Deloitte.

Oregon Department of Transportation

Driver and Motor Vehicle Services

Data Integrity Review (DIR) Project

Final Review Report

February 28, 2025

Table of Contents

Executive Summary

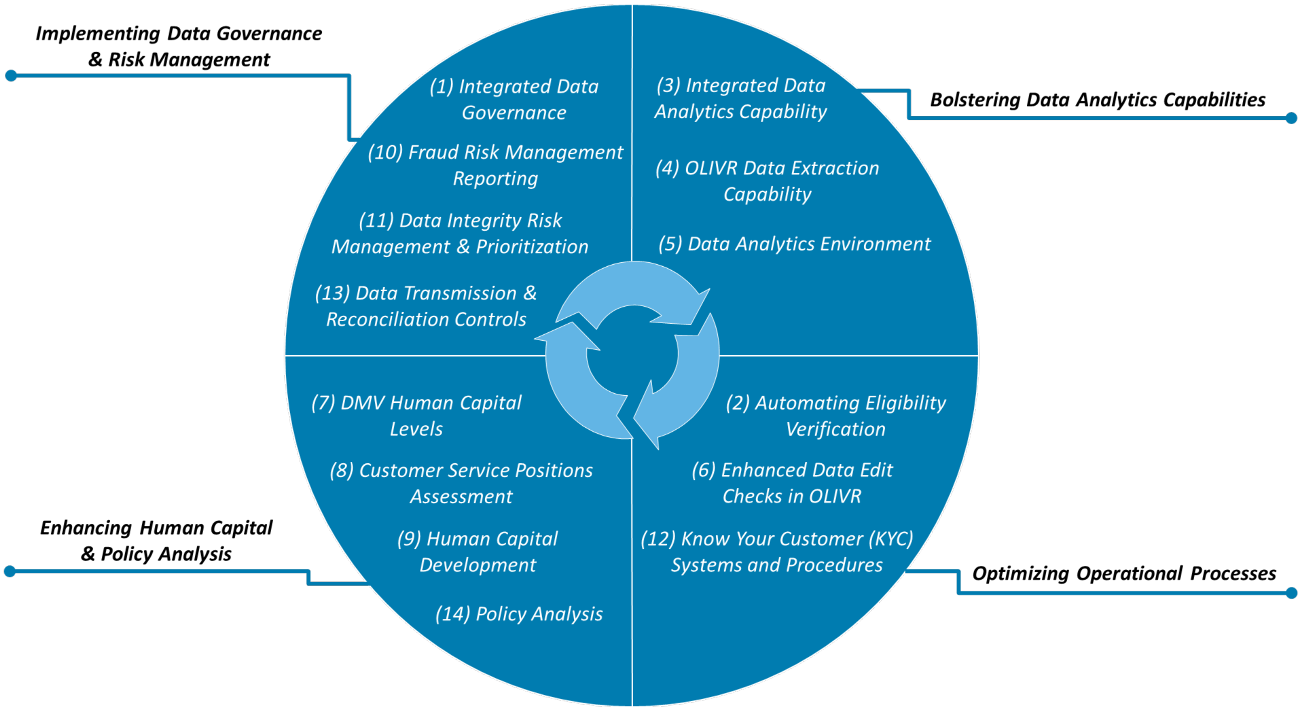
In response to concerns regarding voter registration eligibility, Oregon Governor Tina Kotek directed the Oregon Department of Transportation (ODOT) to initiate a data integrity review of the Driver and Motor Vehicle (DMV) Services Division. As part of the response, Deloitte conducted an initial assessment as the first part of a two-phase process based on the Governor's high-priority timeline to deliver the Preliminary Review Report by December 31, 2024. The results from Phase 1 were foundational and have now been elaborated following the collection and evaluation of additional insights and data as part of this Final Review Report.

During the Phase 1 assessment period, Deloitte conducted a strategic review and analysis of DMV-provided documents, conducted 13 stakeholder and process-owner interviews, and visited three DMV field office locations and the DMV call center headquarters (HQ) to observe driver-related transactions. During Deloitte's introduction to ODOT, it received an orientation to the Oregon License Issuance and Vehicle Registration (OLIVR) system, the transactional system underpinning DMVs functional and operational processes. Our initial results identified 14 Observations, and each one included a proposed action and Business Rationale for management's consideration.

During Phase 2 of the project, Deloitte conducted additional reviews and analyses of DMV-provided documentation, including studies, after-action reports, and DMV feedback on the Preliminary Review Report. Deloitte also conducted 12 additional interviews with identified Points of Contact to refine its understanding of each Observation and to enhance its insights regarding the potential challenges and opportunities available for DMV to address or mitigate these issues. The 14 Observations previously identified in the Preliminary Report now each include Solution Architectures, Solution Profiles, Data and Related Information, and refined Business Rationales that ODOT can consider for future implementation and action.

To offer a structured and foundational overview of the Observation descriptions for ODOT, the graphic below (see Figure 1: Strategic Observations Graphic) organizes the 14 Observations into four distinct categories. These categories – Implementing Data Governance & Risk Management, Bolstering Data Analytics Capabilities, Enhancing Human Capital & Policy Analysis, and Optimizing Operational Processes – contextualize the landscape and provide valuable information to support and inform strategic decision-making.

Figure 1 – Strategic Observations Graphic


Implementing Data Governance & Risk Management
(1) Integrated Data Governance
(10) Fraud Risk Management Reporting
(11) Data Integrity Risk Management & Prioritization
(13) Data Transmission & Reconciliation Controls
Bolstering Data Analytics Capabilities
(3) Integrated Data Analytics Capability
(4) OLIVR Data Extraction Capability
(5) Data Analytics Environment
Enhancing Human Capital & Policy Analysis
(7) DMV Human Capital Levels
(8) Customer Service Positions Assessment
(9) Human Capital Development
(14) Policy Analysis
Optimizing Operational Processes
(2) Automating Eligibility Verification
(6) Enhanced Data Edit Checks in OLIVR
(12) Know Your Customer (KYC) Systems and Procedures

Finally, DMV has put in place a series of system-driven object behavior changes (i.e., the application user interface behavior of OLIVR) and manually driven measures to enhance the internal controls regarding the accuracy and quality of voter registration data within the OLIVR system. We believe these implemented enhanced processes, along with DMV's observations and measurements regarding their effectiveness, provide adequate confidence that data integrity within OLIVR is sufficient to reinstitute the process of Oregon Motor Voter (OMV) data transfers to the Secretary of State. Our view is qualified on the condition that DMV sustains these measures and continues to validate the data files (composed of data exported from OLIVR) transmitted to the Secretary of State for completeness, accuracy, and timeliness.

The manual measures currently in place can be improved in the context of long-term solutions. While they appear to be effective in reducing errors, these manual measures are 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 more automated processes to reduce the potential for human errors impacting data integrity. Leveraging these capabilities and solutions will reduce the manual processes (e.g., such as manual error review and reporting) immediately instituted by DMV after the identification of the historical data integrity issues.

The efficiencies that may be realized through the development and implementation of automated business processes will require training, providing DMV an opportunity to strategically review existing training protocols. These realized efficiencies can support the development of a training plan that equips DMV to proactively address emerging trends, potential risks, and evolving knowledge requirements. Potential investments in advanced technologies to provide the assurances DMV requires can be evaluated, including the potential alleviation of pressures on field personnel. Specifically, DMV can evaluate these options in the context of current staffing levels, employee capabilities, budget limitations, governing policies, and the law.

Project Background

Oregon Governor Tina Kotek directed ODOT to initiate a data integrity review of DMV processes and systems in September 2024. The goal was to produce preliminary actions for improved data governance and 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 DMV's operations, which is essential for informed decision-making, regulatory compliance, and delivering reliable services to Oregonians. 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 transactions 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 license issuance. DMV extracts and provides data to many customers, including drivers, residents, courts, and law enforcement. Additionally, Oregon House Bill (HB) 2177 (2015) - the Oregon Motor Voter law - 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. DMV issues credentials in the form of identity cards, permits, and driver licenses, and it can do this only in concert with establishing identity as required in ORS 807, Oregon's state law covering driving privileges and identification cards.

The Phase 1 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.

As part of the Phase 1 assessment, Deloitte conducted a strategic review and analysis of DMV-provided artifacts, including policies, audits, after-action reports, additional assessments, training materials, and workflows (see Appendix 4). 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 DMV call center HQ to observe driver-related transactions, supplemented by a training environment demonstration of additional transactions (see Appendix 2). The analysis identified 14 Observations, and each comes with associated proposed Actions and a Business Rationale for management's consideration. 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.

The Preliminary Review Report, documenting the results of Phase 1, was delivered on December 20, 2024, and was based on document reviews, interviews, and functional process observations. The 14 Observations identified focused on immediate insights gathered and set the foundation for an expanded set of Observations and Solution Architectures in the Final Review Report.

Objectives

Deloitte conducted a Data Integrity Review (DIR) to assess the accuracy, consistency, and reliability of the DMV's data management processes. This review aimed to identify and propose Actions to enhance processes that affect data integrity, thereby identifying opportunities for improving the overall quality and dependability of the information transacting through DMV's systems. The review also 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 DMV to conduct its operations on a basis of accurate, reliable, secure, and efficient data management processes, which is essential for informed and timely decision-making, regulatory compliance, sustaining customer trust, and delivering reliable services to Oregonians.

Data Integrity 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. Full definitions related to this Review are located in the Definition of Key Terms in Appendix 1. For the purposes of the process review associated with this assessment, based on close alignment with 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:** 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:** 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). This dimension 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:** 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:** 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. Timeliness also 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:** 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.

ODOT Remediation Efforts to Date

ODOT has undertaken efforts to enhance data integrity throughout their data ecosystem. These initiatives have focused on addressing critical data quality issues, improving data governance, and implementing internal controls. To achieve a cohesive agency-wide data governance framework, driven by the Data Solutions Office (DSO) and led by the agency's Chief Data Officer (CDO), ODOT established an annual data governance plan. Within the plan, ODOT HQ requested each of its divisions, including DMV, identify individuals for four formal data stewardship roles: Coordinating Data Stewards, Data Trustees, Business Data Stewards, and Technical Data Stewards. While each role has specific responsibilities, all data stewards support the objective of maturing ODOT's data governance practices with a continuous improvement mindset. Additionally, the CDO requires six trainings for the formally identified data stewards and offers an additional training for all ODOT employees.

DMV has implemented specific manual and system processes aimed at enhancing data consistency. These efforts have predominantly been reactive measures in response to identified data integrity issues. In the instance of driver's license suspensions due to incarceration, DMV coordinated a manual exchange of records with the Oregon Department of Corrections and Oregon county jails, to proactively receive release dates of adults in custody, therefore maintaining consistent driver's license suspension information across state agencies and for the suspended individuals. Additionally, DMV staff manually review conviction and suspension documents, received from both in-state and out-of-state entities, to detect information gaps and incomplete documentation. These processes aim to prevent data discrepancies that previously challenged DMV and relevant parties.

While attempting to leverage OLIVR to perform data analytics, DMV has implemented thorough manual reviews of reports extracted from the system to facilitate business functional requirements. In the instance of the former Governor's executive order to forgive certain unpaid traffic fines and fees, DMV utilized OLIVR to extract a report of all individuals fitting the executive order's criteria. However, because of the complexities of the report and OLIVR's internal relational data architecture, certain individuals that should have been included in the report were excluded. Through remediation, DMV implemented manual checks and coordination with the report builders, confirming the accuracy, consistency, and reliability of the data to identify and correct errors before they impact decision-making processes.

Permanent system changes to OLIVR have also elevated DMV's data integrity. During the driver's license issuance process, customers are required to provide proof documents. The system was initially configured to display the most used documents at the top of the list. On a few occasions, DMV observed that Transportation Service Representatives (TSR) typing "PAS" to select a passport were inadvertently selecting a US passport when presented with a foreign passport. The primary challenge stemmed from the system's prioritization of commonly used documents, leading to TSRs unknowingly entering incorrect customer information. To mitigate this issue, the document listing within the system was restructured to follow an alphabetical order rather than prioritizing common documents. This change, in concert with additional manual checks after entry, ensures that DMV TSRs can more accurately and efficiently locate and select the intended document type.

Additionally, ODOT contracted with Spy Pond Partners, LLC to conduct a data quality maturity assessment for DMV. This highlighted DMV's current data quality maturity level while identifying opportunities for more formalized data quality planning processes, advancements in supporting data processes (architecture management and data operations management), and supporting organizational management processes.

ODOT's collective efforts contributed to improved data integrity, decisive decision making, and enhanced public safety in Oregon's transportation and motor vehicle system.

Scope

The Data Integrity Review assessed DMV's data integrity processes and technology, 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;
- Documentation of information as electronic data in OLIVR;
- Process of establishing records that meet data use requirements as defined by statutes or rules;
- Extraction and transmission of data accurately and securely to appropriate data users; and
- Governance, policies, processes, procedures, and utilization of current systems.

The scope did not include DMV vehicle registration and operations, an assessment of the efficacy of existing laws and regulations, an assessment of the OLIVR system, or an assessment of current or prospective vendors. Deloitte reviewed the "*Oregon Driver and Motor Vehicle Services Division: Licensing and Registration System Accurately Assesses and Collects Fees, but Security Processes Need Improvement"* audit report (DMV OLIVR Audit Report) to gain insights into the OLIVR system. As a result, this report concentrates on how the tool is utilized in relation to various business processes, rather than providing an assessment of the system itself.

Observations have been noted and suggested Actions offered to help DMV consider opportunities for being more effective and assured of its posture with respect to data integrity. Following each Observation and Action, Deloitte provided Solution Architectures, which are specified steps or measures ODOT can consider implementing to assist in remediating identified challenges. Deloitte also supplied supporting Data and Related Information, which includes relevant qualitative and quantitative information to assist in engineering future action that aligns with ODOT's standards and operational goals.

Purpose of the Final Review Report

The Deloitte team used the Preliminary Review Report to validate the initial findings and Observations with relevant ODOT HQ and DMV personnel. The Final Review Report was also used to validate the observations and measurements performed by DMV that indicate the recently enhanced measures are functioning as intended with respect to data integrity. This step helped to ensure that our final written Observations and their supporting Solution Architectures 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 both ODOT HQ and DMV stakeholders in Phase 2, we included in the Final Review Report Solution Profiles that characterize critical decision-informing dimensions, such as cost and timelines, that correspond to each Observation and Solution Architecture.

We elaborated on our Observations and Actions by providing additional details and context. This included expanding the Business Rationales and adding further data and information (labeled as Data and Related Information) citations to underscore a data-driven intent behind the proposed Solution Architectures for ODOT's considerations. This approach provides options for ODOT to consider that are well-supported, actionable, and aligned with ODOT strategic objectives.

To better visualize and correlate identified challenges to a suite of Solution Architectures, we developed a Strategic Challenges and Solutions Crosswalk (see Appendix 5), which maps out key challenges and aligns them with Deloitte's proposed solutions. The crosswalk highlights critical focus areas, such as training and development opportunities, resources constraints, opportunities for automation, and data extraction and reporting. By leveraging Deloitte's industry experience and resources, the crosswalk provides specialized solutions tailored to each challenge. This alignment aims to confirm that the proposed solutions are practical and actionable, while maintaining strategic alignment to ODOT's objectives, thereby highlighting opportunities for enhancing operational efficiency and effectiveness.

In terms of DMV's request to evaluate the current measures instituted to mitigate additional risks associated with OMV data transfers to the Secretary of State, and acknowledging the serious impact and significance of this process, we continue to support our recommendation from Phase 1. We believe these enhanced processes and permanent system changes, along with DMV's observations and measurements regarding their effectiveness, provide adequate confidence that data integrity within OLIVR is sufficient to reinstitute the process of OMV data transfers to the Secretary of State. Our view is qualified on the condition that DMV sustains these measures and 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.

Approach

To assess and address the data integrity challenges faced by DMV, Deloitte undertook a two-phased approach. Phase 1 included a thorough review of background information, documentation, personnel interviews, field and headquarters observations, and transaction walkthroughs. Phase 2 consisted of an in-depth examination into four key focus areas, as follows.

- **Review of ODOT DMV Data Integrity Review Phase 2 Considerations:** We reviewed the *ODOT DMV Data Integrity Review Phase 2 Considerations* document (see full list of Documents Reviewed in Appendix 4) to confirm that our approach remained closely aligned with ODOT's strategic objectives and expectations. This evaluation enabled us to identify key focus areas warranting further attention and deeper investigation. Our Phase 2 strategy concentrated on these critical areas and aimed to address them in greater detail, therefore authenticating an impactful final deliverable. This collaborative approach facilitated more tailored and effective solutioning.
- **Review of DMV Documents:** We conducted a further review of relevant ODOT 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 standard operating procedures (SOPs), technology infrastructure documentation, field operation workflows, and training materials.
- **Interviews with ODOT Personnel:** To gain further insights and understand the various perspectives within the organization, we interviewed key personnel, including executive leadership, functional and technology managers, and field managers (see full list of Stakeholders Interviewed in Appendix 3). These interviews helped us to better understand strategic priorities, operational challenges, technical limitations, and customer service experiences.
- **ODOT Stakeholder Input:** We identified and collaborated with stakeholders to validate and refine the Observation language used in the report (see full list of ODOT Project Team Stakeholders Interviewed in Appendix 3). We engaged stakeholders to confirm that the descriptions accurately reflect their perspectives, allowing for enhanced clarity and a shared understanding of the key focus areas. Additionally, we collaborated with the Expert Review Team (ERT) - a group established by ODOT Executive Sponsors at the direction of the Governor and consisting of transportation data leaders from various states and professional organizations - to evaluate the Preliminary Review Report and provide additional recommendations for Solution Architectures based on their knowledge, skill, and expertise in data management.

By using Phase 2 to expand on the insights identified during Phase 1, we were able to effectively recognize what is operating well, what has been improved based on the actions identified in the *DMV After-Action Report* and identify the root causes of data integrity issues. Deloitte developed actionable solutions for ODOT to consider that, if implemented correctly, could enhance the integrity of the data managed by Oregon DMV.

Observations, Actions, Related Data & Information, Proposed Solution Architectures & Business Rationales

As part of the assessment, Deloitte offers Observations across many of the areas reviewed. The Observations predominantly relate to themes and areas regarding data process management; including Implementing Data Governance and Risk Management, Bolstering Data Analytics Capabilities, Enhancing Human Capital & Policy Analysis, and Optimizing Operational Processes (see Figure 1 – Strategic Observations Graphic). 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 an important baseline for ODOT decision-making around potential future changes to resources, systems, and processes. During Phase 2, all Observations were re-confirmed with specific relevant ODOT HQ staff and/or DMV Points of Contact and supported with underlying data and documentation to ensure there was mutual agreement and concurrence on the specified themes and issues.

The Actions presented, and accompanying Business Rationales, translate the Observations into actionable steps that can drive improvement and address identified issues or gaps. Actions, many supported by industry standards and best practices, 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.

Finally, the Solution Architectures provide a structured approach to designing and implementing solutions that align with the Actions, ensuring that technical decisions support strategic objectives and deliver tangible value. For observations with multiple potential solution architecture options, the options are designed to be mutually non-exclusive, enabling implementation based on ODOT's assessment of feasibility. Each of these options represent a distinct path and can be evaluated independently. In those instances where a single option for a Potential Solution Architecture is presented, Deloitte considered the solution to be the singular, effective method for addressing the data integrity opportunity.

Defining the Solution Profile

When evaluating Solution Architectures, it is crucial to consider each solution's profile through a framework comprising four critical dimensions: Time, Cost, Complexity, and Impact, with each assessed on a scale of low, medium, and high (see Table 1: Solution Profile Definitions). Furthermore, it is imperative to diligently incorporate the dimensions of sustainability and futureproofing into the drafting of Solution Architectures. Therefore, the recommendations do not only provide considerations to current issues but are also scalable and sustainable to effectively address future challenges. This robust evaluation framework allows for a thorough understanding of each solution's feasibility, potential effects, and long-term viability as it pertains to resources (technological and staffing), processes, and infrastructure.

Time refers to the relevant, estimated amount of time required to accomplish the solution.

Cost is another crucial factor and relates to the relevant cost of implementing the solution.

Complexity of the solution refers to the estimated level of difficulty required for implementation and must take into consideration ORS276A.365, which requires data to be governed and managed as a strategic asset throughout its information lifecycle and that data systems/solutions must scale to business needs and are required to promote/enable the separation of data from the application layer to maximize data use and reuse opportunities. Because of the often overwhelming levels of complexity that exist within and between mission-critical data assets, the statute also requires the industry best practices of comprehensive data documentation with at least a data dictionary to create a standardized common understanding that ensures consistent understanding of context, provenance (or lineage), and meaning so data assets are interpreted, applied, and used appropriately and correctly. This is important for empowering data-informed analytics, reports, and decision-making processes instead of them being based on emotion, intuition, and anecdotal narrative.

Additionally, each rating for **Complexity** also accounts for the degree of organizational change management (OCM) activity required for a specific business unit or the changes needed to implement a reengineered business process. This approach considers the human and organizational aspects of complexity, along with long-term implementation requirements, recognizing that the technical challenges are often interconnected with the readiness and adaptability of the organization. Evaluating complexity through these additional lenses ensures a smoother transition, minimizes disruptions, and enhances the likelihood of achieving the desired outcomes.

Impact of the solution on the organization must also be considered, particularly as it relates to anticipated improvements to business functions and the corresponding influence the solutions will have on data integrity responsibilities.

An additional point to consider when evaluating the overall **Impact** of a solution is the organizational change management effort required for implementation. Effective change management ensures that staff are prepared, supported, and equipped to adopt new solutions, maximizing utilization and achieving desired outcomes with long-term implementation as an objective. This is crucial for improving data integrity, as successful adoption and utilization of new tools, best practices, and modernized business processes by staff directly influence the accuracy, consistency, and reliability of data. When employees are well-trained and supported, they are more likely to adhere to data management best practices, reducing errors and enhancing data quality. This holistic approach not only drives operational improvements but also supports reliable, data-driven decision-making and long-term success.

Table 1 - Solution Profile Definitions

	Low	**Medium**	**High**
Time	Up to 12 Months	1 year – 1.5 years	Over 1.5 years
Cost	Up to $500,000	$500,000 – $2,000,000	Over $2,000,000
Complexity	Straightforward to implement with standard technology and minimal amount of OCM activities and minimal challenges	Slightly complex to implement with multiple system integrations and moderate amount of OCM activities and moderate challenges	Highly complex to implement with cutting-edge technologies, extensive customizations, and high amount of OCM activities and with potential for significant challenges
Impact	Limited effects on overall operations and stakeholders with specific enhancements and minimal overall improvements	Noticeable effect on operations and stakeholders with multiple improvements and moderate changes	Transformative to implement with major overhauls and significant improvements to operations and stakeholders

Note: These estimates are intended to provide a general understanding of the solution architectures' size and scope and may be subject to change during implementation.

Specific Observations & Solutions

Obs. #	Predicate #	Topic
1	**N/A**	**Integrated Data Governance**

Observation

DMV, like other ODOT divisions, has participated in, but not fully adopted or engaged with, ODOT's ongoing Data Governance (DG) initiatives and requirements yet. Data governance is a critical enabler of achieving data integrity and continues to be systematically implemented as a strategic discipline across ODOT in conjunction with formalizing the overarching ODOT DG Framework. The Data Solutions Office (DSO), led by the Chief Data Officer (CDO), drives these efforts by designating formal data stewardship roles, such as data trustees and business data stewards, within ODOT's organizational structure. While DMV has identified and assigned representatives to the formal and informal agency DG bodies and coordinating data steward positions, there is room for continued improvement in engagement by DMV. DMV, along with the other agency divisions and business lines, aims to facilitate better communication and coordination under a standard DG Framework with the goal of achieving integrated data governance that is crucial for enhancing future operational efficiency and decision-making processes.

Action

ODOT can consider opportunities to continue advancing integration across the department with respect to data governance. Achieving consensus on, and engagement with, a common data governance framework and fully operationalizing that framework should be the priority. An additional emphasis can be offered to preparing 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. Proper data documentation will allow for transparency, continuity, and consistency for DMV to align with standards relevant across the rest of ODOT. Lastly, an additional focus can be offered to creating new capabilities relating to data management, data availability, data analytics, and control over enterprise data.

People

Data professionals with the requisite skills and experience, within ODOT, can be identified to drive the collaboration and integrated approach to data governance. Roles and decision rights within the integrated data governance bodies are defined within ODOT's DG Framework. Finally, ODOT can consider taking steps to ensure the identified resources have been provisioned with the time allocations necessary to perform the required duties of their assigned data governance roles.

Process

ODOT's integrated DG Framework can be operationalized across DMV so DMV can collaborate, interoperate, and manage the data under its collective control using accepted data governance standards with intentionality. The framework will define the methods and standards for how ODOT governs its data in a consistent, sustainable way.

Technology

Depending on the specific elements of the integrated DG Framework, ODOT may require additional technologies to operationalize it. Examples could include technologies that facilitate utilization of ODOT's data analytics ecosystem (or enhancing the current ODOT analytics data repositories, as applicable), technologies that support the documentation and operations of data flows, data entity relationships, metadata, data dictionaries, controls over data, or other technologies that would assist ODOT in modernizing and integrating data governance.

Related Data & Information

- Historically, ODOT divisions have operated with a level of authority to address their core business functions and goals within ODOT's framework.
- Currently ODOT is fairly early into its data governance maturity journey and leadership is promoting a 'One ODOT' approach for greater collaboration and integration. In addition to prioritizing division goals, there is additional emphasis from ODOT leadership for divisions to focus on standardized processes and data governance across all divisions. Organizational change management efforts to fundamentally shift practices are in progress.
- ODOT's Integrated Data Governance Framework is intended to provide support, training, and set expectations for ODOT divisions. DMV has designated two Coordinating Data Stewards (CDS's).
- Data Trustees are managers who have decision-making authority and are accountable for the data assets related to their key business line functions or program areas. Business Data Stewards are subject matter experts (usually business line leads) who, as part of their work, are responsible for managing data in their business line or program area on a day-to-day basis.
- Each Division, major Branch, or Office is asked to provide a single Data Steering Team (DST) representative to help advance agency data strategies, practices, and governance processes. There have been six regular DST meetings in the last eight months, and there is also a Technology and Data Council that functions as an agency-wide governance body.

Potential Solution Architecture

Approach: The gap in Data Governance (DG) engagement from assigned DMV personnel appears predominantly driven by available time and prioritization alignment. A hybrid-federated model where there are operational links between ODOT's DG organization, the DG oversight team, and DMV with respect to centralized data governance standards, policies, procedures, tools, and oversight would help ensure that decentralized DG roles have a clearly understood accountability for delivery of DG services. Additional human resources and technology could help close the current gap in engagement.

1) ODOT can consider defining a specific set of metrics that denotes indicators of acceptable engagement levels. These could include:
    a. The specific number of hours committed to the designated DG roles that assigned DMV personnel should align to DG responsibilities.
    b. The specific DG tasks (e.g., activities, meetings, etc.) that assigned DMV personnel are required to complete.
    c. Specifically articulated service levels that assigned DMV personnel must satisfy as part of delivering DG responsibilities.
2) DMV can enhance current organizational structures to allow for a collaborative/matrixed reporting structure to include assigned DMV resources having a co-reporting (i.e., matrix reporting) relationship to the ODOT Data Solutions Office.
3) DMV can consider enhancing current performance management practices to allow the ODOT Data Solutions Office to have more performance management input regarding assigned DMV personnel with respect to fulfillment of DG responsibilities.
4) ODOT can seek opportunities to augment currently assigned DMV resource levels in terms of the number of personnel and/or percentage of time designated to DG responsibilities. This may require the addition of new DMV staff with the appropriate DG knowledge, skills, and capabilities who are assigned DG responsibilities.
5) ODOT can consider evaluating whether additional processes and technologies are required to fully activate data governance resources in a manner that conforms with ODOT standards and engagement level expectations.

Solution Profile:

Time	*Cost*	*Complexity*	*Impact*
Medium	Medium	Medium	High

Business Rationale

Modernizing and operationalizing ODOT's Integrated DG Framework would provide synergies and efficiencies in a wide variety of data management processes across ODOT. 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 improved data quality and trust. They would also 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, it warrants mentioning that a fully activated integrated DG framework would likely create benefits between ODOT and its other divisions, in addition to DMV. An integrated DG framework across ODOT would help advance DG maturity and ultimately lead to enhanced data accuracy, consistency, and security.

Obs. #	Predicate #	Topic
2	14	Automating Eligibility Verification

Observation

DMV has implemented some measures, including manual procedures associated with secondary and tertiary reviews of field operations transactions, and system changes, 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 updates are reducing errors and helping to strengthen the integrity of the data leaving DMV, the manual efforts place additional burden on the limited field operations personnel, can create workload balancing strain, and may reduce the timeliness and quality of customer service. There are opportunities to automate the manual nature of these procedures while maintaining the overarching goal of reducing errors.

Action

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 made 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 the Documents Presented & Parent/Guardian Certification form (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

DMV can explore options for developing and deploying automation to replicate the current 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 (iOCR) to extract key data elements from identity documents to reduce manual data input, as well as the error rate that may result from manual data entry. Because iOCR technologies are not 100% accurate, a visual validation of iOCR extractions may be required as a change to the business process.

Related Data & Information

- ODOT stakeholders widely agree that manual reviews are time intensive.
- Customers can select from 18 different types of documentation to prove citizenship for OMV.

- The average time spent by staff on identity verification and processing credentialing data is between two and three minutes.
- A 2022 study calculated average time to complete certain transactions in a field office. “Happy Path” averages, where the transaction is completed with no major issues and on the first visit, were tracked across different transaction types.

Potential Solution Architecture

Approach: Using customer-facing iOCR technologies, such as a document extraction engine, DMV could allow customers to automate the submission of identity and voter eligibility documentation by uploading relevant forms and then displaying the extracted data elements for the customers to confirm or correct as needed. This technology could also be used by DMV customer service representatives to automate field-level data extraction using customer-provided documents. Finally, an appropriately secured AI technology under the department’s oversight and control could be deployed and trained to recognize identification and voter registration eligibility documents for authentication purposes.

1) *Option #1* – Institutionalize recently enhanced manual review procedures:
    a. DMV can continue the recently implemented manual procedures in perpetuity.
    b. Understanding that increased workload on existing field resources represents a moderate risk in terms of sustainability and the prevention of potential errors, DMV can seek opportunities to augment currently assigned DMV resource levels to account for the increased manual review responsibilities. This may require the addition of new DMV staff who are assigned these responsibilities.
2) *Option #2* – Deploy modernized technology-based solutions to automate all verification procedures of identity and voter eligibility documentation:
    a. DMV can deploy new, modernized technology-based solutions to automate all aspects of the verification processes with respect to identity and voter eligibility.
    b. DMV can evaluate its existing document scanning solutions to determine if they could suffice for the scanning aspects of a modernized solution architecture.
        i. Understanding that a modernized solution may require the ability to scan and interpret advanced security features, such as holograms and other embedded document elements, it may be that new, modernized scanning technology would be required.
    c. DMV can then deploy advanced automation software to perform verification procedures relating to identity and voter eligibility.
        i. iOCR would likely form the first level of document verification by parsing relevant data contained within identity and voter eligibility documents and populating that data into OLIVR.
        ii. Robotics process automation software could then address some routine aspects of the identity and voter eligibility verification process.

iii. For more advanced document verification that currently requires human interpretation and/or judgment, AI/machine learning technologies could be deployed.

Solution Profile:

Option #1

Time	*Cost*	*Complexity*	*Impact*
Medium	Low	Low	Low

Option #2

Time	*Cost*	*Complexity*	*Impact*
High	High	High	High

Business Rationale

Based on all currently available information and data, it appears the recent system and 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, sustaining data integrity in a reliable manner, and reducing pressures on field operations personnel, without jeopardizing other aspects of field operations.

Obs. #	Predicate #	Topic
3	1	Integrated Data Analytics Capability

Observation

While experienced data professionals capable of performing data analytics at various skill levels currently exist across ODOT divisions, including DMV, there is no formal integrated data analytics capability within DMV's operational data ecosystem, a situation mirrored across ODOT. Historically, divisions have operated semi-independently with limited integration in data governance and management, leading to opportunities to better connect data management and analytics functions. Analysts within DMV and other units are often hired or developed internally to meet specific business needs or regulatory requirements, but they face competing functional demands that prevent them from fully leveraging coordinated and integrated analytics for reporting, compliance, performance management, risk analysis, decision-making, and transparency. Despite recent upgrades and modernization of legacy transactional systems, including DMV's OLIVR system, these projects are focused on fulfilling business transaction services as timely and accurately as possible and not on the value of data quality beyond what is required for accurate record creation and processing. This results in continued data fragmentation, data silos, and data debt. Transactional systems tend to limit the accessibility, extractability, and usability of transactional data assets, leading to fragmented and siloed reporting and decision-making.

DMV and other ODOT divisions attempt to perform analytics and respond to data requests using their primary operational systems, such as OLIVR, which were never intended for this purpose. Since its inception, OLIVR was designed to manage and record transactional data related to drivers and vehicle registration. This system's architecture and functionality are optimized for handling day-to-day operational transactions, rather than performing complex or integrated analytics. Over time, the need for reporting and data analysis led to OLIVR being leveraged to perform analytics and respond to other reporting requests, including data sharing and data integration. This issue is prevalent among DMVs nationwide, not solely with Oregon DMV, especially as other states also utilize the same COTS that underpins OLIVR. However, the lack of integrated analytics capabilities and the backlog of reporting and monitoring needs hinder DMV's effectiveness.

Action

ODOT can consider building an integrated (core) data analytics team, with a focus on enabling the team to strategically develop solutions that address a range of operational challenges and provide analytics consultation and support for the embedded business-line focused analysts that are federated out. Examples of areas where a dedicated team could support DMV objectives include data analytics and innovation, data quality/accuracy measures, fraud prevention, internal control and monitoring, data-driven decision making, and other areas of operations that relate to data integrity.

People

Data professionals within ODOT can be identified to populate and lead the integrated data analytics capability. This could entail redeploying existing data management professionals within DMV, and/or allocating budget for new human resources. Depending on the details of the roles determined for this capability, a review of job descriptions and job classifications could also be appropriate. Finally, careful consideration can be given to the organizational placement of the team (i.e., ODOT's Data Solutions Office or DMV levels). A hybrid-federated model may ultimately be most effective, where a small core team is deployed at the ODOT HQ 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 focus should be on project intake and prioritization processes while ensuring compliance with State policies and rules. Understanding that there is a backlog of needs relative to reporting and monitoring, prioritizing the 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 needs. (See Obs. #5 for an additional perspective).

Related Data & Information

- ODOT's Automated Application Program Interfaces (API) and scripted Extract Transform Load/Extract Load Transform (ETL/ELT) processes have saved hundreds of staff hours each month.

- While ODOT's analytics are currently federated, a core analytics team could provide analytics consultation and support for the embedded business-line focused analysts.

Potential Solution Architecture

Approach: This begins with establishing an integrated data governance framework (Obs. #1) aimed at ensuring consistency and integration across all divisions within ODOT.

1) By developing and enforcing standardized data definitions, formats, and protocols, ODOT can facilitate seamless collaboration and data sharing. Connection to a centralized data analytics ecosystem (as it currently exists within ODOT) may support data aggregation from various transactional systems, including OLIVR, into a single repository, enabling a unified view of data and allowing relevant, but disparate data assets to be made interoperable. Additionally, implementing data literacy and analytics proficiency programs will enhance the skills of DMV personnel, fostering a culture of data-driven decision-making, which is the aim of many DMVs across the nation.
2) The next phase of the solution architecture focuses on deploying advanced data analytics platforms and tools to address diverse data processing needs. The initial step involves evaluating the existing tools and capabilities within ODOT's analytics ecosystem to identify the necessary technology requirements. This assessment will enable ODOT to conduct a gap analysis, highlighting the differences between current tools and what is needed.
    a. DMV can conduct a data technology assessment using a technology evaluation framework to understand the right analytics that could be applied for DMV's analytics needs and the availability of those tools currently within the ODOT data analytics ecosystem. At a high level, an appropriate analytics technology would include capabilities such as real-time dashboards and predictive analytics tools for data visualization and modeling, as well as data virtualization techniques to provide a complete view of data without physically moving it across systems. Robust data integration and ETL/ELT processes will ensure smooth and consistent data flow between operational systems and the centralized analytics repository. Integrating these tools, while understanding what is currently in operation within ODOT's existing IT infrastructure, will enable DMV to leverage its current investments while enhancing its analytics capabilities.
    b. The implementation of advanced data analytics platforms must include robust cybersecurity measures, such as data encryption, access controls, and continuous monitoring, to protect sensitive information and prevent unauthorized access.
3) Additionally, the solution architecture emphasizes the importance of flexible, self-service analytics capabilities to empower business users and analysts.
    a. Deploying user-friendly Business Intelligence (BI) tools will enable non-technical users to independently perform data analysis and generate ad-hoc reports leveraging only proactively curated authoritative data sources. Modern data governance solutions may be implemented to maintain data quality,

cybersecurity, and compliance, ensuring that data remains reliable and secure, especially for purposes of protecting personal data. Continuing to perform regular audits and performance reviews will help identify areas for improvement and minimize data debt. By following a phased implementation roadmap—starting with assessment and planning, followed by design and development, deployment and integration, training, and adoption, and finally, monitoring and optimization—DMV can transform its data analytics landscape with support from the Agency.

4) Lastly, and most crucially, to perform and implement the identified solution architecture, DMV can consider establishing a centralized data analytics team composed of trained and experienced data professionals from various ODOT divisions, with clearly defined roles and responsibilities.
    a. This team can be dedicated to integrating data analytics capabilities across the organization with roles such as data analysts, data scientists, data architects, data librarians, and data governance specialists. Additionally, the team would be responsible for collaborating with ODOT's central data office to develop the strategy for integrating data from various operational systems, including OLIVR, into a centralized data analytics ecosystem, enabling real-time data access and analytics capabilities to support timely decision-making and performance management. Conducting a thorough needs assessment will identify the required personnel and skill gaps, allowing for targeted training, hiring, and development.

Solution Profile:

Time	***Cost***	***Complexity***	***Impact***
Medium	Medium	Medium	High

Business Rationale

An integrated data analytics capability would enable ODOT to strategically focus on currently under-served or unserved data analytics and reporting needs throughout ODOT, 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. This approach can lead to improved decision-making, enhanced organizational transparency, increased operational efficiency, and better regulatory compliance, ultimately fostering a data-driven culture across the organization.

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 (see Obs. #3 regarding the original intent of OLIVR). In certain instances, concerns have been raised regarding the inapplicability of standard OLIVR reports for business unit needs and purposes. As an example, OLIVR offers over 800 standard and custom-built reports, however, at this time, there is not an easy way to determine how many are actively being used, whether they adequately address the information needed, or deliver the precise data required. Additionally, it is acknowledged that the OLIVR system focuses on transactions, like many other DMVs nationwide, and does not easily facilitate the extraction of back-end data directly from its underlying database tables. While there is opportunity to create specific reports, this process is inefficient and inconsistent because it relies on the same resources that are fixing issues, adding enhancements, and supporting other technology projects. Collectively, this presents a situation where many DMV professionals assert that they do not have access to the data and reporting that they need to effectively manage DMV processes.

It was communicated that this situation represents a data integrity issue as the inability to easily determine the usage and adequacy of OLIVR's 800+ standard reports, coupled with the inefficient and inconsistent process of creating specific reports, undermines the reliability and accessibility of critical data needed by DMV professionals to effectively manage functional processes. These issues have all played a role in contributing to the data integrity challenges faced by DMV.

Action

DMV can consider developing an industry standard set of solutions (such as the implementation of an ETL/ELT process) for allowing the export of data from the OLIVR back-end database environment. The solution could be deployed in such a manner as to allow for the user-directed export of data, or it could be deployed using system-operated and automated capabilities, allowing for the preprogrammed export of selected bodies of data in a more controlled manner.

DMV can also consider enhancing the usage of the reports currently in OLIVR. This may be achieved by:

1. Conducting an evaluation of the existing reports to identify which ones are actively being used and those that are rarely, if ever, used. This can be accomplished by implementing usage tracking mechanisms to gather data on report access and utilization.
2. Engaging with business units to understand their specific reporting needs and ensuring that the reports provided align with their requirements. This may involve continuously customizing existing reports or developing new ones tailored to their needs.
3. Streamlining the report creation process by allocating dedicated resources for report development, separate from those handling system issues and enhancements.
4. Providing training and support to DMV professionals to ensure they are aware of and can effectively use the available reports, thereby enhancing their ability to manage DMV processes efficiently.

People

Once the OLIVR data extraction mechanism is operational, ODOT 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 stewardship, and other relevant topics.

Process

The process-related implications of a user-directed data extraction solution 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 solution, there are additional process-related implications that can involve 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 may consider allocating appropriate technical resources to ensure the necessary infrastructure is in place to support data extraction between OLIVR and the ODOT data analytics ecosystem. This includes understanding and implementing data extraction, transformation, and loading processes, as well as ensuring the required hardware, software, and network capabilities are available. This can be achieved by assigning internal resources or procuring support from an external vendor. ODOT 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 to consider. Finally, there is the question of what environments and platforms ODOT would allow its data to be exported to as part of any transformation. (See Obs. #5 for additional perspective on this factor).

Related Data & Information

- After removing 245 unused reports, there are currently 807 total standard reports in OLIVR.
- Stakeholders report there is an insufficient number of personnel to pull data, and there is a lack of understanding of OLIVR's reporting function or available standard reports.
- During 2024, DMV's Business Systems Support and Application Development groups received 107 data requests and completed 99. As of February 2025, 12 data requests are currently in the queue for assignment to a developer, under development, awaiting more information from the requestor, or in testing.
- There is not a significant backlog of work in terms of data requests. Rather, data requests tend to displace other system changes due to the expedited timelines that are often required.
- There is a challenge in terms of the complexity of the data table structure within OLIVR and the overall COTS platform. The system data architecture is complex, and it is not well documented. This lack of documentation causes issues in terms of pulling the right data from the system, and it is common for data requests to return to a developer multiple times for further work after testing reveals issues.

Potential Solution Architecture

Approach: To enhance the data extraction and data analytics capability of DMV business lines using OLIVR back-end data, a multi-faceted solution architecture is proposed.

1) DMV can consider developing a solution to facilitate the extraction of data from OLIVR's back-end database to set up connection points to ODOT's data analytics ecosystem. The most efficient solution would be a system-operated export, which would automate and pre-program data exports to ensure consistency and control. The technology required for this includes secure database connectors and Application Programming Interfaces (API) to prevent unauthorized access or data breaches, data transformation capabilities to convert raw data into usable formats, and scheduling tools for automated data exports.
    a. In setting up this process, it is crucial to confirm that data exports are encrypted both in transit and at rest, and incorporating robust authentication and authorization protocols will help maintain data integrity and confidentiality throughout the automated export.
2) DMV can then implement an enhanced reporting framework to meet the specific reporting needs of DMV business units. This will involve conducting a needs assessment to identify the unique reporting requirements of each business unit, developing custom reports to address these needs, and implementing a reporting dashboard, embedded with a prioritization matrix, that provides real-time insights and easy access to reports. The necessary technology for this includes BI tools for report creation and visualization, a centralized reporting portal for easy access and distribution, and usage analytics to track report utilization and effectiveness.
3) In addition to following established data governance practices from Obs. #1, new policies and procedures for data extraction, usage, and privacy (e.g. cybersecurity policies) can be developed. ODOT HQ and DMV may collaborate to identify data quality management tools and procedures and establish trainings around usage of these tools. Some examples of potential technologies would include data quality tools that support DMV in detecting and correcting anomalies or data governance platforms to manage policies and procedures.
4) Lastly, adequate resources and collaboration between ODOT HQ and DMV are key components for the successful implementation of this architecture. This includes allocating dedicated technical resources for the development and maintenance of the data extraction solution, engaging vendors or consultants if necessary to supplement internal capabilities, and collaborating with other state DMV agencies to share best practices and lessons learned. It would be helpful for DMV to employ a project management tool to coordinate tasks and resources to closely track the extraction, errors, and any ongoing O&M activities.

Solution Profile:

Time	*Cost*	*Complexity*	*Impact*
Medium	High	Low	Medium

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. 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 and in compliance with an accepted and formalized data governance framework, those risks become much easier to mitigate. Additionally, incorporating future-proofing strategies ensures that the systems and processes in place can adapt to evolving user needs and technological advancements, thereby maintaining their relevance and effectiveness over time. 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. By proactively planning for future changes and ensuring that systems are flexible and scalable, organizations can better support their users and maintain robust data management practices.

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

Observation

ODOT has a centralized data and analytics ecosystem used by various divisions and business domains. Currently, subsets of DMV driver, ID card, and vehicle registration data are provided to the data analytics ecosystem for specific interagency data sharing and internal analytics requirements. However, this does not include a formalized data extraction process for a DMV data and analytics environment. Most ODOT divisions, including DMV, rely on their operational transaction systems, such as OLIVR, for analytics, which has proven challenging with respect to data extraction capabilities, formal data documentation, and often presents issues with providing needed reports (i.e., operational transaction systems are typically not designed for this purpose). This restricts user self-service and tailored data extraction, posing a moderate risk to data integrity. With the growing demand for DMV-related data and its recognition as an authoritative source, the need for a centralized analytics data repository has become evident. A data analytics ecosystem is essential for effective, timely, and accurate data analytics and decision-making across ODOT, including DMV. Alongside the need for a centralized analytics environment, the absence of adequate human capital resources to support the infrastructure can lead to process and system breakdowns. It is essential to have a dedicated human capital team or resources to map, transform, operate, and maintain the data within the analytics environment. Investing in these human resources will optimize the integrity and usability of the data, facilitating more efficient and reliable analytics.

Action

ODOT can consider expanding upon its current data analytics ecosystem (i.e., a business intelligence solution) to host additional data from across ODOT and its divisions. While incorporating data from OLIVR should continue to be the initial focus, adding data from other systems within ODOT can be considered to realize more value from the solution.

People

Technical operations personnel will be required to deploy and operate a DMV-centric 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 Obs. #3.

Process

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

Technology

Significant factors relating to technology are involved in deploying a 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 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 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 can be documented to serve as a basis for building out the environment.

Related Data & Information

- Data management professionals need a better understanding of OLIVR data structures and business rules.
- Additional efforts are required to extract and map data to the ODOT data analytics ecosystem, and more specifically for a DMV analytics environment.
- Ongoing maintenance is necessary as both ODOT, and DMV's data analytics environments evolve.

Potential Solution Architecture

Approach: While a data analytics ecosystem exists to potentially serve as an integrated data analytics environment for DMV, the required data management personnel to analyze, transform, and integrate the data in DMV operational systems (i.e., OLIVR) into the ODOT data analytics ecosystem have not been allocated.

1) DMV can consider performing a needs assessment to determine the type and number of data management personnel that would be required to establish and

sustain an ongoing interface between OLIVR and the ODOT data analytics ecosystem.

2) Based on the results of the needs assessment, data management personnel can be hired or reassigned to develop the necessary interface between OLIVR and the ODOT data analytics ecosystem.
   a. A particular focus of the data management personnel should be in understanding existing contextual factors that relate to the correct functional interpretation of transactional data within OLIVR (i.e., business rules that govern the data). Correctly understanding these contextual factors will allow for the development of a technically accurate interface and will also directly support the accurate usability of the data within the ODOT data analytics ecosystem.
3) Following the development of the data interface, a portion of the data management personnel can be dedicated to sustaining and monitoring the data interface between OLIVR and the ODOT data analytics ecosystem.
   a. Over the natural course of any software's lifecycle, changes will occur, including changes to underlying data structures. Therefore, implementing logging and audit trails will help monitor data interactions and maintain accountability.
   b. Assigned data management personnel should maintain a detailed situational awareness of such changes, so that the data interface into the ODOT data analytics ecosystem can be maintained.

Solution Profile:

Time	*Cost*	*Complexity*	*Impact*
Medium	Medium	Medium	High

Business Rationale

Within ODOT, 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 enable ODOT to analyze data, innovate, and create knowledge without having to be constrained by the operational requirements of the primary DMV production system, OLIVR. Taking full advantage of a data analytics ecosystem would significantly advance ODOT'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 (UI) object behavior changes (i.e. modifying how a specific interactive element within a UI responds to user input) 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 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 work authorization document), OLIVR would not necessarily compel the DMV service representative to require the customer to reauthenticate lawful presence 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 identifying additional object behavior (i.e. actions or functions that a visual element on the screen can perform when interacted with by a user) and edit check enhancements that would help ensure data integrity.

People

To perform the recommended evaluation of OLIVR, skilled service representatives who are deeply familiar with all DMV transaction types and associated process steps can be consulted, along with Business Systems Analysts and IT professionals.

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 (i.e. how the application user interface of OLIVR behaves) and enhanced process steps for the selected transaction types. This may require consultation with the vendor that provides the OLIVR solution to determine if the system is feasible to this change.

Related Data & Information

N.A.

Potential Solution Architecture

Approach: As a result of assessing OLIVR transaction types and operational processes, and following consultation with the OLIVR vendor, DMV can establish its baseline edit check coverage while considering implementation of additional measures to bolster the accuracy and reliability of OLIVR transactional data.

1) *Option #1* – Strengthen existing edit check procedures with additional targeted modifications:

   a. DMV can consider implementing enhanced field-level data edit checks that identify all fields requiring special roles for data addition or editing. DMV can create a framework to display these fields as read-only for users without the necessary access, while allowing users with the correct permissions to modify and validate the information.
   b. DMV can consider exploring increased use of data type validations across transactions to ensure data type matching, expected formats, range checks, and pattern matching involving critical information follow expected patterns.
   c. DMV can consider introducing additional real-time edit checks that cross-reference incoming data to enhanced business rules and historical data patterns to flag for discrepancies.
2) *Option #2* – Deploy technology-based solutions to enhance edit check capabilities:
   a. DMV can explore use of staff-facing iOCR to assist with expediting data field extraction and leveraging automation to run pre-developed logic checks across critical data fields to flag anomalies or data discrepancies.
   b. DMV can consider developing and implementing predictive analytics or other automation tools as part of the data analytics ecosystem to identify and flag potentially erroneous transactions, or data field entry anomalies, based on historical data patterns.

Based on the potential enhancements to edit checks and the incorporation of additional technologies, DMV can consider incorporating robust access control mechanisms, logging and additional audit trails, and encryption to protect sensitive data. DMV may incorporate strong user authentication, data privacy measures, and secure automated processes. By addressing these cybersecurity considerations, DMV can enhance the security and effectiveness of its data management and validation processes.

Solution Profile:

Option #1

Time	*Cost*	*Complexity*	*Impact*
Low	Medium	Low	Medium

Option #2

Time	*Cost*	*Complexity*	*Impact*
Medium	Medium	High	High

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 previous successes and provide further data integrity value. Enhancements could also support critical efficiencies such as tracking regulatory compliance requirements, improving downstream processes by increasing data accuracy, particularly for decision making, and by minimizing errors, thus reducing costly fixes.

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

Observation

Upon initial observation, it appears that DMV staffing levels, relative to the scope of services provided and scale of population served, do not align with other motor vehicle service agencies offering similar services. The constrained staffing levels have caused some ODOT personnel to raise questions regarding its impact 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 comparing 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, backlogs, and challenges associated with the functional units evaluated.

Process

During staffing level analyses, organizations sometimes engage in process improvements or other transformations. 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.

Technology

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

Related Data & Information

- DMV data shows a 19% annual turnover rate over the past five years (2019-2024).
- Leadership is concerned that the frequent changes in state law, averaging 12 annually, require urgent updates and training, which divert limited personnel from customer service delivery.
- Staffing levels in field offices are low, with managers often having to work the counter.
- Among the several states reviewed (Wisconsin, Idaho, Iowa, Maryland, Colorado, and Arizona) there is variation in how external entities are utilized. For example, Idaho involves county auditors; Iowa brings in county treasurers to provide audit oversight of DL and vehicle transactions; and all these states utilize third-party vendors. Especially relevant are Maryland and Wisconsin, which serve a similar

number of drivers as Oregon; Wisconsin has almost the same number of field staff FTEs and Maryland has twice as many field staff FTEs.

- West Virginia is addressing retention with a new pay policy, enabling DMV to evaluate performance and provide appropriate compensation, in line with similar career paths in the region.
- Nevada and California indicate they, like Oregon, send personnel relief across offices daily.
- California is moving to eliminate smaller offices and rely more on larger offices to reduce the frequency that their offices fall below minimum staffing levels. Nevada has large offices (100+ staff per office) to help absorb daily workforce shortages.

Potential Solution Architecture

Approach: The misalignment of DMV staffing levels to the scope of services provided and the scale of the population served appears predominantly driven by available resources and prioritization alignment. While DMV is committed to alleviating human capital demands through ongoing modernization efforts, such as more online services and installing DMV self-service kiosks in grocery stores, additional measures can be applied. An evaluation of human capital levels would help to identify DMV's current staffing levels to accurately compare with desired and optimal staffing levels. Procuring additional technology tools could help in identifying productivity gains.

The evaluation of human capital levels can include:

1) DMV can consider collecting and synthesizing existing staffing and productivity data to generate an understanding of its quantifiable work products and establish baseline insights of each business unit's outputs, pivotal to informing the evaluation's data synthesis and peer agency comparison.
2) DMV can consider establishing relevant peer comparisons, with the understanding that identifying motor vehicle service agencies offering a similar number of services will aid in determining areas for improved operational efficiency.
3) DMV can consider establishing baseline productivity measures by business unit segmentation and/or determined business processes. Estimating the time required to complete the identified tasks and historic workload may assist in discovering key productivity measures.
4) DMV can compare the total time needed to complete the tasks to the total hours available to DMV's employees. The results can be used to identify productivity constraints and areas for optimization in each business unit.
5) DMV can consider leveraging an accelerator tool that uses proprietary and open-source data to provide ODOT and DMV leadership with insights into the impact of future workforce changes. Such tools can identify automation opportunities and make recommendations regarding estimated productivity gains from potential technology implementations.

Solution Profile:

Time	*Cost*	*Complexity*	*Impact*
Medium	Medium	Medium	Medium

This Solution Profile includes the implementation of the accelerator tool because the tool's implementation would be dependent on completing a human capital evaluation.

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 with those of other peer 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. Additionally, outcomes can enable DMV to make informed decisions to enhance productivity and resource utilization, leading to a more efficient and effective operation. 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 Position 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 service representative turnover level, which is approximately 19% over five years. 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-six-year range of tenure. Additionally, as processes and technology have evolved over time, there are concerns that the required skills for 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 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 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 human resources 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, both legacy and new ones that may be implemented, are included.

Technology

DMV can consider the impact of current and prospective technology enablement during 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. The assessment can be conducted in the context of how technology supports customer service positions.

Related Data & Information

- There is an in-depth job classification review effort currently underway for many DMV positions.
- DMV leadership indicates that DMV offices in metro areas lose personnel to other state entities that pay better and offer remote work.
- DMV roles are highly technical and require customer service skills, including de-escalation in the case of aggressive customer behavior. Field staff were previously under pressure for volume and now have been refocused to pay additional attention to data integrity as well.
- DMV field and call center staff perform both driver and vehicle transactions and must know both types of policies and procedures. In many states, DMV type agencies handle <u>only</u> driver related transactions, while other entities handle vehicle transactions.
- Surveys from exiting staff often mention frustrations at a lack of training.

Potential Solution Architecture

Approach: The personnel departure rate among DMV service representatives may have escalated over time and may be driven by several factors, including the possible under-classification of customer service positions. A multifaceted assessment of customer service positions focused on enhancing associated classification levels, synthesizing compensation brackets, and identifying skill gaps, would aid employee retention efforts.

The multi-phased assessment of customer service positions may include:

1) DMV can consider reviewing the current state job classifications and compensations to identify challenges and opportunities for enhancements that reflect market practice and increased efficiency of the classification structure.

2) DMV can analyze the customer service position titles against appropriate market data sources and industry scopes (e.g., government entities and the private sector) to determine updated matches for each position.
3) DMV can consider measuring and evaluating comfort and capability in key and critical skills required to identify skill gaps across the customer service workforce.
4) DMV can consider administering a survey and analyzing the results to identify skill gaps. To enhance the survey's effectiveness, DMV may categorize skills based on their current application and availability of staff performing the required skill.

When evaluating DMV's personnel skills gap, consideration should be given to additional cybersecurity training (as applicable), or improving the current training received, as this knowledge is necessary to understand the importance of protecting sensitive information and mitigating potential cyber events.

Solution Profile:

Time	*Cost*	*Complexity*	*Impact*
Low	Low	Medium	Medium

Business Rationale

Customer service representatives 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 tied to errors in the customer service operation. This underscores the importance of appropriately skilled service representatives to data integrity. DMV can perform an assessment of service representative positions and make any necessary updates to position classification, required skills, and compensation levels, which could help reduce turnover and enhance DMV's capacity for sustaining data integrity. The findings can provide actionable recommendations to address recruitment, retention, and reskilling challenges, including classification adjustments to retain experienced talent long-term, ultimately enhancing data integrity and service quality.

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, there are concerns that the potentially insufficient 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; steps can be taken to correct the situation. Specific areas of training can be articulated for elaboration and implementation.

People

DMV can consider conducting a survey of its workforce with a focus on understanding employee sentiment as it relates to the sufficiency of training provided within 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 external resources to modernize and enhance training for DMV, 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.

Related Data & Information

- There are numerous mandatory annual trainings and occasional gap trainings that are assigned and provided for all of DMV’s approximately 840 employees.
- All training courses are on an annual maintenance cycle. However, if there is a legislative or policy/program change, training modules will be reviewed and revised to meet the required implementation dates determined by managers.
- In addition to DMV and field staff trainings, there are 26 mandatory ODOT policy reviews and trainings for new employees and nine annual policy reviews and trainings for all staff (certain positions also require additional reviews and trainings).
- New call agent staff are required to go through the Customer Assistance training course of about seven weeks.
- DMV field and call center staff provide both driver and vehicle services, which requires more training. This is not always the case in other states where staff responsibilities are more specialized.

Potential Solution Architecture

Approach: Concerns about the adequacy of resources allocated to other areas of training may have a direct effect on data integrity, despite DMV currently supporting a thorough customer service representative training program. Conducting a comprehensive assessment of training functions will help DMV better understand the current state of its training program and the level of resources allocated to other areas of training. DMV may evaluate existing training results to ascertain efficacy. Cross-referencing this data with employee performance outcomes can help identify correlations between training efficacy and performance improvements.

1) *Option #1* – The assessment of training functions can include the following components:
   a. DMV can consider evaluating existing results from customer service representative training to gain a view of the program and assist in determining the efficacy of the trainings offered.
   b. DMV can cross-reference the information with employee performance outcomes, focusing on data integrity, to potentially identify correlations between training efficacy and performance improvements.
   c. DMV can use the target efficacy metrics to highlight and address gaps in training.
   d. DMV can also consider seeking opportunities for modernization through innovative technology around training or the creation of a new curriculum, as a result of understanding the analyzed data.

When evaluating DMV's training program, consideration should be given to including cybersecurity training, so that all DMV personnel have the knowledge and skills necessary to help protect sensitive information and mitigate potential cyber events. Additionally addressed in Obs. # 7, consideration can also be given to the scope of services provided by TSRs, which include driver and vehicle transactions, when assessing training functions.

2) *Option #2* – Explore the implementation of an AI/ML policy chatbot:
   a. The implementation of a policy chatbot can significantly enhance DMV's training program by automating responses to frequently asked questions, thereby reducing the need for extensive self-study and "classroom" training time. This ensures that all representatives receive consistent information, which improves data integrity and reduces discrepancies.
   b. Additionally, the policy chatbot offers real-time assistance and guidance during on-the-job training, helping new hires quickly adapt to their roles. By providing accurate and timely information, the bot can resolve issues at the first point of contact, minimizing the need for escalation. This optimization of resources allows human trainers to focus on more complex training needs, ensuring better allocation of training resources across different areas. Furthermore, the policy chatbot continuously updates its knowledge base, providing up-to-date information and training materials to customer service representatives.

Solution Profiles:

Option #1:

Time	*Cost*	*Complexity*	*Impact*
Medium	Medium	Low	Medium

This Solution Profile includes the implementation of new technology around training or creation of a new curriculum because the modernizations would be dependent on completing a training functions assessment.

Option #2:

Time	***Cost***	***Complexity***	***Impact***
Medium	Medium	High	High

Business Rationale

Workforce 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 could increase its capacity for ensuring adequate data integrity levels and mitigate the risk associated with historical gaps in data integrity. This assessment can help DMV optimize its training resources and enhance the effectiveness of its customer service representatives.

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

Observation

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

Action

ODOT 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 DMV's fraud unit has the human capital required to perform limited fraud risk management functions. However, due to a lack of processes to proactively monitor transactions for irregularities and inadequate access to effective reporting, the fraud unit is unable to achieve greater lead generation and investigation. This prevents the team from running and implementing proper fraud risk management analytics using data-informed intelligence. Furthermore, the 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 DMV's fraud unit is constrained by limited analytics tools and a reactive approach to identifying leads (e.g. calls from the fraud hotlines), which contributes to a restricted scope of fraud and fraud risk identification. This limitation hinders the unit's ability to effectively conduct fraud risk management processes, including lead generation and investigations. To address this, the DMV should consider implementing improved fraud risk management analytics to enhance lead identification. Depending on the volume and quality of leads generated through these enhanced analytics, it may be necessary to update the overall fraud risk assessment processes and expand the portfolio of identified fraud risks. Given the rapid evolution of fraud risks, the DMV should explore opportunities to implement process changes that leverage advanced analytics to stay ahead of emerging threats.

Technology

To support DMV's fraud unit in developing useful and reliable analytics, a mechanism will be required to extract data from OLIVR (see Obs. #4). Beyond the data extraction mechanism, the ability of the fraud unit to perform analytics would be substantially accelerated by having access to a data analytics environment (see Obs. #5).

Related Data & Information

- The Fraud Prevention Team provided several examples of reports created that did not contain all the information necessary to make them usable.
- The Fraud Team indicates that the time involved with having custom reporting built and tested is often impracticable.

Potential Solution Architecture

Approach: Building a strong fraud risk management reporting capability involves a multifaceted process that can include several critical components.

1) *Option #1* – Establish consistent data extraction:
    a. DMV can consider establishing a reliable and efficient extraction of data from OLIVR for the fraud unit. This could be accomplished through an ETL/ELT tool or API that automatically extracts data at scheduled intervals from OLIVR (Obs. # 4 Solution Architecture)
    b. DMV can explore integrating with ODOT's advanced data analytics ecosystem to conduct thorough data analysis. This ecosystem can support data visualization, advanced analytics, and machine learning capabilities. Such tools, when utilized effectively, can assist in developing custom-built analytics dashboards for visualization. Additionally, as mentioned in Obs. #5, a centralized repository for storing extracted data would facilitate the performance of advanced analytics by the fraud unit.
    c. DMV can perform an assessment of personnel knowledge gaps, focusing on analytics and data analysis skills. Building a capable analytics team to handle increased fraud detection tasks and lead investigations effectively based on the adoption of advanced analytics is crucial to combating fraud, waste, and abuse. Additionally, DMV may also consider evaluating the size and structure of the fraud team in performing the requirements and responsibilities in serving the countering fraud mission of the organization. This evaluation should include a comparative analysis of fraud team sizes and positions in other states to identify best practices and optimize the team's effectiveness. The results of these assessments may require DMV to invest in upskilling current staff and/or, hiring additional skilled analysts (e.g., data scientist

professionals), in addition to providing analytics and fraud detection training courses to staff.

d. Once these technical environments, resources, and extraction capabilities are set up, the fraud unit may adopt a Fraud Risk Management Framework that is dynamic and evolves with emerging fraud threats to be able to strengthen their current Fraud Risk Management Reporting capabilities.

    i. An effective Fraud Risk Management Framework requires a proactive approach to identifying, assessing, monitoring, and mitigating risks. Best practices include strong governance and leadership commitment, regular fraud risk assessments, robust internal controls, a fraud response plan, a fraud-aware culture, leveraging technology and data analytics, regular reviews and enhancements, and integration with overall risk management.

2) *Option #2* – Implement a cloud-based fraud risk management technology stack:

e. To be able to fully apply the results of the Fraud Risk Management Framework, DMV should consider adopting a fraud risk management technology that leverages AI and ML models to detect fraud; integrating a risk scoring engine that enables organizations to identify and prioritize high-risk areas. This can also support a streamlined investigative process, allowing for efficient tracking and resolution of cases based on prioritization scores and proper team resource allocation. Additionally, the exploratory reporting engine can offer industry-leading capabilities to increase program transparency and provide valuable insights from various data sources, ultimately helping DMV's Fraud Unit proactively detect and prevent fraudulent activities.

Solution Profiles:

Option #1:

Time	***Cost***	***Complexity***	***Impact***
Low	Medium	Medium	Medium

Option #2:

Time	***Cost***	***Complexity***	***Impact***
Medium	Medium	High	High

Business Rationale

DMV fraud unit's concerns about the quality and availability of OLIVR's standard reporting are shared by other units within DMV, highlighting a broader issue. The fraud unit plays a crucial role in maintaining the integrity of DMV data, especially in the context of increasing reports of fraud within the motor vehicle association professional community, both nationally and internationally. Since the pandemic, identity fraud and other fraudulent activities against government agencies have surged, underscoring the need for DMV's fraud unit to be equipped with the necessary tools and data to effectively fulfill its mission.

Implementing a robust fraud risk management framework for reporting and fraud identification can significantly enhance DMV's ability to proactively detect and mitigate fraudulent activities, further safeguarding its operations and resources. Such a framework would improve data integrity and reliability, leading to more accurate reporting and decision-making. Additionally, fostering a culture of transparency and accountability would boost stakeholder confidence and ensure compliance with regulatory requirements, ultimately strengthening DMV's overall operational effectiveness.

Obs. #	Predicate #	Topic
11	N/A	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 dealt with after there have been operational challenges; they are not proactively managed or prevented.

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 to establish 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 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 DMV with additional 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 solutions, such as a Governance, Risk and Compliance (GRC) software platform. GRC technology provides a structured mechanism to enable the most common workflows and reporting associated with risk management.

Related Data & Information

- There is currently no GRC management solution, risk scoring, nor dedicated risk management program.
- ODOT, in partnership with qualified security professionals, performs security control audits on its IT operating environment. Remediation of control gaps are ranked and prioritized based on vulnerability risk. However, these control improvements do not address all aspects of risk associated with data integrity, for example, risks assumed or created through changes in operational rules do not always drive to a level of process detail required for thorough data integrity risk management.
- File transfers are reviewed daily for success or failure. Email alerts are sent to the staff when tasks fail.

Potential Solution Architecture

Approach: DMV can consider a solution architecture leveraging the GRC model and the NIST Risk Management Framework.

1) The GRC model will provide a structured mechanism to formalize the processes of setting priorities, allocating resources, and launching projects related to data integrity. A critical component of this architecture is the formalization and prioritization of risks, including, operational, financial, strategic, and compliance, which will transform the current semi-formal and reactive methods into a proactive regimen.
    a. The risk prioritization component involves systematically identifying, assessing, and ranking data integrity risks based on their potential impact and likelihood, ensuring that the most critical risks are addressed first. This may help DMV establish a posture where data integrity risks are identified, assessed, and mitigated before they cause operational challenges.
    b. The adoption of a robust remediation process that includes the development and implementation of targeted action plans to address identified vulnerabilities and deficiencies, prioritizes remediation efforts based on risk severity and impact. It also supports the development of acceptable levels of residual risk to ensure alignment with the organization's risk appetite and tolerance levels. This approach will enhance DMV's risk management framework, improve operational resilience, and ensure continued compliance.

By establishing a '*monitor, review, and assess*' process, DMV can maintain situational awareness of emerging data integrity issues, ensuring that both data assets and the systems housing them are managed, while also practicing ongoing optimization of risk thresholds, prioritization scale and attributes. Typically, GRC frameworks are implemented using specialized software platforms that provide tools for risk assessment, policy management, compliance tracking and reporting. Deploying GRC technology may enable common workflows and reporting associated with risk management, DMV can leverage existing technology owned or licensed by DMV to provide suitable options for effective risk management.

Additionally, the implementation of this solution architecture will involve the participation of a defined group of ODOT HQ and DMV leaders, supported by functional resources responsible for executing prescribed risk management activities. Therefore, clear decision rights and responsibilities may be documented to ensure accountability. Risk management processes may be defined, specifying task ownership, and scheduling related activities, with checkpoints for data integrity measurements and periodic updates to DMV leadership.

2) Utilizing the NIST Risk Management Framework can provide DMV with a structured approach to managing risk, particularly the aspects related to identifying controls around information security and cybersecurity for data integrity, ensuring compliance with national standards, and enhancing the overall security posture of an organization. Lastly, a crucial aspect of the NIST framework is its emphasis on the importance of continuous monitoring and improvement to ensure that security controls remain effective over time. This approach will lead to more data integrity, proactive risk management, and enhanced operational efficiency.

Solution Profile:

Time	*Cost*	*Complexity*	*Impact*
Low	Low	Medium	Medium

Business Rationale

Risk management, as a discipline, provides a structured and deliberate approach for organizations to proactively identify and mitigate risks. When risks manifest and become active threats, formalized risk management enhances the agility with which organizations identify, respond to, and resolve those threats. Specifically, in the context of data, implementing or expanding risk management processes contributes significantly to achieving and sustaining adequate levels of data integrity.

By implementing this solution architecture, DMV will experience improved data integrity, proactive risk management, enhanced operational efficiency, and better regulatory compliance. Leveraging frameworks and tools such as the NIST Risk Management Framework, PMBOK (Project Management Body of Knowledge), DMBOK (Data Management Body of Knowledge) (v.2) frameworks for data governance and data management, GRC technology, and data quality management processes, DMV can transform its data integrity and risk management practices, ensuring a robust and reliable data ecosystem.

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

Observation

DMV’s current Know Your Customer (KYC) processes in the call center and field offices require minimal information and reflect an area for potential improvement. In most observations, a DMV customer needed to know only basic information about 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's use of its data, the reality is that DMV serves as a trusted source of identity for a large 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 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 likelihood of adoption. 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 more 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 identity proofing information from DMV customers 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 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.

Related Data & Information

N.A.

Potential Solution Architecture

Approach: Enhancing DMV's KYC processes and procedures can incorporate lower impact solutions that leverage common capabilities to more advanced use of technologies that can increase customer security, trust, and confidence in DMV's ability to protect vital information.

1) *Option #1* – Conduct outreach and collaborate with peer organizations to strengthen KYC procedures.
   a. In addition to conducting a risk assessment concerning the various identity documents DMV retains and processes, DMV should evaluate the KYC procedures of other state DMVs. Furthermore, collaborating with the American Association of Motor Vehicle Administrators (AAMVA) to identify best practices and lessons learned will facilitate the implementation of enhanced KYC measures. These measures should be tailored to address the specific risks associated with DMV's transactions and the utilization of various datasets.
   b. DMV can adhere to Identity Assurance Levels (IAL) defined by NIST SP (Special Publication) 800-63-3, specifically on IALs where checks performed against data provided by a customer are complemented by additional verification methodologies and include a supervised remote or in-live session to link documents provided by a customer to whom they claim to be.
2) *Option #2* – Evaluate and select technological solutions to bolster DMV's KYC procedures in field offices and call centers.
   a. DMV can consider implementing an identity validation solution that incorporates standard proofing components such as document verification, database checks, multifactor authentication, fraud risk indicator deployment, and risk scoring. These capabilities are designed to immediately strengthen existing tools and procedures while meeting regulatory compliance and bolstering operational efficiency.
   b. DMV can consider integrating various biometric authentication methods, to supplement existing KYC procedures and identity proofing capabilities to enhance security by requiring biological traits that are difficult to replicate.
   c. DMV can consider deploying Robotic Process Automation (RPA) to address the collection, processing, and validation of KYC documents. RPA can assist with automating routine tasks, thus enhancing data integrity while ensuring required KYC processes are documented and traceable.
   d. DMV can implement AI technologies to automate the verification of customer identities. These technologies can analyze vast amounts of data quickly and accurately, identifying patterns and anomalies that may indicate anomalous behaviors or potentially fraudulent activity.
   e. DMV can also leverage the voluminous data sets available from OLIVR and apply advanced analytics to develop risk profiles to inform future risk assessments and further application of previously identified solutions.

While evaluating the need for enhancing DMV's KYC processes and procedures, DMV can consider critical cyber enabling requirements, such as security, training, and the supporting infrastructure needed to implement these solutions.

Solution Profile:

Option #1

Time	*Cost*	*Complexity*	*Impact*
Low	Low	Low	Low

Option #2

Time	*Cost*	*Complexity*	*Impact*
High	High	Medium	High

Business Rationale

Data integrity is rooted in the accuracy of transactions that affect 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 DMV, its customers, other government agencies, and the broader community by more rigorously ensuring the sustainment of data integrity. Additionally, advanced automated KYC procedures can streamline customer interactions, reduce manual workloads, minimize errors, and improve overall efficiency.

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 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 the extent and nature of these controls to further enhance data integrity. Opportunities also exist to renegotiate the scope and content of data transmissions with data exchange partners (e.g., courts) to facilitate higher levels of internal control. Furthermore, opportunities exist to improve the completeness and accuracy of the catalog of data interchange interfaces that DMV maintains.

Action

DMV can consider enhancing data transmission reconciliation controls, with an emphasis on the completeness, accuracy, and timeliness of 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 an update to the data interchange interface catalog. 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 to enhance data validation routines. For example, this could include record count reconciliation controls to support completeness, uniformly applied hash total reconciliation controls (i.e. quantitative methods to help ensure the accuracy of data received versus data sent) controls to support accuracy, and/or timestamp versus schedule comparisons to support timeliness. Designing and implementing these controls may likely require collaboration with DMV's data exchange partners, to include the possibility of redefining the data transmission file contents to allow for improved internal controls 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 catalog 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 catalog. Other metadata, as deemed necessary by DMV policy or guidance, should also be included. DMV data trustees and data stewards can collaborate with qualified internal control professionals (e.g., IT auditors, risk management professionals) 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. They can also monitor the data exchange dashboard for missing exchanges or anomalies.

Process

Once the data interchange interfaces are cataloged 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 be periodically tested both by ODOT and 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 catalog. The completeness, accuracy, and timeliness of updates to the catalog can also be periodically evaluated by ODOT and by a qualified auditor. Finally, it is possible that data transmission errors can originate from outside of ODOT or 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.

Related Data & Information

- All data interfaces are documented in the OLIVR Gateway Manager as well as the data encryption solution. All real-time interface traffic, documentation for the real-time interfaces, and file processing interfaces can be viewed from the application in the Gateway Manager.
- There are approximately 300 encryption solution tasks comprised of inbound, outbound, and internal to ODOT.
- OLIVR has 35 inbound connections, 33 outbound connections, and 1 bidirectional connection. There are 25 inbound and 61 outbound OLIVR web service connections.
- All activities in the OLIVR system are logged and snapshots of the users' interactions are recorded in OLIVR with full auditing capabilities. All transfers are monitored daily for successful completion.
- The current transmission process is manually monitored and measured against the historical system processing. The inventory in development will allow for the creation of alerts for atypical transfer frequency events. Validation controls for incoming data resides within the OLIVR system's intake.
- The OLIVR system will create an error when an interface transmission is not complete by creating an 'intervention' task for the team to review. These are reviewed daily, and if errors exist the team creates an SQR to address the error and complete the processes. Also, the system can alert when a critical file fails to generate. The OLIVR server that runs the nightly batch services will auto send emails/texts when configured.
- The OLIVR system itself does more in-depth validations for many files prior to ingestion into the database tables, based on the risk of malformed data, to ensure the data is valid.

Potential Solution Architecture

Approach: Enhancing data transmission controls will reinforce existing procedures and help instill greater trust and confidence in DMV's customers, data exchange partners, and stakeholders in DMV's ability to securely handle sensitive data.

1) DMV can consider the implementation of enhanced automated data reconciliation tools that continuously monitor and reconcile data transmissions between systems. DMV can nominate critical data points, such as accuracy and completeness, for verification. The system should include an immediate alerting mechanism upon identification of discrepancies and include a specific focus on error handling.
2) DMV can consider implementing additional data validation rules at both the sending and receiving ends to ensure only validated data is transmitted and accepted. This prevents invalid data from entering the system, reducing the need for reconciliation. The enhanced rules can be based upon business or regulatory requirements, data integrity, security, and the results of assessments or best

practices evaluations. These additional data validation rules can be deployed in the data analytics environment referenced in Obs. #5.

3) DMV can consider replacing or strengthening its end-to-end data encryption and integrity checks. Strengthened encryption for securing data transmissions and integrity checks reduces the risk of data corruption, data tampering, and ensures customer confidence and trust in DMV's ability to protect sensitive data.
4) DMV can consider developing and implementing a centralized monitoring and reporting system, including a dashboard, to provide real-time updating of data transmissions and reconciliations. Such a system would enable awareness and insights to transmission effectiveness as well as immediate notifications of anomalies that warrant timely mitigations.

While assessing the need for potential enhancements to data transmission controls, DMV can consider including the cyber resources and staff necessary to implement the solution and monitor its effectiveness. By focusing on data security, system integration, regulatory compliance, scalability, cost, and user training, DMV can drive a successful implementation that enhances data protection and operational efficiency.

Solution Profile:

Time	***Cost***	***Complexity***	***Impact***
Medium	Medium	Medium	High

Business Rationale

Data interchange is a key aspect of ODOT and 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 requires 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 because Oregon law prohibits it. REAL ID issuances require positive verification through national databases that verify the legitimacy of US passports and lawful status. In both REAL ID and non-REAL ID transactions, DMV utilizes a manual inspection process conducted by field operations personnel. In the case of non-REAL ID issuances, DMV relies entirely on a manual inspection process, and the quality control check is limited to verifying the consistency between the information the staff documented on paper and the information that was entered into the system. 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. In instances of REAL ID issuance, even if capturing document images does not eliminate human error, it does provide a more definitive method for post-transaction verification. The sole 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

DMV can consider reviewing relevant statutes 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

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

Process

DMV can evaluate and then document the results of its review in a position paper, including an analysis of potential opportunities to enhance data integrity through an agreed upon strategy leveraging technology. DMV leadership can evaluate the conclusions of the analysis and determine the most effective steps available and decide upon those for immediate and long-term implementation. Once those steps are identified, DMV can explore opportunities to implement more efficient and effective automation solutions, including an additional 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 DMV's environment, making it accessible to relevant personnel. Additionally, DMV should consider whether certain parts of the position paper should be shared with other Oregon state government agencies or the public.

Related Data & Information

- There are Oregon statutes, Administrative Rules, Field Driver License Procedure Manual chapters, and Field Services Administration Manual chapters that apply to the identity requirements for standard and REAL ID credentials.
- Portions of the Code of Federal Regulations also apply to REAL ID credentials.

Potential Solution Architecture

Approach: In understanding the details of the functional and technical processes involved with identity and voter eligibility documentation verification, certain policy and regulatory factors govern these processes. Those factors require careful analysis to support DMV's prospective decisions with respect to enhancing its operations. DMV had a vested interest in continuing to comply with all governing compliance obligations with respect to document scanning and retention.

1) Once DMV selects the enhancement changes it will implement to identity and voter eligibility documentation verification, DMV can engage all appropriate parties within ODOT to develop a proposed position with respect to how DMV will continue to comply with its compliance obligations.
2) DMV can begin by developing a complete inventory of the relevant compliance obligations relating to this topic.
3) On a line-item basis, DMV can then determine and document its position for how it will continue to maintain a posture of compliance with its obligations.
4) Once fully compiled, DMV can submit the compliance strategy to appropriate parties within ODOT for review and consensus.
    a. Ultimately, this review process could involve collaborative review with state officials outside of ODOT.

Solution Profile:

Time	*Cost*	*Complexity*	*Impact*
Low	Low	Low	High

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, to enhance data integrity while still complying with related law. These advanced technologies should only be developed from a posture of compliance with applicable guidance and requirements, to remain within the boundaries of DMV policies relating to data integrity.

Final Report Summary

The final report presents 14 Observations and related opportunities, focusing on the themes of data management, automation, extraction, quality, analytics, governance, internal controls, resources, and training. The Observations highlight areas where processes and controls were incomplete, insufficient, or otherwise limited. The potential solution architectures focus on assessing, analyzing, and enhancing the processes and controls in those areas to minimize and mitigate the identified risks. The final opportunities also include refined Business Rationales for consideration.

Deloitte used the Preliminary Review Report to validate the initial findings with ODOT HQ and DMV personnel and receive additional feedback. This step was crucial in confirming our preliminary Observations accurately reflected the current state of data integrity and aligned with the operational realities of DMV and the expectations of its stakeholders. Information requests and interviews with personnel assisted in this process. Further documentation was gathered to gain deeper insights into the challenges faced by ODOT.

As a result of the validation and continued conversations with ODOT HQ and DMV stakeholders in Phase 2, the Final Review Report includes actionable steps that correspond to each Observation and potential action. This was structured around the People, Process, and Technology framework. The 14 opportunities fall within four distinct categories: implementing data governance and risk management; bolstering data analytics capabilities; enhancing human capital and policy analysis; and optimizing operational processes. This report consistently highlights the importance of data and its accuracy, application, and reliability throughout all DMV operations.

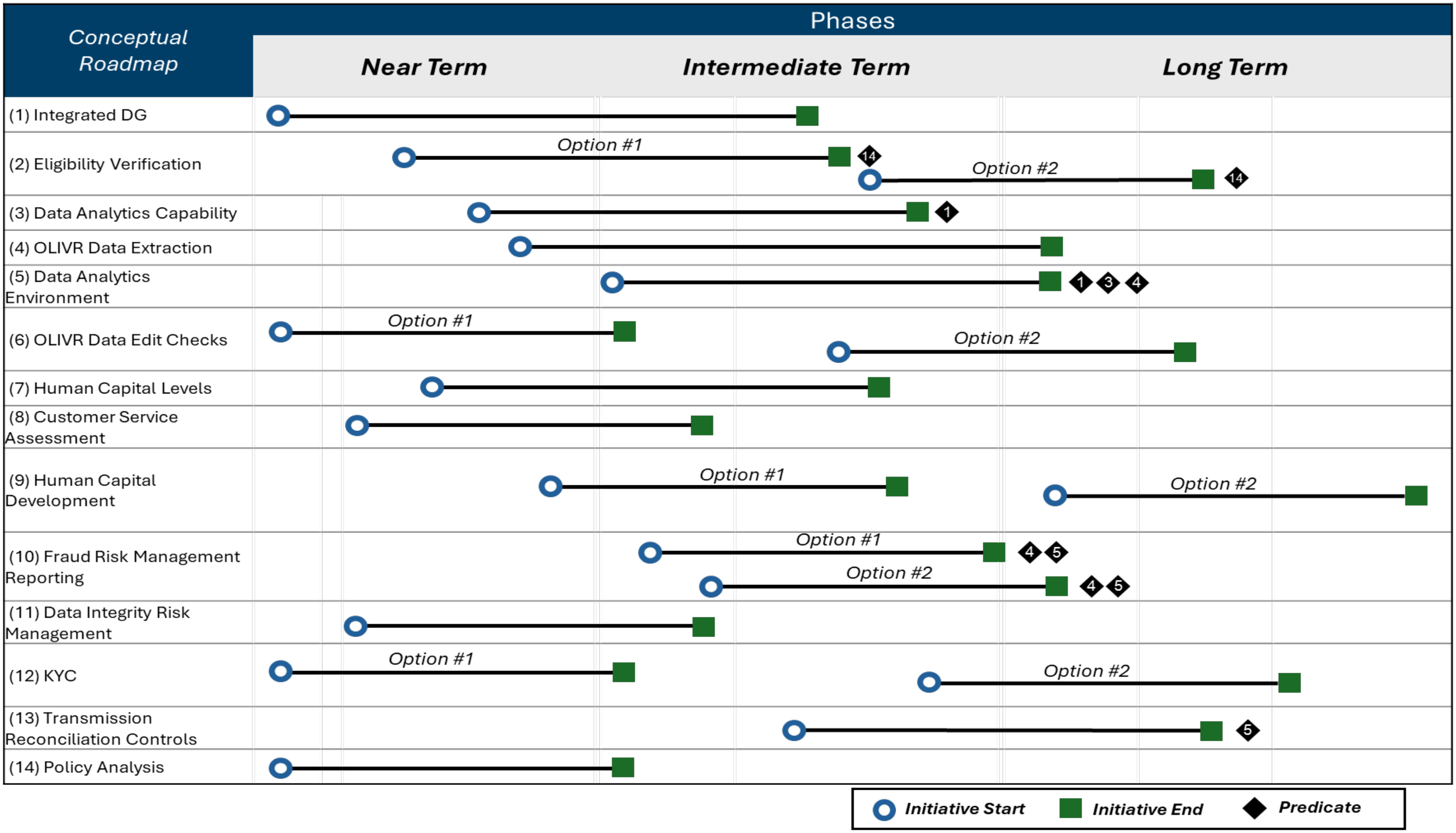
Suggested Next Steps for ODOT’s Consideration

After an evaluation and discussions with ODOT HQ and DMV personnel, Deloitte has identified key areas for ODOT to consider for enhancing data integrity. The roadmap below (see Figure 2: Conceptual Roadmap) is characterized by three phases: **Near, Immediate, and Long Term**. These phases are strategically aligned with the Observations and Solution Architectures in accordance with DMV's mission and priorities. This roadmap is designed to address current challenges as well as offer scalable and sustainable solutions for future needs, with a deep understanding of each solution's feasibility, potential impacts, and long-term viability across resources, processes, and infrastructure.

The below roadmap should be viewed as conceptual as ODOT will need to determine, which, if any, of the Observations and Solution Architectures may be appropriate for implementing.

ODOT will need to consider such things as seeking additional budget, adding or redirecting staff resources, statutory requirements, impacts on and alignment with existing organizational priorities, re-evaluation of existing priorities to determine potential alignment with solution architectures, as well as further evaluation of solution architectures to ensure integration with ongoing change management initiatives.

Figure 2 - Conceptual Roadmap



Potential Solution Architecture Profile Summary

The Potential Solution Architecture Profile Summary (see Table 2: Potential Solution Architecture Profile Summary) provides a strategic overview connecting the individual Observations with their associated ratings. This summary provides estimates of **time, cost, complexity, and impact** for all Potential Solution Architectures presented in this report and is intended to facilitate an aggregate analysis of options available for ODOT's consideration.

Table 2 – Potential Solution Architecture Profile Summary

Observation	Solution Ratings			
1 - Integrated Data Governance				
	Time	***Cost***	***Complexity***	***Impact***
	Medium	Medium	Medium	High
2 - Automating Eligibility Verification				
	Option#1			
	Time	***Cost***	***Complexity***	***Impact***
	Medium	Low	Low	Low
	Option #2			
	Time	***Cost***	***Complexity***	***Impact***
	High	High	High	High
3 - Integrated Data Analytics Capability				
	Time	***Cost***	***Complexity***	***Impact***
	Medium	Medium	Medium	High
4 - OLIVR Data Extraction Capability				
	Time	***Cost***	***Complexity***	***Impact***
	Medium	High	Low	Medium
5 - Data Analytics Environment				
	Time	***Cost***	***Complexity***	***Impact***
	Medium	Medium	Medium	High
6 - Enhanced Data Edit Checks in OLIVR				
	Option #1			
	Time	***Cost***	***Complexity***	***Impact***
	Low	Medium	Low	Medium
	Option #2			
	Time	***Cost***	***Complexity***	***Impact***
	Medium	Medium	High	High
7 - DMV Human Capital Levels				
	Time	***Cost***	***Complexity***	***Impact***
	Medium	Medium	Medium	Medium

Observation	Solution Ratings			
8 - Customer Service Positions Assessment				
	Time	***Cost***	***Complexity***	***Impact***
	Low	Low	Medium	Medium
9 - Human Capital Development	*Option #1*			
	Time	***Cost***	***Complexity***	***Impact***
	Medium	Medium	Low	Medium
	Option #2			
	Time	***Cost***	***Complexity***	***Impact***
	Medium	Medium	High	High
10 - Fraud Risk Management Reporting				
	Option #1			
	Time	***Cost***	***Complexity***	***Impact***
	Low	Medium	Medium	Medium
	Option #2			
	Time	***Cost***	***Complexity***	***Impact***
	Medium	Medium	High	High
11 - Data Integrity Risk Management & Prioritization				
	Time	***Cost***	***Complexity***	***Impact***
	Low	Low	Medium	Medium
12 - KYC Systems and Procedures				
	Option #1			
	Time	***Cost***	***Complexity***	***Impact***
	Low	Low	Low	Low
	Option #2			
	Time	***Cost***	***Complexity***	***Impact***
	High	High	Medium	High
13 - Data Transmission & Reconciliation Controls				
	Time	***Cost***	***Complexity***	***Impact***
	Medium	Medium	Medium	High
14 - Policy Analysis				
	Time	***Cost***	***Complexity***	***Impact***
	Low	Low	Low	High

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.

Application Programming Interface (API)- rules and protocols that allow different software applications to communicate with each other.

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 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.

Coordinating Data Stewards – a single staff person designated by their business leadership team to serve as a data governance and stewardship coordinator/facilitator and change champion for a Division, Business Area, or Delivery and Operations Branch.

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 Debt - refers to the accumulation of suboptimal data practices and decisions over time, which can lead to increased costs and efforts required to manage, maintain, and improve data quality.

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. Data integrity rules and standards help prevent unauthorized modifications and ensure 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 Analytics Ecosystem - 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 Leakage - the inadvertent exposure of sensitive information to unauthorized parties, either due to technical vulnerabilities or human error.

Data Management Body of Knowledge (DMBOK) - a framework that outlines the essential practices, principles, and guidelines for effective data management within an organization.

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 - Managers with decision making authority and accountability for data related to their key business line functions and/or program areas (e.g., planning, project delivery, highway operations, highway assets, driver licenses, public transportation, etc.).

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

Expert Review Team (ERT) - a group established by the Governor of Oregon that is made up of transportation department personnel from various states. The purpose of the group is to provide ODOT input on the Data Integrity Review.

Extract, Load, Transform (ELT) Process - a process used in data warehousing and data integration to acquire data from various source systems (Extract), copy them into a centralized data repository (Load), and use the processing power of the data repository to convert them in situ into a form/format that can be used for business processes and analytics (Transform).

Extract, Transform, Load (ETL) Process - a process used in data warehousing and data integration to acquire data from various source systems (Extract), convert them while in transit into a form/format that can be used for business requirements and for analytics (Transform), and copy them into a centralized data repository (Load).

Federal Standards - Federal standards include 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.

Identity Assurance Levels (IAL) - refers to the levels of confidence or assurance that a system can have in a user’s identity and credentials. There are three levels:
IAL 1 (Some confidence): Completed via self-assertion, often a password.
IAL 2 (High confidence): Provides higher confidence in the user's identity.
IAL 3 (Very high confidence): The most robust level of identity assurance.

Intelligent Optical Character Recognition (iOCR) - iOCR is an advanced form of Optical Character Recognition (OCR) used for recognizing and digitizing handwritten text and often uses machine learning techniques to improve its accuracy over time.

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.

Oregon Revised Statutes (ORS) 276A.365 (ORS276A.365) - pertains to the state's regulations regarding information management by state agencies. Specifically, ORS 276A.365 outlines the responsibilities to manage data and information throughout their lifecycles, ensuring collection and creation that supports downstream processing and use, accessibility and interoperability, privacy and confidentiality, scalability and flexibility, and extractability in multiple formats.

Project Management Body of Knowledge (PMBOK) - a framework that outlines the standards, guidelines, and best practices for project management.

Robotic Processing Automation (RPA) - is the term used for software that partially or fully automates human activities that are manual, rule-based, and repetitive. They work by replicating the actions of an actual human interacting with one or more software applications to perform tasks such as data entry, process standard transactions, or respond to simple customer service queries.

State Standards - state standards in 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 DMV headquarters.

During site visits and in 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 HQ 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
- Data Transmission Controls Specialist
- Error-Proofing Team
- Fraud Team

DMV Contractors

- FAST personnel

ODOT Personnel

- Chief Information Officer
- Chief Data Officer
- Chief Data Steward

Appendix 4: Documents Reviewed

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

- Oregon State DG Policy 107-004-160
- ODOT Managing Data Quality Training for Data Stewards
- ODOT Data Stewardship Training Modules
- ODOT Data Governance Plan 2025-2026
- 2017 ORS 276A.350-374 (Oregon statutes on Data Governance, public records)
- ODOT Data Stewardship Roles Fact Sheets
- ODOT Data Governance, History, Groups, and Training
- ODOT Data Literacy Efforts, May 23, 2024
- *Draft* ODOT Data Quality Management Plan
- *Draft* ODOT Managing Data Quality Training
- ODOT DMV Data Integrity Review Phase 2
- 2021 DMV Exit Survey Detail by Question
- May 2023 AAMVA Recruitment and Retention Survey
- June 2021 AAMVA Attrition After COVID Survey

Appendix 5: Strategic Challenges and Solutions Crosswalk

The following Strategic Challenges and Solutions Crosswalk (see Table 3: Strategic Challenges & Solutions Crosswalk) is an analysis that maps out key challenges faced by ODOT to Deloitte's proposed corresponding solutions. This crosswalk identifies key focus areas such as training and development opportunities, resource constraints, opportunities for automation, and data extraction and reporting, and aligns them with specialized solutions that leverage Deloitte's extensive industry experience and resources.

Table 3 - Strategic Challenges & Solutions Crosswalk

		Challenges									
	Strategic Challenges & Solutions Crosswalk	Limited Integration of Data Governance (ODOT & DMV)	Voter Identification Integrity	Insufficient Data Extraction, Analytics & Reporting Tools	Unmet Human Capital Training and Development Needs	Inadequate Staffing Levels & Elevated Workforce Turnover Rates	Manual Processing for Error Proofing	Limited Fraud Risk Management Reporting	Limited Data Integrity Risk Management	Insufficient KYC Procedures	Limited Data Transmission Controls
Solutions	Enhance Performance Management Processes	x			x						
	Implement Technologies for Process Automation		x				x				x
	Establish Centralized Data Governance and Advanced Analytics	x		x					x		
	Enhance Data Analytics Capabilities			x				x			
	Allocate Personnel for Data Integration	x									
	Implement Enhanced Data Validation and Automation Tools		x				x				x
	Identify Productivity Constraints				x	x	x				
	Identify Critical Skills Gaps	x			x	x			x		
	Assess and Modernize Training Programs				x	x			x	x	
	Develop a Fraud Risk Management Framework							x			x
	Implement GRC and NIST Framework								x		
	Deploy Advanced Technologies and Establish Best Practices		x		x		x		x	x	
	Strengthen Data Transmission Controls										x
	Analyze Policy and Regulatory Factors		x		x	x		x		x	

Deloitte.