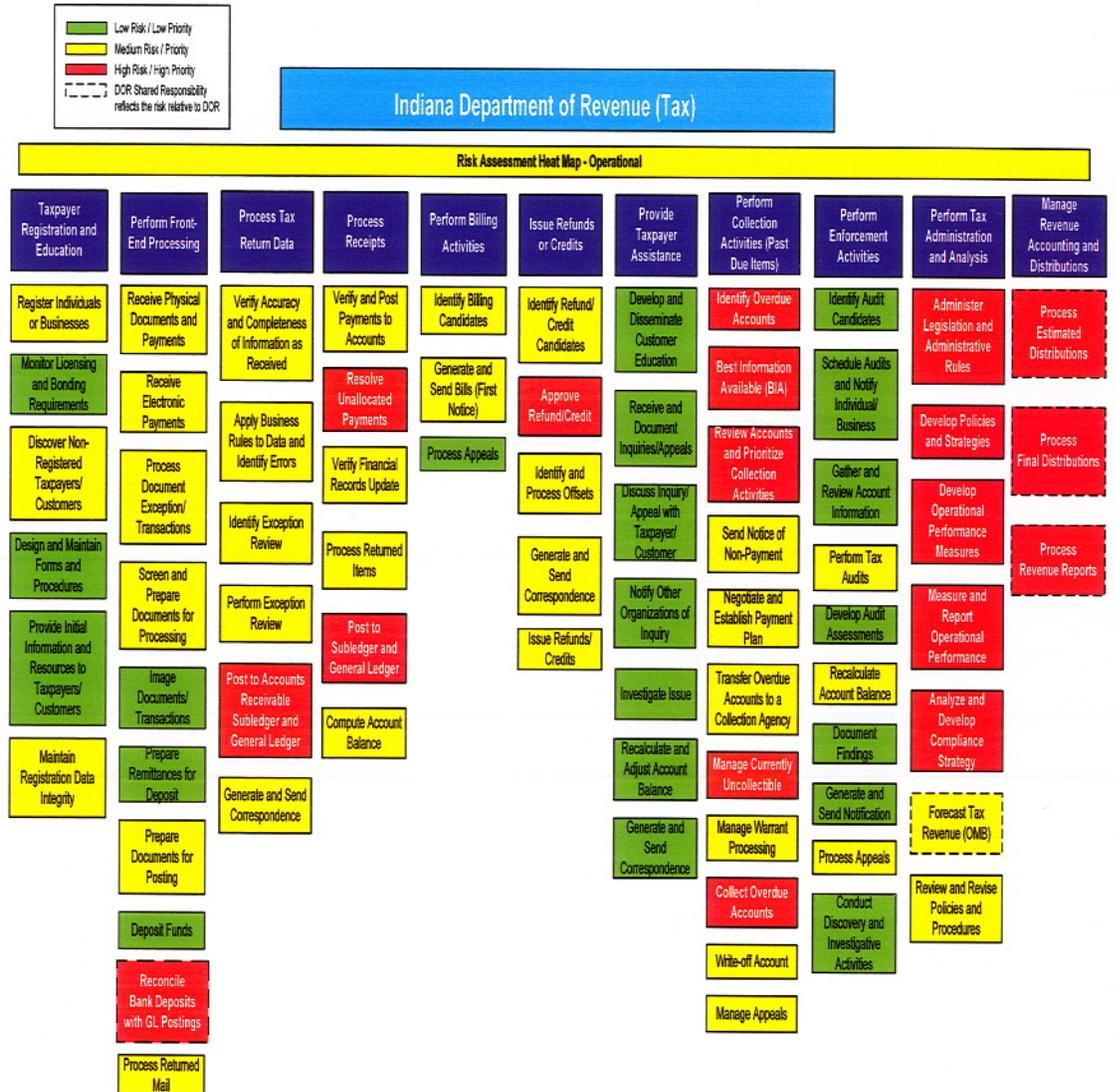
Process-Level Risk Map

As stated previously, DOR-specific risks that were collected through the interviews were identified and combined with the inherent risks that are pervasive within revenue agencies and similar governmental organizations. An overall ranking was assessed for each key business process and corresponding subprocesses. These risks rankings were then captured on the controls and performance audit plan by color-coding each area with its overall risk score. A pictorial view of the risk rankings for the key business processes and the subprocess view are reflected on the next pages.



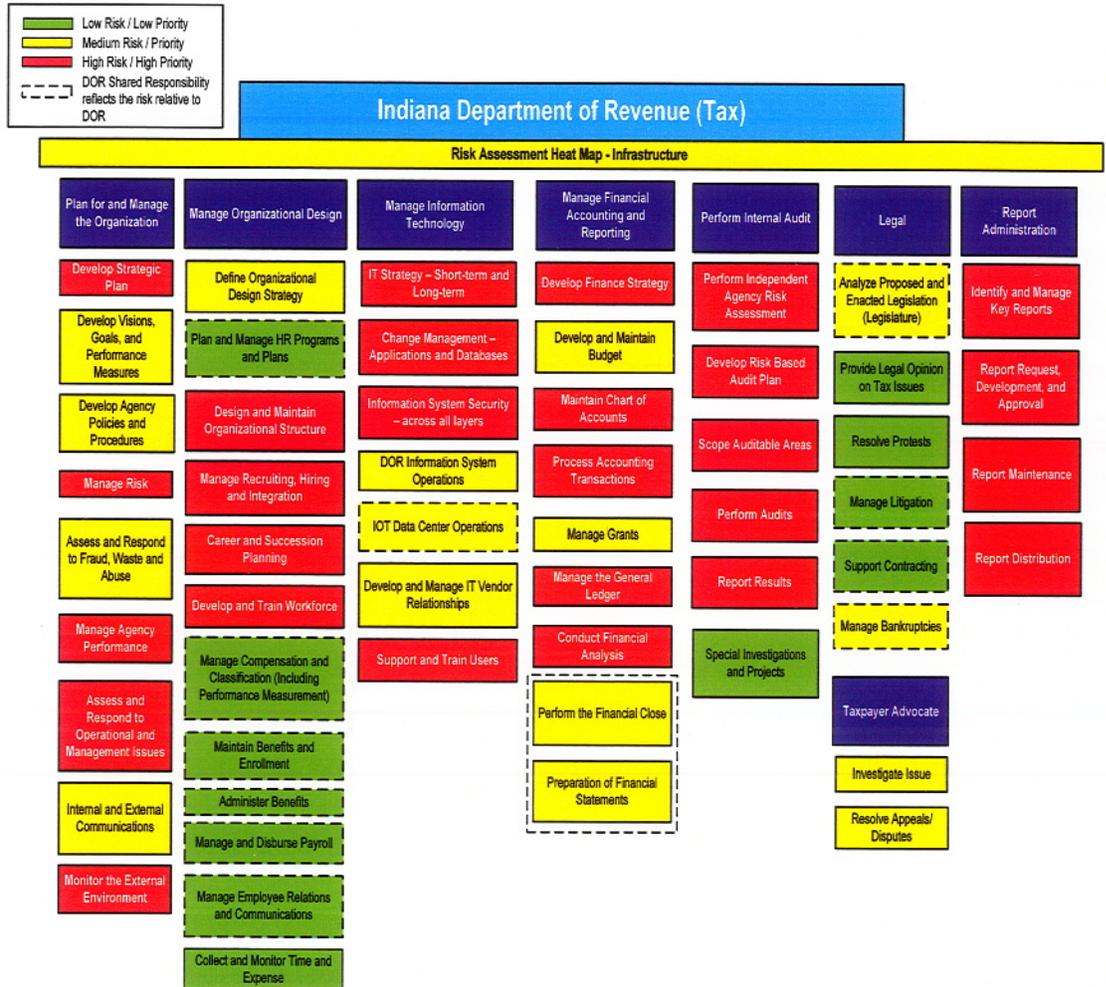
Operational-Level Risk Map

As stated previously, DOR-specific risks that were collected through the interviews were identified and combined with the inherent risks that are pervasive within revenue agencies and similar governmental organizations. Below is a pictorial map of DOR's risk rankings by operational subprocess. Operational subprocesses are those related to DOR's key mission of collecting and accounting for taxes. Subprocesses outlined by a dotted line indicate a shared responsibility, as noted in the legend below:



Infrastructure-Level Risk Map

As stated previously, DOR-specific risks that were collected through the interviews were identified and combined with the inherent risks that are pervasive within revenue agencies and similar governmental organizations. Below is a pictorial view of DOR's risk rankings by infrastructure subprocesses. Infrastructure subprocesses are those related to the support and management of DOR. Subprocesses outlined by a dotted line indicate a shared responsibility, as noted in the legend below.



Key Business Process Risks

Risk is broadly defined as “what can go wrong.” It is the possibility of an event occurring that will have an impact on the achievement of objectives. “Risk” is not synonymous with “problem,” and the risks that are identified in this report are a combination of risks that exist at DOR and risks that are inherent in state revenue agencies. These inherent risks may or may not cause loss exposure to DOR and are not a statement that a problem exists.

The focus of the controls and performance audit will be the prioritized risks, including DOR-specific risks and inherent risks. The risk assessment results are the primary driver for developing the controls and performance audit approach and are a point in time assessment of the Organization. DOR leadership has begun to implement mitigation plans for certain risks that have been identified. These mitigation plans will be reviewed as part of the procedures explained in the controls and performance audit approach (see page 24 for details on the controls and performance audit approach).

The key business process risks are represented below and are separated into the two categories shown in the previous pictorial maps. These categories are operational processes and infrastructure processes.

Operational Business Process Risks

Below are the DOR-specific and inherent risks identified for the key operational business processes. Operational processes, as used here, are those areas that run the day-to-day business of the Organization and support the key mission of collecting and accounting for taxes. The color of the top box represents the risk ranking of this process as defined in Section III — Scope and Methodology.

Taxpayer Registration and Education

Overall Process Description	Registering taxpayers by tax types, identifying potential taxpayers, designing and maintaining forms and procedures, and maintaining the integrity of registration information; possibly serving as a source of general information for taxpayers regarding tax types, fees, fines, etc.
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • The registration process for creating a tax ID does not appear to be integrated with the Returns Processing System (RPS) • RPS is not a fully integrated taxpayer system and may not capture all tax types, which prevents DOR from easily determining the universe of taxpayer obligations

Perform Front- End Processing

Overall Process Description	Receiving payments and documents, opening mail, capturing electronic data, and sorting and preparing documents for potential imaging and distribution to ensure accurate and timely recording of payments to accounts and same-day deposit
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • Reconciliation of payments in RPS to PeopleSoft may not be consistent, and errors may not be identified in a timely manner due to the manual nature of the reconciliation • RPS may allow accounts receivable ("AR") and liabilities to be overwritten rather than require adjustments; audit trail of changes may be lost • Incompatibility issues may occur with third-party filing options (e.g., TurboTax, H&R Block, etc.) and integration with RPS; returns may be rejected or funds may be misapplied

Process Tax Return Data

Overall Process Description	Reviewing information and revenue received for a given transaction and/or liability to verify appropriateness, and validating information and remittance amounts
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • RPS and other tax-processing applications may not support automated feeds to PeopleSoft; this system limitation could lead to data entry errors • Inaccurate and incomplete information received and processed through predefined thresholds may result in unresolved data capture discrepancies and delay transactions from being posted • Delinquency correspondence may not be generated as necessary and may delay further information gathering or the receipt of payments

Process Receipts

Overall Process Description	Updating accounts to reflect payments, verifying and posting payments to accounts, adjusting accounts, making transfer payments when accounts are improperly credited, and processing returned items
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • The Voucher Commit Report may not provide the type of detail needed to post data accurately to the general ledger in PeopleSoft • Manually created Excel worksheets may be used to upload journal entries to PeopleSoft and may not have adequate review; data entry errors and inaccurate financial reporting may occur • RPS seems to have been designed with a focus on returns processing and not financial reporting; therefore, AR and liabilities may not reconcile to the general ledger (PeopleSoft) • Batch reports that are unacknowledged and not processed in the system may not be identified in a timely manner; delays in processing batch reports may result in misreporting on the Voucher Commit Report • RPS holds unallocated items in a suspense queue, which may not be reviewed regularly and may delay account resolution • RPS does not maintain a universal identifier to connect returns and payments; reconciliations may not be completed without a connection between returns and payments • Policies and procedures do not appear to be in place to guide control activities, such as reconciliation and account aging; some key processes and control activities are not defined and may not be consistently applied

Perform Billing Activities

Overall Process Description	Accumulating data; calculating account balances; applying interest, outstanding charges, and/or credits; and preparing appropriate documentation (e.g., bills)
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • Systematic restrictions may not be in place to limit the ability to manually adjust taxpayer accounts; unauthorized adjustments may be made • RPS is not a fully integrated taxpayer system and does not capture all tax types, which prevents DOR from easily determining the universe of taxpayer obligations; unidentified liabilities may lead to lost revenue/understated AR

Issue Refunds or Credits

Overall Process Description	Reviewing offsets in other organizational and/or organization systems, consolidating multiple accounts, and generating and sending relevant documentation/refunds
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • There may not be consistent and comprehensive authorization limits set for issuing refunds according to monetary value, which may allow for large refunds to be processed without appropriate management awareness • Taxpayer-initiated corporate refunds for trust taxes may not provide an audit trail or approval workflow for refunds; erroneous refunds may be issued • RPS is not a fully integrated taxpayer system and may not capture all tax types, which may prevent DOR from easily determining the universe of taxpayer obligations; unidentified liabilities may lead to lost revenue/understated AR if refunds are erroneously issued • Individual refunds are automatically generated by RPS, and limited systematic restrictions may allow adjustments by certain IT personnel without a formal approval process to identify whether the refund is required; unauthorized refunds may be issued

Provide Taxpayer Assistance

Overall Process Description	Serving as the initial point of contact for taxpayers, and other account holders who have questions regarding their account; referring complex issues to specialists, resolving appeals/disputes; and providing education to the public regarding revenue and fee issues, law changes, and procedural changes (e.g., tax filing changes)
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • Taxpayer issues may not be properly investigated and researched; issues may remain unresolved • Inquiries may not be handled properly, which can result in repeat inquiries

Perform Collection Activities (Past-Due Items)

Overall Process Description	Targeting taxpayers or other account holders to pursue for collection, determining the type of collection method most appropriate, and prioritizing accounts within the type of collection method so that collections with the greatest expected benefit are executed first
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • Collection of past-due accounts may not be efficiently and effectively prioritized due to the lack of an adequate past-due accounts aging report; higher-priority accounts may not be pursued or may be sent to collection agencies, rather than being targeted and determining and executing the most appropriate collection method, which may reduce the amount recovered • Best information available (BIA) returns may not be monitored and adjusted once the taxpayer files the correct return; subsequent payments may result in inaccurate taxpayer balances • RPS may not accurately monitor payment schedules for taxpayers on a payment plan, and taxpayers who default may not be appropriately pursued; when notices of nonpayment are produced, returns may suspend in RPS, which may result in a delay in posting received payments • Policies and procedures may not be in place to guide activities such as prioritizing collection efforts and aging taxpayer accounts; key processes that were once performed may no longer be consistently applied

Perform Enforcement Activities

Overall Process Description	Conducting audits or investigations to identify whether taxpayers or other account holders are complying with laws, policies, and procedures
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • RPS allows AR and liabilities to be overwritten rather than require adjustments; audit trail of changes may be lost • Higher-risk taxpayers may not be selected for audit, which may result in reduced collections, underreported AR, and missed revenue • Findings that are not well documented may result in the inability to address appeals and quickly collect receivables

Perform Tax Administration and Analysis

Overall Process Description	Administering legislation and administrative rules affecting revenue collection and receivables management, developing performance goals and targets for revenue and receivables management, developing specific policies and strategies that enable the Organization to meet related performance goals, along with the analysis and management of accounts
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • Clear processes and procedures for implementing legislative changes may not be in place or consistently applied; implications of new tax laws may not be understood or reflected in tax systems • There may be a lack of coordination between the tax policy group and other functions for the coordination of legislative changes • Performance measures may not reflect the goals of management, and the Organization's business lines may not have strategies based on information such as stated goals and direction of governing administration, organizational/enterprise-wide performance goals and objectives, and the Organization's directives; this may result in limited accountability within the Organization • The Organization lacks business line performance reporting measures by type of tax; trends in collections and payments may not be effectively monitored • Revenue estimates are derived from upstream accounting and may be inaccurate or compromised • There may be a lack of business analysts or experienced personnel who are responsible for understanding operating procedures by tax type, including analyzing, trending, forecasting, and reporting on the revenue

	<ul style="list-style-type: none"> • A compliance strategy that reflects enforcement and voluntary compliance goals may not be in place; opportunities to improve collections efficiency may not be identified
--	---

Manage Revenue Accounting and Distributions

Overall Process Description	Processing estimated distributions and final distributions, and preparing revenue reports
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • The procedures for the tax distribution process and revenue reporting may not be documented and regularly reviewed by management; distributions and revenue may not be reported correctly or completely • The DOR-managed Collections Fund is not analyzed and reviewed regularly by management for trends and expected movement; reconciliation of final distributions is not performed; errors may not be identified and corrected in a timely manner • Excel worksheets are used to manually manipulate large volumes of data for reporting and to upload journal entries to PeopleSoft; data entry errors and inaccurate financial reporting may occur • Journal entries may not be regularly reviewed and approved by management • Upstream accounting and underlying data may result in inaccurate revenue estimates • A formalized data warehouse strategy does not exist and may result in inflexible reporting capabilities that do not support an integrated analytic framework • There may be a lack of business analysts or experienced personnel who are responsible for understanding operating procedures by tax type, including analyzing, trending, forecasting, and reporting on the revenue • Unbilled revenue, Suspense, A/R Holding, and Clearing accounts may not be reconciled monthly to clear and post amounts to the appropriate accounts

Infrastructure Business Process Risks

Below are the DOR-specific and inherent risks identified for the key operational business processes. Infrastructure processes, as used here, are those areas that are the foundation of the Organization and run in the background to support the day-to-day functions. The color of the top box represents the risk ranking of this process as defined in Section III — Scope and Methodology.

Plan for and Manage the Organization

Overall Process Description	Assessing community conditions and needs; defining an overall organizational strategy and corresponding operational, capital, and financial plans; developing specific performance goals and targets; and monitoring and reporting performance to stakeholders
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • There may not be adequate strategic goals in place for the Organization and there may be a lack of an overall governing strategy that guides the Organization to achieve its goals • The strategic plan set out by DOR has historically been focused on the efficiency of return processing, with secondary focus on financial reporting and controls • There is currently a lack of resources who understand both business and technology implications of changes to systems; the roles of current resources may not be adequately defined and communicated • Organizational structure may not be designed to promote a sound control environment (i.e., there may be little systematic control over delegation of authority or adequate segregation of duties or a reduction of staff without understanding implications on required controls) • There may be a lack of recognition of the importance of a strong system of governance and internal controls • Organization-wide policies and procedures may not exist or be consistently applied for operations and financial departments, and knowledge transfer does not always occur as employees retire; furthermore, accountability and responsibility for financial information may be an issue • There may be a lack of business analysts or experienced personnel who are responsible for understanding operating procedures by tax type, including analyzing, trending, forecasting, and reporting on the revenue

Manage Organizational Design

Overall Process Description	Planning and managing human resource aspects of the Organization, including organizational design, employee development, employee data/information retention, and employee succession planning
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • Positions may not exist for those areas that may not historically have been a focus, such as financial reporting, accounting, business analytics, and revenue accounting • The organizational structure of the Organization may not be designed to support DOR strategies and goals; key roles and responsibilities may not be adequately defined or communicated, and key positions have been vacant or only recently filled • Organization-wide succession planning may not include plans for retirement of tenured individuals and knowledge transfer of their responsibilities • Internal controls may not be emphasized throughout all levels and departments of the organization • Employee training plans may not be robust to include specific areas of expertise needed around systems and applications, e.g., data warehouse users

Manage Information Technology

<p>Overall Process Description</p>	<p>Defining an IT strategy and annual business plan, assessing current and future IT architecture requirements, developing and managing vendor relations, selecting and implementing new products and services, and managing the IT environment and information security</p>
<p>Risk Identified DOR-Specific and Inherent Risks</p>	<ul style="list-style-type: none"> • There does not appear to be an overarching DOR IT strategy to address the short- and long-term needs of the Organization, and there may not be a SDLC process defined; policies and procedures related to technology may be unclear or undocumented • A formal change management process and policy may not be place, which may result in changes occurring without authorization or testing and ownership or accountability; business rules may not be correctly implemented • Systems may not offer proper analytics and controls, which leads to concerns about data integrity • It appears that limited transfer of knowledge occurred and limited documentation exists following the departure of Accenture, and DOR was left with limited resources who had the appropriate knowledge to maintain RPS • RPS and other tax-processing applications do not support automated feeds to PeopleSoft; this system limitation may lead to data entry errors • RPS and other tax-processing applications are inflexible and antiquated and may not fulfill the needs of the Organization or adapt to the changing environment in which the Organization operates • RPS and other tax-processing applications do not appear to have an audit-logging feature that allows for proper controls, such as reconciliation to mitigate potential risk • Complexity of the code and limited resources (people and capacity of technology) of RPS and other systems may create a potentially unstable environment for future enhancements and maintenance of the application and may cause unintended results or errors in processing; existing codes are not periodically reviewed for legislative and policy changes that may have an impact • DOR has not recently tested disaster recovery and may not have business continuity plans in place for several systems • Security monitoring of access to systems may not be completed; employee access may not be updated in coordination with changes in roles and responsibilities • Application and data security may not be effective to mitigate risk and protect tax information • Employees outside of IT may not receive adequate training in system use, which may reduce their ability to complete reconciliation of financial activity • System and data audit logging, change monitoring, and system history maintenance for tax-processing information may not be occurring • The Organization may not have personnel or business analysts who are knowledgeable in both IT and business processes in that they would be able to develop necessary business requirements to correspond with IT changes

Manage Financial Accounting and Reporting

Overall Process Description	Developing and maintaining a finance strategy and budget, along with managing a chart of accounts, maintaining a general ledger, conducting financial analysis, performing financial close, and preparing financial statements
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • Key financial reconciliations are not consistently and adequately performed; in processes where there are reconciliations performed, they may not be sufficient to identify issues • Policies and procedures may not be in place to guide financial accounting; key processes and control activities are not well defined and may not be consistently applied • Direct interface does not exist between RPS and PeopleSoft, which may cause data to be manually manipulated and transferred into PeopleSoft and may result in inefficiencies and increased risk for errors • Excise taxes that are processed outside of RPS may not be subjected to the same level of controls as taxes processed within RPS and may not be reconciled to the general ledger • The Finance department does not appear to have adequate personnel with knowledge and skills around financial controls that may prevent or detect errors and limit opportunities for fraudulent activity, e.g., robust journal entry controls may not exist, including reviews by management and dollar-amount authority levels • The Finance department may not receive appropriate training in system use; inadequate understanding of RPS and PeopleSoft may hinder the department's ability to monitor financial activity • Ownership and responsibility for reconciliation of DOR PeopleSoft general ledger accounts may not exist; errors may not be identified due to a lack of accountability for the management of the chart of accounts • Unbilled revenue, Suspense, A/R Holding, and Clearing accounts may not be reconciled monthly to clear and post amounts to the appropriate accounts

Perform Internal Audit

Overall Process Description	Independent risk assessment, developing a risk-based audit plan, performing and reporting audits, and conducting special investigations and projects
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • Independent risk assessments do not appear to be performed, and internal control systems may not be monitored; there is a role within DOR for internal audit responsibilities, but the position is not placed in an independent position within the organizational structure • A risk-based audit plan and traditional internal audits with formal internal audit reports do not appear to be performed; rather, special projects and investigations are being conducted • Internal audit may not have sufficient personnel to function independently of the finance department and to operate to the standards of the governing body of internal auditors, the Institute of Internal Auditors

Legal

Overall Process Description	Analyzing, interpreting, and evaluating legislation for impact, issuing legal opinions on tax issues, resolving protests, managing bankruptcies, and managing taxpayer advocacy, including investigating issues and resolving appeals and disputes
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • Tracking of bankruptcy cases, generation of bankruptcy letters, tracking of bankruptcy claims, and issuance of other reports do not appear to be managed within the RPS system • There is currently no system that imports bankruptcy data from the U.S. bankruptcy courts; identifying taxpayers who have filed for bankruptcy may be manually intensive • The Legal department may not be staffed appropriately to support the needs of the Organization

Report Administration

Overall Process Description	Identifying and managing key reports, maintaining and distributing reports, and developing and approving ad hoc report requests
Risk Identified DOR-Specific and Inherent Risks	<ul style="list-style-type: none"> • A robust process for managing reporting may not exist and there seems to be no list of key reports that management needs to run the business • There may be limited management knowledge associated with key reports to ensure they are complete and accurate and meet the needs of the user • There may be limited clear processes for controlling distribution and use of key management reports • Underlying standards or policies governing the reporting process for DOR may not exist, including requests for new reports and limits on ad hoc reporting and reviews for completeness and accuracy prior to distribution in DOR and outside the Organization; reports that could be incomplete or inaccurate may be distributed and relied upon by DOR or other agencies • There may not be periodic maintenance of key management reports to ensure they are sustainable and repeatable • DOR may be lacking in sufficient data warehouse power users with knowledge to execute ad hoc reports and conduct analytical reporting • The reporting impact of legislative changes, new tax revenue streams, changes to payment or tax types, and corresponding business rules may not be fully tested or validated for completeness and accuracy; certain data may not be captured and reported • Employees outside of IT do not have an understanding of system-reporting capabilities, which may reduce their ability to monitor and reconcile financial activity

Controls and Performance Audit Plan

Areas to be Audited

Utilizing the risk-ranked controls and performance audit universe identified previously, a proposed controls and performance audit plan was developed to focus more extensive audit attention to the areas with high to medium risk within the Organization. As such, areas with high to medium risk are included in the audit plan for testing and review, including sample based transaction testing in processes where transactions are performed. The area with predominately low risk is included in the controls and performance audit plan but will receive a lower level of review than the riskier areas.

Special attention will be made to review the known errors that occurred in corporate tax and LOIT. Analysis of the identified distribution errors, including a walk-through of the processes to identify the past procedural breakdowns, and evaluation of management’s remediation plans to identify whether risks have been properly mitigated will be performed.

Level of Risk	Process Description	Controls and Performance Audit Review
Low-Risk Processes	<ul style="list-style-type: none"> • Provide Taxpayer Assistance 	<ul style="list-style-type: none"> • Compare policies, procedures, and controls against leading practices • Identify opportunities for enhancement
Medium-Risk Processes	<ul style="list-style-type: none"> • Issue Refunds or Credits • Legal • Perform Billing Activities • Perform Enforcement Activities • Perform Front-End Processing • Process Receipts (Post Payments to Taxpayer Account) • Process Tax Return Data • Taxpayer Registration and Education 	<ul style="list-style-type: none"> • Compare policies, procedures, and controls against leading practices • Conduct a walk-through of process • Perform high-level tests of operating effectiveness • Identify and review key reports, data sets, and analytics (i.e., reconciliations, trending, forecasts, etc.) for completeness, accuracy, and relevancy • Identify opportunities for enhancement • Identify preventative and detective controls • Select and review a sample from the testing population where transactions occur • Perform an analysis and walk-through of management’s remediation plans

Level of Risk	Process Description	Controls and Performance Audit Review
High-Risk Processes	<ul style="list-style-type: none"> • Manage Financial Accounting and Reporting • Manage Organizational Design • Manage Information Technology • Manage Revenue Accounting and Distributions • Perform Collection Activities (Past-Due Items) • Perform Internal Audit • Perform Tax Administration and Analysis • Plan for and Manage the Organization • Report Administration 	<ul style="list-style-type: none"> • Compare policies, procedures, and controls against leading practices • Conduct a walk-through of process to Review implementation • Identify and review key reports, data sets, and analytics (i.e., reconciliations, trending, forecasts, etc.) for completeness, accuracy, and relevancy • Identify opportunities for enhancement • Identify preventative and detective controls • Perform detail tests of operating effectiveness • Select and review a sample from the testing population • Perform an analysis of the identified distribution errors, including a walk-through of the processes, and evaluation of management’s remediation plans

Controls and Performance Audit Approach

There are four stages within the controls and performance audit approach for the areas identified above. The four stages are outlined below:

Stage I: Controls and Performance Audit Planning

Controls and performance audit planning includes developing controls and performance audit procedures for the key business processes identified in Stage I. At a high level, these procedures include the following:

- Identify the approach for assessing design and operational effectiveness of key business processes identified in the risk assessment
- Prepare controls and performance audit programs for each of the key business processes, including test plans
- Confirm existence and availability of documentation to be used during the controls and performance audit
- Develop timeline for performing the underlying procedures for each of the key business processes
- Identify resources to perform procedures, including the use of subject matter specialists
- Identify the level of effort, establish budget, and update the statement of work, as appropriate

Stage II: Evaluate Design

Evaluate the design of DOR strategy and governance as it relates to process, technology, and people. At a high level, these procedures include the following:

- Perform an analysis of the identified distribution errors, including a walk-through of the processes to identify the past procedural breakdowns, evaluation of management’s remediation plans to identify if risks have been properly mitigated and testing of the mitigating controls
- Identify preventative and detective controls in DOR’s key business processes

- Compare these controls against leading practices within the industry and of similar state organizations to identify gaps and opportunities for improvement
- Assess the entity-level controls, which includes the control awareness, management philosophy, operating style, employee values, and general “tone at the top” of the Organization
- Assess at a high level whether DOR’s organizational structure is sufficient and ties to organizational strategy and operations
- Assess at a high level whether sufficient policies and procedures to guide daily operations have been documented and communicated to staff
- Assess at a high level whether staff are appropriately trained and held accountable for following DOR policies and procedures
- Assess at a high level whether DOR has staff with the proper level of knowledge, skills, and abilities necessary to execute the organization’s responsibilities
- Assess the design of processes for identifying, escalating, and mitigating organizational risks
- Ascertain whether policies, procedures, and key controls have been implemented into daily operations
- Ascertain whether IT systems (e.g., RPS, PeopleSoft, Data Warehouse, INtax), processes, and related components are sufficient to address the risks in support of DOR operations, accounting and reporting
- Identify and review key reports, data sets, and analytics (i.e., reconciliations, trending, forecasts, etc.) for completeness, accuracy, and relevancy
- Assess DOR’s internal audit methodology and approach
- Identify deficiencies in design and develop recommendations for improvement

Stage III: Test of Operational Effectiveness

Testing of operational effectiveness includes the evaluation of whether key policies, procedures, and controls are operating with sufficient effectiveness to provide reasonable assurance that the Organization’s objectives are being met. These procedures include the following:

- Perform testing of operating effectiveness for a defined period of time
- Document tests of the operating effectiveness of key controls, evidence obtained, results of tests, and conclusions within working papers
- Identify deficiencies in operating effectiveness, highlighting critical issues and common themes across the Organization
- Assess effect of control deficiencies on other key control activities and business processes
- Develop recommendations for enhancing the effectiveness of policies, procedures, and controls

Stage IV: Prepare and Issue Audit Report

Reporting includes the communication of the controls and performance audit results to OMB, DOR management, and the State Budget Committee. The procedures include the following:

- Define the format, structure, and content of the final report

Controls and Performance Audit Timeline

The controls and performance audit timeline for the project has been broken up into four stages as outlined in the previous Controls and Performance Audit Approach section.

	August		September		October		November		December		January	
	8/6- 8/17	8/20- 8/31	9/3- 9/14	9/17- 9/28	10/1- 10/12	10/15- 11/2	11/5- 11/16	11/19- 11/30	12/3- 12/14	12/17- 12/28	12/31- 1/18	1/21- 2/1
Detailed controls and Performance Audit Planning	■											
Evaluate Design			■									
Test of Operational Effectiveness					■							
Prepare and Issue Audit Report								■				

Assumptions to Timeline

- It is assumed that this timeline is supported by client management and the assumption is made that client personnel will be available to assist where needed to reach this timeline. Substantial and meaningful involvement of DOR management is critical to the success of the engagement.
- Testing of newly implemented controls will focus on the design phase of the testing approach. These controls may not have enough instances of occurrence to be able to gather an adequate sample size.
- When testing transactions and controls, the test results may lead to more sampling. If errors are found, expanded sampling could impact the timing and duration of the controls and performance audit. As a result, the timeline may go past end of the year if further risks are identified and/or further errors are found.