Deloitte.

Oregon Department of Transportation

Driver and Motor Vehicle Services

Data Integrity Review (DIR) Project

Preliminary Review Report

December 20, 2024

Table of Contents

Executive Summary

Deloitte conducted an initial data integrity review for the Oregon Department of Transportation (ODOT) Driver and Motor Vehicle (DMV) Services Division as the first of a two-phase process based upon Governor Tina Kotek's high priority timeline to deliver the Preliminary Review Report by December 31, 2024. The results should be viewed as foundational and will be further elaborated and expanded following the collection and evaluation of additional insights and data as part of Deloitte's Final Review Report. This assessment used a People, Process, and Technology (PPT) model as the overarching framework. The 'People' aspect emphasized the importance of skilled, motivated, and highly trained DMV employees who are adept at leveraging technology while adhering to DMV policies and procedures. The 'Process' component focused on DMV workflows and procedures that drive consistency and quality across its operations. Finally, the 'Technology' view assessed DMV tools and systems that facilitate operational transactions, data management, communication, and automation. Underpinning the PPT model and Deloitte's evaluation was the importance of data, particularly regarding its accuracy, consistent application, and reliability throughout all DMV operations.

During the initial assessment period, Deloitte conducted a strategic review and analysis of DMV-provided artifacts (See Appendix 4), including policies, audits, after-action reports, additional assessments, training materials, and workflows. Deloitte then conducted 13 stakeholder and process-owner interviews (See Appendix 3) to gain a deeper understanding of, among other things, DMV's strategic goals and objectives, data governance, field operations, change management, and training. Additionally, Deloitte conducted live, in-person visits to three DMV field office locations and the HQ DMV call center to observe driver-related transactions, supplemented by a training environment demonstration of additional transactions (See Appendix 2). Our initial analysis identified 14 observations, and each comes with associated proposed actions and a business rationale for management's consideration. The identified gaps could potentially impact DMV business operations by causing transactional errors driven by compromised data integrity and include areas for improvement in data automation, extraction, quality, analytics, governance, internal controls, resources, and training. By addressing these areas, DMV can improve its data integrity, streamline operations, and foster a culture of continuous improvement, ultimately driving better outcomes and customer experiences.

DMV has put in place a series of system driven object behavior changes and manually driven measures to address the internal controls to provide assurance regarding the accuracy of voter registration data within the Oregon License Issuance and Vehicle Registration (OLIVR) system. Based upon our preliminary review, we believe these systemic and manual measures provide adequate levels of assurance that data integrity within OLIVR is sufficient to reinstitute the process of Oregon Motor Voter data transfers to the Secretary of State. Our view is qualified on the condition that DMV sustains the systemic measures, continues to validate the data files (i.e., which are composed of data exported from OLIVR) transmitted to the Secretary of State for completeness, accuracy and timeliness, and existing manual measures recently

implemented be continued and monitored. Deloitte also believes the manual measures currently in place, absent additional automation, could pose risks in the context of a long-term solution. These manual measures appear to be taxing on field operations personnel, do not have a long history of performance and testability, and may not be sustainable over the long term. DMV can explore the implementation of multiple automation capabilities, to include automated processes to reduce the potential for the original human-centric errors previously associated with data integrity. Leveraging these capabilities and solutions may also address the manual processes (such as manual error review and reporting) immediately instituted by the DMV after the identification of the historical data integrity issues. The efficiencies that may be realized through the implementation of automated processes can also provide the DMV with the opportunity to strategically review existing training protocols. These realized efficiencies can support the development of a comprehensive training plan that equips the DMV to proactively address emerging trends, potential risks, and evolving knowledge requirements. Therefore, investing in advanced technologies can be evaluated to provide the assurances DMV requires while alleviating pressures on field personnel. DMV can evaluate these options in the broader context of current staffing levels, employee capabilities, budget limitations, governing policies and the law.

Project Background

In response to concerns regarding voter registration eligibility, Oregon Governor Tina Kotek directed ODOT in September 2024 to initiate a comprehensive data integrity review of the DMV. The goal was to produce preliminary actions for improved data management by the end of 2024, including enhancements to staff training to ensure they have every available resource to succeed. This directive underscored the critical importance of maintaining accurate, reliable, and secure data within the DMV's operations, which is essential for informed decision-making, regulatory compliance, and delivering reliable services to the citizens and residents of Oregon. As part of ODOT's efforts to address data integrity challenges, Deloitte was engaged to assess DMV-related data integrity processes and systems.

DMV obtains many types of data from customers via various modes, such as mail, online, telephone, email, and in-person through its 59 field offices, DMV2U Online, and headquarters in Salem. Data is entered and processed in DMV's Oregon License Issuance and Vehicle Registration System (OLIVR). This Commercial Off-the-shelf (COTS) system was implemented in Oregon DMV in 2019 for vehicle titling and registration and in 2020 for driver licenses. DMV extracts and provides data to many customers, such as, drivers, residents, courts, law enforcement, etc. Additionally, the Oregon Motor Voter law HB2177 (2015) requires DMV to provide the Elections Division of the Secretary of State's office with electronic records containing legal name, date of birth, residence, citizenship information, and electronic signature of each person that meets voter registration qualifications. Further, DMV also serves as a credentialing agency. The DMV issues credentials in the form of identity cards, permits, and driver licenses, and it can do this only in concert with the act of establishing identity as required in ORS 807, Oregon's state law covering driving privileges and identification cards.

Objectives

Deloitte conducted an initial data integrity review for DMV to assess the accuracy, consistency, and reliability of the data under DMV's management. This initial review aimed to identify and propose actions to correct discrepancies, errors, or inconsistencies in the data, thereby identifying opportunities for improving the overall quality and dependability of the information transacting through DMV's systems. Also, the review evaluated the effectiveness of current data management processes and systems to identify opportunities to mitigate future data integrity concerns. Our review included a focus on understanding current resource utilization, capacity, and training issues.

Achieving enhanced data integrity will empower the DMV to conduct its operations on a basis of accurate, reliable, secure, and efficient data management processes, which is essential for informed decision-making, regulatory compliance, sustaining customer trust, and delivering reliable services to the citizens and residents of Oregon.

Data Integrity, by acceptable industry standards, is a fundamental concept that encompasses aspects of data quality and security. It ensures that data remains accurate and consistent throughout its entire lifecycle, from creation and storage to retrieval and deletion. This is achieved by implementing rules and standards designed to prevent unauthorized modifications to the data. (For full definition and additional Key Words related to this Review refer to the Definition of Key Terms in Appendix 1). For the purposes of this assessment, and based on close alignment of industry standards, the components of data integrity include:

- **Accuracy:** the extent to which a data element correctly reflects the entity or event to which it relates, in fact, and in substance.
- **Completeness:** is the degree to which all essential data points are present in a dataset, ensuring that no vital information is omitted, and that the data achieves the anticipated level of thoroughness. Essentially, it is about having a complete and gap-free set of information.
- **Validity:** is the extent to which data is accurate, reliable and conforms to the intended format and requirements. It ensures that the data correctly represents the defined structure it is supposed to model and adheres to preset rules and constraints (such as data type, format specifications and, range). The dimension that speaks to data values complying with a defined structure or a defined domain of values as defined by business rules. The domain must also define the data type, the format, and the precision of expected values.
- **Quality:** is the extent to which data conforms to business definitions and business rules. It is the overall utility of data for its intended purpose; meaning it is specific to the business requirements and processes to which it applies and meets defined standards.
- **Timeliness:** is the extent to which data is up-to-date (also known as *Data Currency*) and available when needed for its intended use. This dimension also addresses data volatility, which pertains to the frequency and reasons for data changes. Additionally, timeliness encompasses the concept of latency, defined as the interval between the creation of data and its readiness for use.

- **Security:** the extent to which data is restricted to the appropriate parties for use or modification
- **Privacy:** the extent to which data is disclosed only to the appropriate parties and protected from unauthorized access, use, disclosure, alternation, or destruction.
- **Uniqueness:** is the attribute of data that ensures each record within a dataset is distinct and not duplicated. It involves verifying that there are no redundant entries, which helps maintain the integrity and accuracy of the dataset. Ensuring data uniqueness is tightly integrated with the concept of referential integrity within a dataset which implies that a key value is unique to a specific entity.
- **Consistency:** refers to the ways in which data remains accurate, uniform, and synchronized across all systems and databases where it is stored or accessed. It is crucial for maintaining data integrity, preventing errors, and supporting reliable decision-making.

Scope

The initial review assessed DMV's data integrity processes and systems, focusing on driver, voter registration, and human-identity related data. The scope for observations and analysis included DMV's collection and verification of customer documentation and data; documenting of information as electronic data in OLIVR; DMV's process of establishing records that meet data use requirements as defined by statutes or rules; and DMV's extracting and transmitting data accurately and securely to appropriate data users. DMV governance, policies, processes, procedures, and utilization of current systems were within the scope of this report. The scope did not include DMV vehicle registration and operations, an assessment of the efficacy of existing laws and regulation, assessment of the COTS system, or an assessment of current or prospective vendors. Deloitte reviewed the recent *Secretary of State DMV System Audit Report* to gain insights into the COTS system. As a result, this report will concentrate on how the tool is utilized in relation to various business processes, rather than providing an assessment of the system itself.

Deloitte sought to learn whether DMV is accurately evaluating and validating data provided by customers; documenting data within the systems and ensuring its integrity; extracting and transmitting required records to data users and requesters; and creating and transmitting records to various customers, such as records to the Secretary of State that meet voter registration eligibility requirements. Observations have been noted, and actions offered to help DMV consider opportunities for being more effective and assured of its posture with respect to data integrity.

Purpose of the Preliminary Review Report

This Preliminary Review Report provides initial observations, proposed actions, and business rationales in a strategic overview for the purpose of articulating validation, feedback, and guidance on the topic of data integrity. The Preliminary Review Report is based on document reviews, interviews, and observations focused on immediate insights gathered and sets the foundation for an expanded and further elaborated set of observations in the Final Review Report.

The purpose of the Final Review Report is to elaborate on each observation, action, and business rationale, providing a more detailed summary and analysis. It may also include target completion timelines for each observation and action based upon further Phase 2 conversations or interviews with ODOT/DMV stakeholders. Additionally, it will include an elaboration of initial actions that ODOT/DMV may consider, based on additional evaluations of systems, and processes, interviews, and further document analysis. Furthermore, the Final Review Report will include additional references to authoritative data to support the rationale for each action offered.

Approach

To assess and address the data integrity challenges faced by the DMV, Deloitte undertook a multi-faceted approach. This approach included a thorough review of background information, documentation, personnel interviews, field and headquarters observations, and transaction walkthroughs.

- **Review of Background Information:** We began by examining the historical context and existing challenges related to data integrity within the DMV. To provide a few examples, we focused on the *After-Action Report* that highlighted an evaluation of the accuracy, completeness, and reliability of data related to Oregon Motor Voter (OMV), the State's automatic voter registration system. We reviewed ODOT's *Strategic Action Plan* to understand the organization's mission, vision, and top priorities. We read the *DMV Strategic Plan Key Priority Charters* to better understand challenges, measurable metrics, and proposed actions. Deloitte was also provided the *Oregon DMV Data Quality Maturity Assessment* results, where Oregon DMV's overall data quality management maturity was given a rating by the assessing entity. This informed Deloitte's understanding of the parallels and differences in the approach taken, findings, and actions outlined.
- **Review of DMV Documents:** We conducted a review of relevant DMV documents (see full list of Documents Reviewed in Appendix 4) to understand the organization's structure, policies, processes, technology operations, field operations, and training programs. This included examining organizational charts, standard operating procedures (SOPs), technology infrastructure documentation, field operation workflows, and training materials.
- **Interviews with ODOT and DMV Personnel:** To gain insights from various perspectives within the organization, we interviewed key personnel, including executive leadership, functional and technology managers, and field supervisors (see full list of Stakeholders Interviewed in Appendix 3). These interviews helped us understand strategic priorities, operational challenges, technical limitations, and customer service experiences.
- **Observations of Field Personnel:** We observed field operations both in the HQ DMV call center and multiple field offices (i.e., Stayton, North and South Salem DMV). This allowed us to assess the efficiency of call handling processes, transaction processing workflows, customer interaction practices, and to identify common challenges faced by frontline staff; this evaluation afforded us an opportunity to assess whether resource constraints contributed to downstream impacts to operations and training (see full list of Site and Transaction Observations in Appendix 2).
- **Observation of Transaction Walkthroughs:** Finally, we observed transaction walkthroughs for the most common DMV transaction types in field offices, the call center, and the OLIVR training environment (see full list of Site and Transaction Observations in Appendix 2). This involved a step-by-step review of processes such as driver's license and other identity issuances, suspension clearances, renewals and other transaction types, to evaluate the effectiveness of current practices and to identify opportunities for improvement.

By following this comprehensive approach, we aimed to understand and recognize what is operating well, what has been improved based on the actions identified in the *After-Action Plan*,

and to identify the root causes of data integrity issues. Deloitte developed actionable options for ODOT to consider that may enhance the integrity of the data managed by Oregon DMV.

Observations, Actions, and Business Rationales

As part of the initial assessment, Deloitte offers observations across many of the areas reviewed, and the observations predominantly relate to themes of data management, automation, extraction, quality, analytics, governance, internal controls, resources, and training. The observations provide an account of the current situation in each area reviewed and are aligned to the PPT model described in the Executive Summary. By documenting these observations, the report offers a basis upon which further analysis can occur. This summary also allows stakeholders to have an aligned understanding of the existing conditions, which is crucial for ODOT/DMV's informed decision-making around potential future changes to resources, systems and processes.

The actions presented and accompanying business rationales serve to translate the observations into actionable steps that can drive improvement and address identified issues or gaps. Actions are articulated to be practical and achievable, providing clear guidance on how to enhance processes, mitigate risks, or capitalize on opportunities. The business rationales accompanying each action explain the underlying reasons and expected benefits, linking the proposed actions to strategic business outcomes. This helps stakeholders understand not only what needs to be done but also why it is important.

Obs #	Predicate #	Topic
1	N/A	Integrated Data Governance
Observation		
A history of collaboration exists between ODOT and DMV regarding data governance, a strategic enabler of achieving data integrity. This collaboration has included designating an ODOT Chief Data Officer and further designating data trustees and stewards throughout the ODOT/DMV ecosystem. Additionally, DMV has driven a strategic initiative for Enhanced Data Management and is collaborating with ODOT on an Enhanced Data Management Strategy Implementation. Even with the progress, there remain opportunities for further enhancing of collaboration with respect to data governance. It is a widely held view within ODOT/DMV that DMV (as well as other divisions within ODOT) operate in a predominantly independent manner with respect to data governance. However, ODOT and DMV aim to facilitate better communication and coordination with the understanding that achieving integrated data governance is crucial for enhancing operational efficiency and decision-making processes. Additionally, integrated data governance can aid in ensuring data across these entities are accurate, consistent, and secure. As ODOT and DMV continue to advance along the data governance maturity spectrum, it is essential to maintain momentum and build upon the established framework.		

Action

ODOT/DMV can consider opportunities to continue advancing integration and synergies between ODOT and DMV with respect to data governance. Achieving consensus on a common data governance framework and fully operationalizing that framework should be the priority. An additional emphasis can be offered to doing an inventory of data governance internal control documentations such as data flow diagrams (DFDs), and entity relationship diagrams (ERDs) to understand gaps in conventional data governance documents and to create new ones as needed. Having proper documentation will allow for transparency, continuity, and consistency between ODOT and DMV. Lastly, another crucial aspect can be placed on creating new capabilities relating to data management, data availability, data analytics, and control over enterprise data.

People

Appropriate data professionals, with the requisite skills, within ODOT and DMV can be identified to drive the collaboration and integrated approach to data governance. Roles and decision rights within the integrated data governance team should be defined.

Process

An integrated data governance framework can be developed so ODOT/DMV will collaborate, interoperate, and manage the data under its collective control. The framework should define the methods and standards for how ODOT/DMV governs its data in a consistent, sustainable way.

Technology

Depending on the specific elements of the integrated data governance framework, ODOT/DMV may require additional technologies to operationalize the framework. Examples could include technologies that facilitate the creation of a data lake (or enhancing current data warehouses, as applicable), technologies that support the documentation and operations of data flows, data entity relationships, data dictionaries, or controls over data, or other technologies that would assist ODOT/DMV in modernizing and integrating data governance.

Business Rationale

Developing and operationalizing an integrated data governance framework would provide for synergies and efficiencies in a wide variety of data management processes across the ODOT/DMV ecosystem. More specifically, having common processes in data management and oversight of enterprise data would provide for reduced error rates, higher innovation levels, clearer pathways to data availability, simplified decision-making, and would generally contribute to an environment where enhanced data integrity levels are easier to achieve and sustain. Finally, while divisions outside DMV are beyond the scope of this report to address, it warrants mentioning that an integrated data governance framework would likely create benefits between ODOT and its other departmental divisions, in addition to DMV.

Obs #	Predicate #	Topic
2	14	Automation of Identity and Voter Eligibility Documentation Verification

Observation

DMV has implemented measures, including some manual procedures associated with secondary and tertiary reviews of field operations transactions, to reduce historical errors and achieve the required level of assurance for data integrity with respect to identity verification and voter registration eligibility. While these measures appear adequate for the near term, some are taxing on field operations personnel and likely reduce the timeliness and quality of customer service. Additionally, questions exist within DMV regarding how sustainable these measures are over the long term.

Action

ODOT/DMV may consider opportunities to implement process automation or other advanced technologies to automate the analysis and verification of authenticating documents of DMV customers.

People

DMV field operations personnel can be trained in the operations of the proposed technology. Early in the lifecycle of the technology, an emphasis should be placed on field personnel validating the verification decisions of the technology based on their functional expertise. Efforts can also be invested to ensure that teams' functional expertise is sustained over time.

Process

Field operations processes and transaction flows for identity validation may be adjusted to accommodate the use of a proposed technology. This implementation may include simplification of existing manual review processes, including possible elimination of Form173DP. That said, in instances where field personnel detect errors in the decisions of the technology, alternative manual processes should be available to meet operational needs and provide data integrity.

Technology

ODOT/DMV can explore options for developing and deploying automation to replicate the currently human-driven processes for how customer identity is verified, and voter eligibility is validated. For example, automation could be used to enable intelligent optical character recognition (OCR) to extract key data elements from identity documents to reduce manual data input, and the error rate that is so often a result of manual data entry. Because OCR technologies are not 100% accurate, a visual validation of OCR extractions may be required as a change to the business process.

Business Rationale

Based on all currently available information and data, it appears the recent process adjustments that DMV has implemented have addressed the data integrity issues that led to the historical errors in voter eligibility data. That said, these processes are the result of measures that are somewhat manually driven and some of the processes continue to be very taxing on field operations personnel. As a result, these measures may not be sustainable over the long term. Automation or other advanced technologies could replicate these manually driven measures and sustain data integrity in a reliable manner, and reduce pressures on field operations personnel, without jeopardizing other aspects of field operations.

Obs #	Predicate #	Topic
3	1	Integrated Data Analytics Capability

Observation

While ODOT and DMV currently have teams of data management professionals, there is not currently an integrated data analytics capability with the ODOT/DMV ecosystem. Additionally, there exists within the ODOT/DMV ecosystem a backlog of needs relative to reporting and monitoring.

Action

ODOT/DMV can consider building an integrated data analytics team, with a focus on enabling that team to strategically develop solutions that address a range of operational challenges. Examples of areas where a dedicated team could support DMV objectives include exploratory data analytics and innovation, fraud prevention, internal control and monitoring, data-driven decision making, and other areas of operations that relate to data integrity.

People

Appropriate data professionals with the ODOT/DMV can be identified to populate and lead the integrated data analytics capability. This could entail redeploying existing data management professionals within ODOT/DMV, and/or it could involve allocating budget for new human resources. Depending on the details of the roles determined for this capability, a review of job descriptions and job classification could also be appropriate. Finally, careful consideration should be given to the organizational placement of the team (i.e., ODOT or DMV levels). A hybrid-federated model may ultimately be most effective, where a small core team is deployed at the ODOT level, and a supporting, federated team is deployed at the DMV level.

Process

A variety of processes can be instituted to operationalize the integrated analytics capability. Relative to data integrity, the project in-take and prioritization processes should receive focus. Understanding that there is a backlog of needs relative to reporting and monitoring, prioritizing that backlog for support will be key to the success and effectiveness of the integrated analytics team.

Technology

The integrated analytics team can be enabled with technologies that allow it to deliver on ODOT/DMV needs. See observation #5 for an additional perspective.

Business Rationale

An integrated data analytics capability would allow ODOT/DMV to focus strategically on currently under-served or unserved data analysis and reporting needs that exist throughout the ODOT/DMV ecosystem, including those relating to data integrity. Deploying the team in a hybrid-federated model would contribute to the strategic management and prioritization of projects, while fostering functionally specific expertise within DMV.

Obs #	Predicate #	Topic
4	N/A	OLIVR Data Extraction Capability

Observation

It is reported by multiple teams within DMV that standard reporting from OLIVR is sometimes insufficient to manage DMV functional processes. In certain instances, concerns have been raised regarding the availability of standard OLIVR reporting. Additionally, it is widely acknowledged that OLIVR either does not permit or does not easily facilitate the extraction of back-end data directly from its underlying database tables. OLIVR offers thousands of standard reports, and it is estimated that half are not used. Collectively, this presents a situation where many DMV professionals assert that they do not have access to the data and reporting that they need it to effectively manage DMV processes. It was communicated that this situation has directly and substantially contributed to data integrity challenges experienced by DMV.

Action

DMV can consider developing a technological mechanism for allowing the export of data from the OLIVR back-end database environment. The mechanism could be deployed in such a manner as to allow for the user-directed export of data, or it could be deployed in a manner such that it was system-operated and automated, allowing for the preprogrammed export of selected bodies of data in a more controlled manner.

People

Once the OLIVR data extraction mechanism is operational, ODOT/DMV technical and/or functional personnel may require training and guidance on its appropriate use. Depending on the methods of export allowed (i.e., user-directed and/or system-operated), additional policies and procedures may require development to address the topics of data loss prevention, appropriate data use, data exfiltration, data privacy, data ownership and other relevant topics.

Process

The process-related implications of a user-directed data extraction mechanism are difficult to fully articulate as those implications depend upon which users extract which data in support of which functional processes for what purposes. The downstream process implications may require consideration upon each new instance of data being extracted and used. Under a system-operated data extraction mechanism, there are additional process related implications that relate primarily to the technical teams responsible for the scheduling and operation of the mechanism.

Technology

To successfully develop and deploy a data extraction mechanism for OLIVR, ODOT/DMV may need to dedicate the appropriate technical resources to allow for the development of the technology. This could include assigning internal resources or procuring support from an external vendor. ODOT/DMV may also consider searching its network of state agency relationships. We are aware of DMV teams in other states that have successfully developed data extraction mechanisms for the COTS platform upon which OLIVR is based, and shared learnings may be available for ODOT/DMV to consider from other state DMV agencies. Finally, there is the question of what environments/platforms to which ODOT/DMV would allow its data to be exported. See observation #5 for additional perspective on this factor.

Business Rationale

It is conventionally accepted that functional users of systems will have needs that evolve over time, as operating environments change. This reality can create difficulties when functional users are not provided with the reporting they require, as the evolution in needs occurs. Many organizations account for this need by allowing back-end data extraction from systems of record, which users can analyze to fulfill their own information and reporting needs. While this can introduce operating risks relating to data leakage, those risks can be mitigated effectively under the right management and internal control regimen. Furthermore, when a data extraction mechanism is deployed in conjunction with a controlled data analytics environment, those risks become much easier to mitigate. While the specific types of data and their sensitivities must be considered in any decision to allow for back-end data extraction, when done responsibly, it is widely regarded as accretive to user needs being met and to data integrity being enhanced.

Obs #	Predicate #	Topic
5	1, 3, 4	Exploratory Data Analytics Environment

Observation

DMV currently only has the foundational elements of, or not fully developed data management environment that replicates the content of its operational system of record, OLIVR. This creates a situation where users must obtain the data and information needed to manage DMV operations directly from OLIVR. Deloitte observed multiple instances where functional users claimed that there are limited or no data extraction capabilities easily available in OLIVR, and in some instances, the reports are not extracted appropriately. This limits user self-service and business unit tailored data extraction, resulting in a moderate to elevated risk of users not having the data and information available that is needed to maintain data integrity.

Action

ODOT/DMV can consider developing or expanding upon its current exploratory data analytics environment (i.e., a business intelligence solution), such as a data lake or other environment, that hosts data from throughout ODOT and DMV. While the data from the OLIVR system should be the initial focus of the environment, other data from other systems within ODOT/DMV could be added over time to realize more value from the solution.

People

Technical operations personnel may be required to deploy and operate the exploratory data analytics environment. Those personnel could be sourced from internal staff, recruited

externally, or procured through a third-party service provider. Additional personnel would be required to develop and report on the data analytics. These personnel would likely align to the integrated data analytics team referenced in observation #3.

Process

System maintenance and support processes may need to be deployed as part of developing an exploratory data analytics environment. These processes likely already exist within ODOT/DMV and would only need to be extended to include the proposed environment.

Technology

Significant factors relating to technology are involved in deploying an exploratory data analytics environment. First, it is likely that this environment would be deployed on some form of cloud architecture. Given the sensitivity of the data involved, ODOT/DMV can consider a private cloud architecture (versus a multi-tenant solution). Next, there is a variety of software components that would need to be included in the solution. ODOT/DMV can perform a technical evaluation of such components, including options for data visualization software, data management software, code development platforms, report development platforms, AI engines, robotic process automation engines, scheduling systems, security management systems, data loss prevention solutions, and others. Based on the results of the evaluation, a business intelligence solution architecture and strategy should be documented to serve as a basis for building out the environment.

Business Rationale

Within ODOT/DMV, it is a widely held view that opportunities exist to take a more strategic approach to analytics and the development of operational/business insights. A key component to that effort would be having a supporting platform that would allow ODOT/DMV to analyze data, innovate and create knowledge without having to be constrained by the operational requirements of the primary DMV production system, OLIVR. Deploying an exploratory data analytics environment would significantly advance ODOT/DMV's ability to monitor, measure, sustain, and advance data integrity, among many other benefits the environment would provide.

Obs #	Predicate #	Topic
6	N/A	Enhanced Data Edit Checks in OLIVR

Observation

Substantial enhancements have been made to OLIVR since the identification of the voter registration issues that precipitated the current projects relating to data integrity at DMV. Among these enhancements to the system are user interface object behavior changes and field level data edit checks performed by the OLIVR application. While these enhancements have contributed to improving data integrity at DMV, there appear to be additional opportunities for exploiting data integrity value from OLIVR by making additional enhancements. As one example, it was observed during transaction walkthroughs that in OLIVR, if a customer was to submit an identity document that would cast doubt on a previous DMV transaction (e.g., if a customer who is noted as a US citizen in OLIVR was to present a current foreign passport), OLIVR would not necessarily compel the DMV service

representative to require the customer to reauthenticate citizenship status, depending on the type of transaction the customer was attempting.

Action

DMV can consider performing an evaluation of the OLIVR transaction types and the operational process steps associated with its various transaction types. The focus of the evaluation can be in identifying additional object behavior and edit check enhancement that would help ensure data integrity.

People

In order to perform the recommended evaluation of OLIVR, skilled service representatives who are deeply familiar with all of the DMV transaction types and associated process steps can be consulted.

Process

Based on the opportunities identified in the proposed evaluation, DMV can adjust the service representative process steps associated with the selected transaction types. This may require a keystroke-level analysis of service representatives with respect to how they currently and prospectively operate OLIVR.

Technology

Based on the opportunities identified in the proposed evaluation, DMV can update OLIVR to align to the system object behaviors and enhanced process steps for the selected transaction types. This may require consultation with the COTS vendor who provides the OLIVR solution to determine if the system is feasible to this change.

Business Rationale

As DMV has already observed with the enhancements implemented in OLIVR, small adjustments to system object behaviors and process steps can drive significant improvements in system operations, driving error rates lower and improving data integrity. Additional enhancements to OLIVR would build upon the successes already achieved and provide further data integrity value.

Obs #	Predicate #	Topic
7	N/A	DMV Human Capital Levels

Observation

Upon initial observation, it seems that DMV staffing levels, relative to the scope of services provided and scale of population served, do not appear to align with other motor vehicle service agencies offering similar services. The constrained staffing levels have caused some ODOT/DMV personnel to raise questions regarding the impact of relatively lower staffing levels on DMV's data integrity.

Action

DMV can consider performing an objective benchmarking and data-driven evaluation of DMV human capital levels. This is a staffing level study that focuses on assessing workload by process and assigned resources and then compares those results with peer agencies in other

jurisdictions to assess the appropriateness of overall headcount levels. Headcount reallocations within DMV functional units can also be considered in the evaluation.

People

DMV management personnel can be involved in interviews over the course of the evaluation. An emphasis should be placed on understanding workload balancing, backlog, and challenges associated with the functional units evaluated.

Process

In staffing level analyses, organizations sometimes engage in process improvements or other transformations during the course of the evaluation. DMV can focus on assessing its staffing levels based on any prospective, updated process definitions, resource allocation metrics, industry standards or best practices, and common key performance indicators (KPIs).

Technology

Similar to process improvements, in staffing level analyses, sometimes organizations identify and implement technology transformations to improve processes or optimize them for efficiency. DMV can focus on assessing its staffing levels based on any prospective technological enhancements.

Business Rationale

The concept of data integrity is linked to the real impact of human capital levels. When organizations are under-resourced, processes become difficult to sustain, and data integrity is no different. While anecdotal evidence suggests that staffing levels do not align or peer with those of other motor vehicle agencies of similar scale and scope, it is important to make important staffing level decisions from a posture of an informed, data-driven evaluation. It is also important to perform the evaluation in the context of future state processes and systems. This will help ensure that the evaluation is commensurate to the intended, prospective processes of DMV. By achieving appropriately resourced human capital levels, DMV would contribute meaningfully to the objective of sustaining adequate data integrity.

Obs #	Predicate #	Topic
8	N/A	Customer Service Positions Assessment

Observation

Within DMV, there is a commonly held view that many DMV service positions are under-classified and under-compensated. The belief is that this situation has contributed to the turnover level associated with service representatives, which currently is approximately 20%. It has also been noted that the turnover level has contributed to DMV having less experienced staff, which has been linked to some historical data integrity challenges. The turnover issue is most acutely experienced among employees in the one-to-five-year range of tenure. Additionally, as processes and technology have evolved over time, there are concerns that the required skills for the customer service positions should be updated, including potential position classification and compensation updates.

Action

DMV can consider performing an assessment of its customer service positions, including those associated with the Call Center and with DMV field operations. An emphasis can be

placed on assessing the appropriate position skills requirements, position classification, and compensation levels. Special consideration should be given to considering position classification adjustments that would support DMV in retaining experienced talent over the long term.

People

DMV management personnel can be involved in interviews over the course of the position assessment. The assessment can be performed by qualified Human Resource (HR) professionals with experience in assessing position classification, required skills, and compensation levels.

Process

During the proposed assessment, steps can be taken to ensure that the full scope of customer service processes are included in the scope. This includes both legacy and any new processes that may be implemented as a result of ongoing efforts.

Technology

DMV can consider the impact of current and prospective technology enablement in the course of the proposed assessment. In some cases, such as when technology is sufficiently intelligent and automated, position complexity and skills requirements can be lowered. In other cases, technology operations can require higher level skills for successful execution to occur. The assessment can be conducted in the context of how technology supports customer service positions.

Business Rationale

Customer service representatives are the employees who sit closest to DMV's data, and they have the most direct impact on DMV's overall data integrity. The historical data integrity challenges relating to voter registration eligibility were directly driven by errors associated with customer service operations. This fact demonstrates the clear link between appropriately skilled service representatives and data integrity. DMV can perform an assessment of service representative positions and make any appropriate updates to position classification, required skills, and compensation levels would likely contribute to reducing turnover and enhancing DMV's capacity for sustaining data integrity.

Obs #	Predicate #	Topic
9	N/A	Human Capital Development

Observation

DMV currently supports a thorough customer service representative training program that involves a blend of module-based self-study, classroom facilitated training, and on-the-job training. However, concerns about the adequacy regarding the level of resources allocated to other areas of training may have a direct effect on data integrity.

Action

DMV can consider performing an assessment of its training function, with an emphasis on determining whether adequate resources have been allocated to training curricula development and training delivery. Consideration should also be given to the evolving capabilities of DMV and whether training programs fully accommodate the deployment of

current and prospective technologies. Additional consideration should be given to promoting awareness among DMV personnel regarding the critical importance of sustaining data integrity in operations. In the event the assessment reveals that training resources have not been sufficiently allocated to DMV, steps can be taken to correct the situation. Specific areas of training focus can be articulated for elaboration and implementation of training content.

People

DMV can consider conducting a survey of its human capital with a focus on understanding employee sentiment as it relates to the sufficiency of training provided within the DMV. Consideration should also be given to the option of cross-referencing survey results with employee performance outcomes relating to data integrity, with the intent of identifying data points that corroborate the need for increased training capabilities.

Process

Where training needs are identified, DMV can engage internal and/or training development resources in a project to modernize and enhance training for DMV human capital, with a focus on curricula that relates to data integrity. A mix of training modes should be considered, including classroom, self-study, on-the-job and technology facilitated.

Technology

Over the course of performing the suggested assessment, it may be appropriate for DMV to make available certain technological capabilities in support of the assessment, such as an online survey mechanism. Consideration should be given to factors such as the distribution of survey recipients, survey content, privacy, completion rates, and other factors.

Business Rationale

Human capital development is critical to the health of any enterprise, and it is a significant contributor to the achievement and sustainment of data integrity. By evaluating and supporting its training needs, DMV would increase its capacity for ensuring adequate data integrity levels and mitigate the risk associated with historical gaps in data integrity.

Obs #	Predicate #	Topic
10	4 or 5	Fraud Risk Management Reporting

Observation

DMV's fraud unit expressed a lack of confidence in the availability and extractability of standard reports in OLIVR to support fraud risk management. This creates a situation where the fraud unit's ability to reliably and proactively identify fraud and investigate leads is constrained. This, in turn, contributes to a diminished capacity for data integrity at DMV.

Action

ODOT/DMV can consider providing the fraud unit with the ability to obtain the data it needs from OLIVR to confidently perform fraud risk management. This includes providing a mechanism for extracting data from OLIVR and providing the necessary data analytics capability to assess that data.

People

Currently, it appears that the DMV fraud unit has the human capital required to perform limited fraud risk management functions. However, due to a lack of tools to proactively monitor transactions for irregularities and inadequate access to effective reporting, the unit is unable to further advance work towards greater lead generation and investigation. Consequently, this prevents the team from running and implementing proper fraud risk management analytics. Furthermore, use of analytics and greater access to reporting may generate a backlog of leads, including previously uncovered leads. Depending on the extent of leads identified by implementing improved fraud risk management processes, additional resources, particularly skilled in analytics, may be required for the fraud unit.

Process

Currently, it appears that the DMV fraud unit is limited in its ability to conduct fraud risk management processes to perform lead generation and lead investigations. Depending on the extent of leads identified by implementing improved fraud risk management analytics, DMV should consider whether updates are needed to its overall fraud risk assessment processes and its portfolio of identified fraud risks. Fraud risks evolve rapidly, and DMV should consider opportunities to implement process changes to meet those evolving threats, particularly with analytics.

Technology

In order to support DMV's fraud unit in developing analytics it is confident in, a mechanism will be required to extract data from OLIVR (i.e., see observation #4). Beyond the data extraction mechanism, the ability of the fraud unit to perform analytics would be substantially accelerated by having access to an exploratory data analytics environment (i.e., see observation #5).

Business Rationale

The DMV fraud unit's view on the availability of OLIVR's standard reporting is not isolated, as other units within DMV share it. The role of the fraud unit is particularly important in maintaining the integrity of DMV data. In the broader motor vehicle association professional community (i.e., nationally and internationally), reports of fraud have become rife. This is particularly true with respect to identity fraud, and it's been particularly true since the period of the Pandemic. The reality is that the risks of fraud committed against government agencies have never been higher, and DMV's fraud unit should be enabled with the tools and data required to effectively deliver on its mission space.

Obs #	Predicate #	Topic
11	1, 3	Data Integrity Risk Management and Prioritization

Observation

While DMV exercises care and attention to detail in the management of its data and considers the impact of its decisions on operations, it does not currently appear to have a mature and consistently executed method for performing risk management with respect to data integrity. Furthermore, the process of setting priorities, dedicating resources, and launching projects relating to data integrity is semi-formal or informal, and often reactive. This results in a situation where data integrity risks are not proactively managed and issues are not prevented, but rather they are contended with only after causing operational challenges.

Action

DMV can consider options for implementing a proactive regimen for performing risk management relating to data integrity. An additional emphasis can be placed on formalizing how DMV sets priorities and allocates resources to prevent data integrity risks from manifesting. This can include efforts in establishing a 'monitor, review, and assess' process for maintaining acceptable levels of situational awareness with respect to emerging data integrity issues. Finally, consideration can be given to both data assets and the systems that house them in defining a comprehensive risk management regimen.

People

The recommended risk management regimen can include participation by a defined group of DMV leaders, supported by a specific cadre of functional resources who execute the prescribed risk management activities. Decision rights and responsibilities should be clearly defined and documented.

Process

Risk management processes can be defined, including the specification of task ownership and schedule of related activities. Checkpoints can be set for data integrity measurements to occur, and DMV leadership can be appropriately updated on the periodic findings and activities of risk management processes. In addition, the National Institute of Standards and Technology (NIST) has a Risk Management Framework that provides a structured approach to managing risk, including measures for data integrity specific controls. Using this type of framework could provide ODOT/DMV with the assurance that they are effectively managing risks to data integrity in compliance with national standards.

Technology

Consideration should be given to the deployment of risk management technologies, such as the Governance, Risk and Compliance (GRC) technology. GRC technology provides a structured mechanism to enable the most common workflows and reporting associated with risk management. Existing technology owned or licensed by ODOT/DMV may provide suitable options.

Business Rationale

Risk management, as a discipline, provides a structured and deliberate approach for organizations to proactively identify and mitigate risks. Additionally, when risks manifest and become active threats, formalized risk management enhances the agility with which organizations identify, respond to, and resolve those threats. As it relates to data, implementing risk management processes or expanding existing ones would contribute meaningfully to the achievement and sustainment of adequate levels of data integrity.

Obs #	Predicate #	Topic
12	N/A	Know Your Customer (KYC) Systems and Procedures

Observation

DMV's current KYC processes in the call center and field offices require minimal information and reflect an area for potential improvement. In most observations conducted, a DMV customer needed to know only basic information of a subject to conduct changes to DMV

data or engage in most other transactions. Especially when transactions are conducted with the call center over the phone, this approach to KYC poses meaningful risks. While it may be that the current procedures are proportional to the risks associated with DMV use of its data, the reality is that DMV serves as a trusted source of identity for a wide portion of society. Other government agencies, law enforcement, the healthcare community, financial institutions, and countless private companies rely on the integrity of DMV-issued identity documents, and it may be that the current KYC procedures are not proportional to the risks associated with those broader use cases.

Action

DMV can consider performing a risk assessment related to the variety of identity documents that it issues. A focus can be offered to understanding the potential impacts of DMV customer data being inappropriately accessed or altered, due to DMV's current KYC procedures. The risk assessment can consider the context of internal DMV and external use cases associated with broader society. If it is determined that KYC procedures are not sufficient, given the risks identified, DMV can consider updating its KYC procedures to enhance their level of rigor. Additionally, DMV can consider deployment of an identity proofing technology solution to augment existing and prospective updated procedures. The overall enhanced KYC processes should be commensurate with the risk levels identified in the suggested risk assessment.

People

In potentially updating its KYC procedures, DMV can consider the impact on its customer community and the adoption capability of that community. It may become necessary for DMV to engage in enhanced customer service or surge-support activities to support the transition to enhanced KYC procedures. This may result in a need for increased call center personnel as well as increased field service representatives.

Process

Based on the results of the recommended risk assessment, KYC procedures would likely need to be updated to require more identify proofing information from DMV customers in order to conduct DMV transactions. Ideally, the extent of information required for identity proofing should be proportionate with the risks of the transactions being attempted while adhering to relevant federal and state regulations, such as the Driver's Privacy Protection Act (DPPS) and other data protection laws.

Technology

In the event DMV deems it necessary to deploy an identity proofing technology solution, DMV can engage in an initiative to define system requirements for that solution in accordance with the findings described in Observation 14. Furthermore, an evaluation of leading COTS solutions can be conducted, where each solution is compared to the requirements identified. DMV can engage in a procurement to acquire, implement, and operate the solution, consistent with its information technology lifecycle processes.

Business Rationale

Data integrity is rooted in the accuracy of transactions that affect that data, processing tasks that manipulate data, the people who have access to those data after acquisition, as well as

the ability of a party to obtain an identity document. To have confidence in data quality, DMV must have assurance that the party with whom it is transacting is truly the subject of the transaction. More sophisticated KYC procedures, including identity proofing technology, would contribute significantly to modernizing DMV's capability in this area. It would also reduce risks to the DMV, its customers, other government agencies and the broader community by more rigorously ensuring the sustainment of data integrity.

Obs #	Predicate #	Topic
13	5	Data Transmission Reconciliation Controls

Observation

DMV engages extensively in data interchange with many parties. In some cases, DMV is the recipient of data (e.g., Courts, vital records, law enforcement), and in other cases it is the transmitter of data to other parties (e.g., Secretary of State). The significance of maintaining data integrity is evident in several historical challenges faced by the DMV. A notable example includes issues associated with the reversal of the suspension of driving privileges. While foundational internal controls over data interchange appear to be in place, many opportunities exist to improve upon the extent and nature of these controls as to further enhance data integrity, and/or opportunities exist to renegotiate the scope and content of data transmissions with data exchange partners (e.g., Courts) as to facilitate higher levels of internal control. Furthermore, opportunities exist to improve the completeness and accuracy of the catalogue of data interchange interfaces that DMV maintains.

Action

ODOT/DMV can consider enhancing its data transmission reconciliation controls, with an emphasis on the completeness, accuracy, and timeliness aspects of the internal controls. For all practical purposes, automation of these controls is the only viable method of realistically deploying them, and therefore this recommendation is presented in that context. The effort can begin with a thorough update to the data interchange interface catalogue. Once the data interchange interfaces are catalogued fully, internal controls should be defined such that, on an automated basis, the completeness, accuracy, and timeliness of each individual data transmission is tested and monitored, thus enhancing data validation routines. For example, this could include record count reconciliation controls to support completeness assurance, hash total reconciliation controls to support accuracy assurance, and/or timestamp versus schedule comparisons to support timeliness assurance. Designing and implementing these controls may likely require collaboration with ODOT/DMV's data exchange partners, to include the possibility of redefining the data transmission file contents as to allow for improved levels of internal control and reconciliation. Once deployed, the data transmission reconciliation controls should be operated and monitored consistently, and exceptions observed in operations should be researched and resolved.

People

Data trustees and stewards can be consulted in updating the catalogue of data interchange interfaces that DMV supports. A general description of the functional purpose of each interface should be included. The directional alignment (i.e., receive, transmit, both) of each interface should be noted, along with a data dictionary of the data elements involved. Format

specifications for each data field can also be included in the catalogue. Other metadata, as deemed necessary by ODOT/DMV policy or guidance, should also be included. ODOT/DMV data trustees and data stewards can collaborate with qualified internal control professionals (e.g., IT auditors, risk management professionals, etc.) in the design and implementation of the data transmission reconciliation controls. Additionally, data trustees and stewards can be assigned responsibility for collaborating with data trading partners in researching and resolving any exceptions noted to data interchange reconciliation.

Process

Once the data interchange interfaces are catalogued fully and automated controls are implemented, resolution procedures can be developed that provide guidance on how exceptions are resolved. The design and effectiveness of the reconciliation controls should also be periodically tested, both by ODOT/DMV management and by a qualified auditor. Both the automated processes and the manual resolution aspects of the controls should be periodically evaluated. Additionally, procedures can be put into place to ensure the ongoing maintenance of the data interchange interface catalogue. The completeness, accuracy and timeliness of updates to the catalogue can also be periodically evaluated by both ODOT/DMV management and by a qualified auditor. Finally, it warrants mention that it is possible that data transmission errors can originate from outside ODOT/DMV, and resolving such errors may require elevated levels of collaboration with data exchange partners.

Technology

The technology aspect of deploying data transmission reconciliation controls involves codifying the controls and deploying them through automation. Of particular importance is to deploy the controls at the individual data transmission level, so that every instance of a data transmission is evaluated for completeness, accuracy and timeliness. The simplest option is likely to deploy the controls in the exploratory data analytics environment proposed in observation #5.

Business Rationale

Data interchange is a key aspect of ODOT/DMV operations. Data exchange partners rely extensively on DMV data and its integrity, and data interchange therefore is of critical importance in maintaining the integrity of DMV data. Enhancing data transmission reconciliation controls would help DMV achieve higher levels of assurance regarding data integrity, and it would help DMV ensure its posture as a reliable exchange partner for other parties. Additionally, adjusting the schedule of data transmissions may allow DMV more time to ensure adequate data integrity levels are achieved, prior to transmission.

Obs #	Predicate #	Topic
14	N/A	Policy Analysis

Observation

Oregon law permits the DMV to electronically scan and retain identity verification documentation for the issuance of Real IDs. Currently, DMV does not electronically scan identity verification documentation for non-Real ID issuances. In such cases of non-Real ID issuances, the DMV relies on a manual inspection process conducted by field operations personnel. This manual process involves inspecting and recording identity verification

documentation, which has, at times, resulted in data integrity issues; including those related to voter eligibility. The reliance on manual procedures for non-Real ID transactions introduces a higher risk of human error, which can compromise the accuracy of voter eligibility records and undermine public trust.

Action

ODOT/DMV can consider reviewing relevant statues and guidance with a specific focus on evaluating opportunities to improve DMV operational efficiency. This will help DMV understand the extent to which it can incorporate modern technologies to enhance data integrity in the future.

People

ODOT/DMV can engage key stakeholder staff to lead and conduct the policy and guidance analysis. ODOT/DMV can further consider which personnel should receive the analysis.

Process

DMV can evaluate and then document the results of their review in a position paper, including an analysis of potential opportunities to enhance data integrity through an agreed upon strategy leveraging technology. ODOT/DMV leadership can evaluate the conclusions of the analysis and determine the most effective steps available and decide upon those for immediate and then long-term implementation. Once those steps are identified, ODOT/DMV can explore opportunities to implement more efficient and effective automation solutions, including an additional comprehensive review of the applicable statutes, administrative rules, and policies that govern these practices.

Technology

The position paper produced from this activity can be stored within ODOT/DMV's environment, making it accessible to relevant personnel. Additionally, ODOT/DMV should consider whether certain parts of the position paper should be shared with other Oregon state government agencies or the general public.

Business Rationale

Depending on the results of the analysis, there may be additional opportunities for DMV to take advantage of modern technologies, such as automation, in a manner as to enhance data integrity while still complying with related law. Additionally, notably important is that these technological possibilities should only be developed from a posture of compliance against applicable guidance and requirements; to remain within the direction and boundaries of DMV policies in exploring advanced technology opportunities relating to data integrity.

Summary and Suggested Next Steps

To deliver a Final Review Report, Deloitte intends to use the Preliminary Review Report to validate the initial findings with ODOT/DMV personnel. This step is crucial to ensure that our observations accurately reflect the current state of data integrity and align with the operational realities of DMV and the expectations of its stakeholders. As a result of the validation, and continued conversations with ODOT/DMV stakeholders in Phase 2, we will include in the Final Review Report actionable timelines (short and long term) for completion that corresponds to each observation and recommended action.

Following this validation, we will elaborate on our observations and actions by providing additional details and context. This will include expanding the business rationale with further data and information citations to underscore a data-driven intent. By doing so, we aim to further enhance the substance and value of our proposed options for improvement. This comprehensive approach provides options for ODOT/DMV to consider that are well-supported, actionable, and aligned with the strategic objectives of ODOT/DMV, providing a framework for future data integrity initiatives.

In terms of DMV's request to evaluate the current measures instituted to mitigate additional risks associated with Oregon Motor Voter data transfers to the Secretary of State, as noted in the executive summary, we believe the recently enhanced systemic and manual measures provide adequate levels of assurance that data integrity within OLIVR is sufficient to reinstitute the process. Our view is qualified on the condition that DMV sustains the systemic measures, continues to validate the data files (i.e., which are composed of data exported from OLIVR) transmitted to the Secretary of State for completeness, accuracy and timeliness, and existing manual measures recently implemented be continued and monitored. Deloitte also believes the measures currently in place, absent additional automation, could pose risks in the context of a long-term solution.

Appendices

Appendix 1: Definition of Key Terms

American Association of Motor Vehicle Administrators (AAMVA) - is a non-profit organization that develops model programs in motor vehicle administration, law enforcement, and highway safety. AAMVA's mission is to support and serve its members—state, provincial, and territorial officials in the United States and Canada—by providing expertise, tools, and resources to enhance the effectiveness and efficiency of motor vehicle and law enforcement agencies.

Business Data Glossary - a business glossary contains metadata that assigns meaning or semantic context to data. A business glossary is usually an artifact produced by a data governance initiative and is most often controlled by the business not the database administrators.

Critical Data Elements (CDE) - a data element that is determined to be vital to the successful operation of the organization (Loshin, David (2009). Master Data Management. The MK/OMG Press). CDEs include the data elements that represent identifying information of master data, the elements that are critical for a decision-making process, or the elements that are used for measuring organizational performance.

Data Currency - refers to the timeliness and relevance of data, indicating how up-to-date the information is at any given moment. It ensures that the data being used for decision-making and analysis reflects the most current state of the real-world events or conditions it represents.

Data Dictionary - a centralized repository that provides detailed information about data elements, including their definitions, formats, relationships, and usage within an organization. It ensures consistency, standardization, and validation of data, thereby supporting data integrity and quality across various systems and processes.

Data Flow Diagram (DFD) - is a graphical representation that depicts the flow of data within and through business processes, illustrating how data is processed, stored, and communicated between different components, procedures, and external entities.

Data Governance - execution and enforcement of authority over management of data, which should be sustainable, embedded, and measured. Data governance touches all aspects across the enterprise.

Data Integrity - encompasses the principles of data quality and security, ensuring the accuracy and consistency of data throughout its lifecycle, from creation and storage to retrieval and deletion. By implementing rules and standards, it prevents unauthorized modifications and guarantees that data remains correct and accessible while being protected against tampering. Maintaining data integrity is crucial for organizations, as it ensures that information used for decision-making, reporting, and compliance is accurate and reliable, thereby supporting operational efficiency and regulatory adherence.

Data Lakehouse - is a modern data architecture that creates a single platform by combining the key benefits of data lakes (large repositories of raw structured and unstructured data in its original form) and with the data management and transactional capabilities of data warehouses (organized sets of structured data). This hybrid model allows for efficient data processing and analytics by supporting both structured and unstructured data within a unified platform.

Data Latency - is the delay between the occurrence of an event and the point at which the data representing that event is available for use in a system or application. It is a critical factor in data processing and analytics, impacting the timeliness and relevance of information.

Data Quality - degree to which data conforms to business definitions and business requirements and is generally considered high quality if it is "fit for [its] intended uses in operations, decision making and planning. Data quality is defined as the degree to which data meets a company’s expectations of accuracy, validity, completeness, and consistency (SAS).

Data Stewards - are individuals responsible for ensuring the quality and fitness for purpose of the organization's data assets, including the metadata for those data assets, accessibility, release, appropriate use, security, and management of data. A data steward also participates in the development and implementation of data assets. A data steward seeks to improve the quality and fitness for the purpose of data assets their organization depends upon, including making disparate data assets interoperable.

Data Trustees - managerial authorities who approve and grant access.

Entity Relationship Diagram (ERD) - visual representation of how data elements in a database relate to each other.

Federal Standards - Federal standards encompass regulations such as the Real ID Act, commercial driver's license (CDL) requirements, vehicle safety standards set by the National Highway Traffic Safety Administration (NHTSA), and emissions regulations by the Environmental Protection Agency (EPA).

Governance, Risk and Compliance (GRC) - a framework used by organizations to align their IT and business strategies with regulatory requirements and risk management practices. It ensures that the organization operates ethically, manages risks effectively, and complies with laws and regulations, thereby enhancing overall corporate governance and accountability.

National Institute of Standards and Technology (NIST) - a U.S. federal agency that develops and promotes measurement standards, guidelines, and technologies to enhance innovation, economic security, and quality of life by advancing measurement science, standards, and technology in ways that improve the reliability and accuracy of various industries and sectors.

State Standards - state standards in the DMV include requirements for driver licensing, vehicle registration, emissions and safety inspections, and enforcement of traffic laws.

Appendix 2: Site and Transaction Observations

Deloitte observed customer interactions, transactions, and operations at the following sites:

- North Salem DMV Field Office
- South Salem DMV Field Office
- Stayton DMV Field Office

Deloitte also shadowed representatives in the Call Center at HQ DMV.

During site visits and in the DMV training environment transaction walkthrough, Deloitte observed the transactions outlined below. This allowed further understanding of the various data fields and steps to complete each transaction type.

- Real ID Applications and Renewals for DL, ID, and Permit
- Non-Real ID Compliant applications and renewals for DL, ID, and Permit
- Replacement DL, ID, and Permit
- Teen Driver
- CDL Transaction
- Change of Address
- Suspension Reinstatement for DL, Permits

Appendix 3: DMV Project Team Stakeholders Interviewed

Deloitte conducted stakeholder interviews with ODOT and DMV personnel. The insights and experiences gleaned from the interviews provided Deloitte with valuable perspectives that are integral to our initial observations and actions.

DMV Personnel

- DMV Administrator
- Innovation and Planning
- Program Services
- Change and Engagement Team Manager
- Field Services
- Data Governance Team
- Trainings (SOPs, Protocols) Team
- Voter Registration Transmission Team
- Data Sharing Agreement Team
- Confidential Records Desk
- Fraud Examiner

ODOT Personnel

- Chief Information Officer
- Chief Data Officer

Appendix 4: Documents Reviewed

Deloitte reviewed and gathered insights from the following list of documents. The examination of these materials supported our initial observations and actions.

- After Action Report
- ODOT Strategic Action Plan
- DMV Internal Site URL
- DMV Strategic Plan URL
- Field Services URL
- DMV Strategic Plan Key Priority Enhanced Data Mgt Charter
- DMV Strategic Plan Key Priority Comprehensive Change Mgt Charter
- DMV DIR Data Maturity Assessment Overview
- Oregon DOT DMV Data Quality Maturity Assessment (FINAL 12.12.2024)
- Secretary of State DMV System Audit Report_2024-28
- Suspension Data Issues
- Audit Files & Reports
- Confidential Records Desk (CRD) Information
  - CRD Policies and Procedures
  - Protected Address Programs Summary
  - Work-in-Lieu Address Protection Program
  - Fictitious Undercover License Program
  - Confidential Address Protection Program
  - DOJ Address Confidentiality Program
- DMV Org Charts
  - CSG Org Chart
  - DMV Org Chart
  - DMV-IS-Org Chart
  - FSG-Org Chart
  - IAP-Org Chart
  - MT_Photo_Org Chart
  - PGSG Org Chart
  - TSO Org Chart
- Manuals and Procedures
- Process Maps and Reports
  - Field Transaction Summary
  - 173DPfill and 173 3rd Review Presentation
  - Issue OD Credential Process
  - Issue NCL Credential Process
  - OLIVR Diver Transaction Demo
  - OLIVR Roles and Permissions
- Supplemental Process Maps
- Training Manuals
- Training Manuals-FSG

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Copyright © 2024 Deloitte Development LLC. All rights reserved.