



# An Audit of Data Management and Data Governance at the Department of Motor Vehicles

- The Department did not update its permitted data disclosure contracts to address privacy requirements that went into effect in June 2021.
- The Department did not comply with all statutory requirements for data management.
- The Department did not implement a recommendation regarding user access made in a prior audit report.

Lisa R. Collier, CPA, CFE, CIDA  
State Auditor

The Department of Motor Vehicles (Department) had significant weaknesses in its overall data governance and in certain data management processes for its Registration and Title System (RTS) data. The Department should improve its oversight and administration of key data management functions as it undertakes a multi-year, \$131 million project to modernize RTS.

- [Background](#) | p. 4
- [Audit Objectives](#) | p. 16

*This audit was conducted in accordance with Texas Government Code, Sections 321.013 and 321.0132.*

## **PRIORITY**

### **PROTECTION OF CONSUMER PRIVACY**

The Department did not implement the required safeguards to protect consumers' information from unauthorized disclosures.

[Chapter 1 | p. 6](#)

## **HIGH**

### **DATA GOVERNANCE**

The Department did not comply with all statutory requirements designed to safeguard data or establish and implement key data governance processes.

[Chapter 2 | p. 10](#)

## **NOT RATED**

### **PRIOR RECOMMENDATION FOLLOW-UP**

The Department did not implement a recommendation made in a prior audit report.

[Chapter 3 | p. 14](#)

---

## Note on Confidential Findings

---

To minimize security risks, auditors communicated in a separate report to the Department details about other audit findings related to certain security weaknesses.

**PRIORITY**

One chapter was rated Priority, because of issues that could critically affect the Department's ability to effectively manage and govern its data. Immediate action should be taken to reduce the risk.

**MEDIUM**

Three chapters were rated Medium, indicating moderate risk. Action is needed to address the noted concerns and reduce risks to a more desirable level.

Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Government Auditing Standards*, certain information was omitted from this report because that information was deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. Under the provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

---

## Summary of Management's Response

---

Auditors made recommendations to address the issues identified during this audit, provided at the end of certain chapters in this report. The Department agreed with the recommendations.

---

## Ratings Definitions

---

Auditors used professional judgment and rated the audit findings identified in this report. The issue ratings identified for each chapter were determined based on the degree of risk or effect of the findings in relation to the audit objective(s).

**PRIORITY:** Issues identified present risks or effects that if not addressed could *critically affect* the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern(s) and reduce risks to the audited entity.

**HIGH:** Issues identified present risks or effects that if not addressed could *substantially affect* the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.

**MEDIUM:** Issues identified present risks or effects that if not addressed could *moderately affect* the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.

**LOW:** The audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks *or* effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

For more on the methodology for issue ratings, see [Report Ratings](#) in Appendix 1.

# Background Information

---

## Registration and Title System Modernization

---

**Registration and Title System.** The Registration and Title System (RTS) is the Department of Motor Vehicles' (Department) core business technology system. RTS contains consumer registration and title information, including personal identifying information such as name and address. Online vehicle registration portals, county tax assessor-collector offices, automobile dealers, and other motor vehicle-related businesses all make use of RTS data.

**RTS Modernization Project.** The Department is in the process of a multi-year, \$131 million project to replace RTS and its associated applications with a new, modernized system that will be compatible with necessary advancements in technology.

---

## Texas Data Management Framework

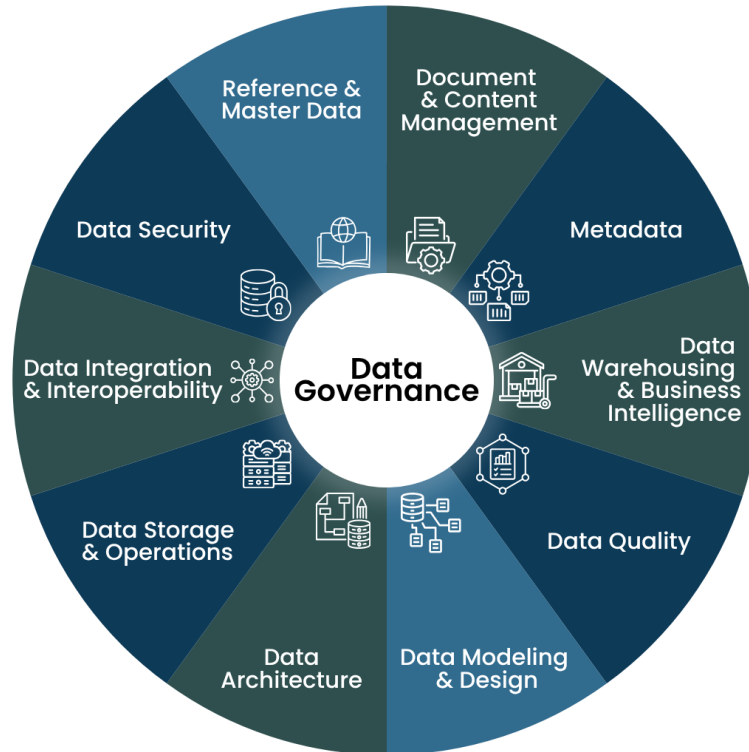
---

The Department of Information Resources (DIR) developed the Texas Data Management Framework (Framework) to provide state agencies with a set of best practices and a guide to the crucial components of data management.

The Framework is based on DAMA International's *Data Management Body of Knowledge* (DAMA-DMBOK) and describes the core principles of data management—including data governance, architecture, quality, storage, and security—among other foundational elements that equip organizations for success (see Figure 1 on next page).

Figure 1

### *Data Management Knowledge Areas*



Source: DIR’s Texas Data Management Framework.



**PRIORITY**

## Chapter 1 Protection of Consumer Privacy

The Motor Vehicle Records Disclosure Act authorizes the Department of Motor Vehicles (Department) to disclose personal information associated with motor vehicle records to approved companies for a reasonable fee (see text box for examples of permitted data disclosures). The Department entered into contracts to provide allowable vehicle registration and title information to companies.

However, the Department did not comply with all statutory requirements designed to protect that consumer information and allow the State and consumers to pursue remedies in the case of unauthorized disclosures.

### Data Disclosures

The disclosure of consumer data is permitted for certain uses, such as:

- A towing company notifying the owner of a vehicle that was towed or impounded.
- An insurer processing claims.
- A toll road operator communicating with road users.

Source: Texas Transportation Code, Chapter 730.

---

**The Department did not implement the required safeguards to protect consumers' information from unauthorized disclosures.**

---

Specifically, the Department continued to provide data to companies—including consumers' personal identifying information such as names, addresses, and vehicle registration and title data—without updating certain contracts to address the state consumer privacy requirements that went into effect in June 2021.<sup>1</sup>

As of October 2025, the Department had 1,778 permitted data disclosure contracts with companies. This includes 42 bulk contracts, on which the State imposed additional requirements to protect the privacy of consumer data. Bulk

---

<sup>1</sup> The Legislature amended the Motor Vehicle Disclosure Act in June 2021 to implement additional safeguards to protect consumer privacy.

contracts present the greatest risk of unauthorized disclosure because they permit the disclosure of at least 250 motor vehicle records containing personal information and, in some cases, allow for the disclosure of the Department's entire database of records.

The Department took certain steps to verify the identity of the companies, their planned business use for the requested data and, if applicable, that the companies were licensed and registered. However, of the 25 contracts tested, 22 (88 percent) did not incorporate all the required consumer privacy protections—including 18 bulk contracts.

Specifically, those 22 contracts did not:

- Prohibit the redisclosure of records to unauthorized recipients and establish fines for noncompliance.
- Require that companies instruct unauthorized recipients to delete any information obtained.
- Establish civil suit liabilities for unauthorized disclosures.

The 18 bulk contracts also did not require the companies to:

- Comply with the prohibition of the sale or redisclosure of personal information for the purpose of marketing extended vehicle warranties.
- Notify the Department of any system security breach within 48 hours.
- Provide the Department with an annual report on all third parties to which the data was redisclosed.
- Include a provision in each subcontract for redisclosure that the third party obtaining consumer information must comply with federal and state laws pertaining to that information.

Without required provisions establishing protections in Department contracts, the Department is not able to adequately monitor either the initial data disclosures to contracted companies or the resale of data to third parties, placing consumer data at increased risk of unauthorized disclosure.

---

## The Department did not verify that its companies with bulk contracts had the required financial coverage for potential unauthorized data disclosures.

---

As discussed above, bulk contracts have additional minimum requirements for protecting the State's interests related to the use and disclosure of motor vehicle registration and title data. However, the Department did not have a process to obtain proof or otherwise verify that its bulk-contract companies complied with those requirements.

Specifically, as of October 2025, the Department:

- Had not verified that 17 (89 percent) of 19 companies tested had posted the required \$1.0 million performance bond (a bond that establishes a financial consequence if a company fails to fulfill the obligations stated in the contract).
- Had not verified that 13 (68 percent) of 19 companies tested held at least the required \$3.0 million in general liability and cyber-threat insurance coverage.

As a result, the Department cannot demonstrate that it is providing consumers' personal data only to companies that can meet the financial requirements to cover potential losses and/or damages in the event of any type of unauthorized disclosure of that information.

---

## Recommendations

---

The Department should:

- Update all existing permitted data disclosure contracts to incorporate applicable consumer privacy protection requirements and monitor companies' compliance with those requirements.
- Verify bulk-contract companies' compliance with financial coverage requirements, including obtaining proof of the companies:
  - Posting a \$1.0 million performance bond.

- Holding at least \$3.0 million in general liability and cyber-threat insurance coverage.

---

## Management's Response

---

The Department agrees with the recommendations and has already completed a comprehensive review and conversion of all 2,002 permitted data disclosure contracts and user access agreements. In response to statutory changes enacted under Chapter 730, Texas Transportation Code, and corresponding amendments to Texas Administrative Code, Chapter 217, Subchapter F (November 2022), the Department undertook a major conversion and reapplication initiative for all motor vehicle record (MVR) data contracts. All contracted entities were required to reapply for access and submit updated applications, photo identification, business verification, and detailed intended use documentation.

By December 2024, all re-applications had been fully reviewed and, following extensive vetting, 1,778 were approved at staff level. Enhanced compliance reviews led to the termination of 224 contracts and accounts due to failure to reapply or lack of a valid permitted use. On April 17, 2026, the Department sent a letter to the remaining entities to give notice that their contracts will be terminated if they do not come into compliance with the bond and insurance requirements within 30 days. While affected entities have made good faith efforts to comply with these additional requirements, small businesses have reported significant and persistent barriers due to the high cost of a required \$1.0 million performance bond.

As of April 17, 2026, the status of the remaining 22 sampled contracts is as follows:

- 14 contracts have been fully executed.
- 8 contracts were provided with the 30-day notice of pending termination due to the entity's lack of compliance

Responsible Parties: General Counsel and Vehicle Titles and Registration Division Director

**HIGH**

## Chapter 2 Data Governance

The Department did not establish critical processes necessary to protect consumer data, as required by Texas statute and the Department of Information Resources' (DIR) guidelines. As a result, sensitive consumer data is at risk.

Data governance is the foundation of a successful data management program. Weaknesses in data governance prevent stakeholders from making informed and strategic decisions and ensuring data integrity.

---

### The Department did not comply with all statutory requirements designed to safeguard data.

---

The Department designated a full-time Data Management Officer, coordinated with DIR's Chief Data Officer, and increased awareness of the Department's record management programs as required. However, the Department did not establish processes for other data management requirements in Texas Government Code, Chapter 2054, that went into effect in June 2021. Non-compliance with these functions places the Department at increased risk of mishandling data, operational inefficiencies, and potential security breaches.

Specifically, the Department did not:

- Conduct and submit every other year a data maturity assessment to identify and address potential weaknesses in its data management program. The Department submitted only an initial assessment (covering 2022) to DIR in August 2025. A data maturity assessment gives management a shared understanding, and it also highlights data quality issues, security vulnerabilities, policy gaps, and technological limitations.
- Classify its data according to data privacy classifications specified in DIR's *Data Classification Guide* and Department policy. These classifications identify data containing confidential or other sensitive information. As a result, confidential consumer data is at increased risk of unintended disclosure.

- Designate individual employees as data stewards and data owners as specified in Department policy to clearly identify who is responsible for managing data quality, approving access, conducting proper data classification, and ensuring compliance with statutory requirements.

---

## The Department did not establish and implement key data governance processes.

---

The Department did not adopt the best practices outlined in DIR’s *Texas Data Management Framework Fast Start Learning Guide* and DAMA International’s Data Management Body of Knowledge (DAMA-DMBOK). Specifically, the Department did not establish the agencywide data governance processes and documents listed in Figure 2. The lack of these foundational elements could result in inconsistent and inefficient data use, poor data quality, and operational inefficiencies.

Figure 2

### *Recommended Data Governance Standards*

Component	Function
Data policies	Codify principles and management intent into fundamental rules governing data.
Business glossary	Define key business terms and help ensure that consistent language is used for data across the agency to communicate essential data concepts and terms and tie them to business functions.
Data management scope statement	Establish specific goals and objectives for a defined planning period with roles, organizations, and individual leaders accountable for achieving the objectives.
Data management implementation roadmap	Identify specific programs, projects, task assignments, and delivery milestones for data governance and management.
Data quality strategy	Define an integrated, agencywide strategy to achieve and maintain a defined level of data quality required to support the business goals and objectives, including data profiling methodologies and a data cleansing approach.

Source: The Framework Guide, DAMA-DMBOK

The Department initially established a Data Governance Steering Committee (Committee) to provide resources for the Department’s data management program, as recommended by the Framework Guide.

However, the Committee stopped meeting and no longer provided the support for data management functions that was originally intended.

---

## Recommendations

---

To strengthen its data governance and data management program, the Department should:

- Conduct a data maturity assessment of its data governance program at least every other year.
- Document its data classifications in accordance with DIR guidance and Department policy.
- Designate individual employees as data owners and data stewards.
- Establish agencywide data governance processes and fundamental documents, to include:
  - Data governance and management policies, standards, or procedures.
  - Business glossary.
  - Data management scope statement.
  - Data management implementation roadmap.
  - Data quality strategy
- Reestablish the Data Governance Steering Committee so that it can provide resources for the Department’s data management functions.

---

## Management’s Response

---

The Department agrees with the recommendations and is committed to strengthening its data governance and data management program through its RTS Modernization initiative. This effort will enable implementation of the recommendations and reduce overall risk.

The Department’s Data Management Officer (DMO) will conduct a maturity assessment of the data governance program at least biennially

going forward. The initial Data Management and Analytics Maturity Assessment (DMAMA) was submitted to DIR on August 23, 2025. Development of the 2026 DMAMA is currently underway and is scheduled for completion by June 1, 2026.

The Department's Data Classification Policy, dated March 30, 2023, aligns with DIR's Data Classification Policy v1.1 and uses the same classification terminology. The Department currently uses software that applies DIR prescribed classification labels to individual documents. In addition, the Department submits an annual DIR Shared Technology Services (STS) Data Classification Report using DIR provided templates and required standardized headers.

The Department maintains a partial list of designated data owners and data stewards. This list will be updated by December 2026 and incorporated into the annual DIR STS Data Classification review process to ensure ongoing accuracy. Data Management and Governance documentation is currently under review and will be updated on a rolling basis throughout the year. The Department's goal is to establish and update core governance processes and documentation by the end of 2026.

The Department has recently implemented a data catalog tool to support development of its business glossary and has configured the tool to operate within the Department's legacy system environment. Over the next year, the DMO will collaborate with business stakeholders to expand and refine both the business glossary and data catalog. As part of the RTS Modernization initiative, the DMO will also implement data quality workflows within the data catalog to strengthen data quality across the Department. Supporting data quality strategy documentation is targeted for completion by the end of 2026.

Efforts are currently underway to reestablish and reschedule Data Governance Steering Committee meetings by no later than August 2026.

Responsible Parties: Chief Information Officer and Data Management Officer

**NOT RATED**

## Chapter 3

# Prior Recommendation Follow-up

*An Audit Report on Motor Vehicle Crime Prevention at the Department of Motor Vehicles (State Auditor's Office Report No. 23-020) was released March 2023 and contained a recommendation related to appropriately limiting system access to the Department's webDEALER system.*

---

### The Department did not implement the prior recommendation.

---

The Department did not implement the recommendation to comply with its policies and procedures to limit user access to its systems to current employees and to grant users only the access privileges required for their job responsibilities.

Specifically, 34 (6 percent) of 548 webDEALER users tested did not require access, including 17 users identified in the prior SAO report as having inappropriate access to the system.

---

### Management's Response

---

The Department acknowledges that the recommendation was not fully implemented. In response to the recommendation, the Department began efforts in 2023 to strengthen user access controls by limiting system access to current employees and ensuring users only have the access required for their job. TxDMV's standard process is for webDEALER access to be removed through the Department's established offboarding process. Manual review of accounts are conducted to identify and remove access on a case-by-case basis; however, additional improvements are warranted. Currently, webDEALER does not provide efficient reporting capability to support comprehensive user access reviews.

To address this, the Department initiated a webDEALER enhancement effort in September 2023 to implement an identity verification and

authentication framework aligned with applicable National Institute of Standards and Technology (NIST) standards. This project will reduce the risk of unneeded access to the system, strengthen protection of sensitive information, and create a more secure environment. The pilot for this project is scheduled to complete in April 2026. These capabilities will be further advanced through the broader Registration and Titling System Modernization effort, which will include enhanced account management, user authentication, and access governance tools to improve policy compliance and reduce operational risk.

Responsible Parties: Chief Information Officer and Vehicle Titles and Registration Division Director



## Appendix 1

# Objectives, Scope, and Methodology

## Objectives

The objectives of this audit were to:

- Determine whether the Department of Motor Vehicles (Department) has implemented data management and data governance programs for managing their data assets.
- As applicable, determine the status of selected prior audit recommendations issued by the State Auditor's Office.

## Scope

The scope of this audit included selected data management and data governance processes and related information security and significant internal controls over the Department's Registration and Title System (RTS) data from September 1, 2023, through October 31, 2025, and the follow-up of selected prior audit recommendations.

The following members of the State Auditor's staff performed the audit:



- Cody Bogan, CISA, CIA, CFE (Project Manager)

- Robby Webb (Assistant Project Manager)
- Nicholas de Sanctis, CFE
- Joe Kozak, CPA, CISA
- Josh Lee
- Theodore Ulmer, CFE
- Dana Musgrave, MBA, CFE (Quality Control Reviewer)
- Anna Howe, CIA, CFE (Audit Manager)

---

## Methodology

---

We conducted this performance audit from August 2025 through April 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. In addition, during the audit, matters not required to be reported in accordance with *Government Auditing Standards* were communicated to Department management for consideration.

### Addressing the Audit Objectives

During the audit, we performed the following:

- Interviewed Department staff to gain an understanding of processes and related controls over data management and data governance.
- Identified the relevant criteria:
  - Texas Government Code, Chapter 2054.
  - Texas Transportation Code, Chapter 730.
  - Texas Administrative Code, Title 1, Chapters 202 and 218.
  - Texas Administrative Code, Title 43, Chapter 217.
  - Department of Information Resources' (DIR) *Security Control Standards Catalog*, Version 2.2.
  - DIR's *Texas Data Management Framework Fast Start Learning Guide*.
  - DIR's *Texas Data Portals Resource Guide*.
  - DIR's *Data Classification Guide*, Version 1.1.
  - DAMA International's *Data Management Body of Knowledge (DAMA-DMBOK)*, 2nd Edition.
  - *COBIT 2019 Framework: Governance and Management Objectives*.
  - Department policies and procedures.

- Reviewed Department policies, procedures, and supporting documentation and observed controls over the Department's significant information technology systems and assets containing RTS data for compliance with statutes and information security and data management standards.
- Reviewed and tested data management and data governance processes to verify whether the Department implemented relevant data processes to comply with applicable requirements and best practices.
- Tested user access to the Department's webDEALER system to determine whether system access permissions for users were appropriate and assessed the implementation status of a prior audit recommendation.
- Tested a risk-based sample of 25 contracts with companies for permitted data disclosure out of a population of 1,778, including 19 of 42 bulk contracts, to determine whether the Department was complying with relevant data privacy requirements. Sample items were selected to ensure review of various factors, such as bulk contracts and certain business types. This risk-based sample is not representative, and it would not be appropriate to project these test results to the population.

### **Data Reliability and Completeness**

Auditors determined that the Department's population of companies with permitted data disclosure contracts was sufficiently reliable for the purposes of the audit. To determine the reliability of the dataset, auditors interviewed Department personnel knowledgeable about the data and analyzed the population for reasonableness and completeness.

### **Report Ratings**

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Auditors also identified and considered other factors when appropriate.



Copies of this report have been distributed to the following:

## **Legislative Audit Committee**

The Honorable Dan Patrick, Lieutenant Governor, Joint Chair

The Honorable Dustin Burrows, Speaker of the House, Joint Chair

The Honorable Joan Huffman, Senate Finance Committee

The Honorable Robert Nichols, Member, Texas Senate

The Honorable Greg Bonnen, House Appropriations Committee

The Honorable Morgan Meyer, House Ways and Means Committee

## **Office of the Governor**

The Honorable Greg Abbott, Governor

## **Department of Motor Vehicles**

Members of the Texas Department of Motor Vehicles Board

Mr. Daniel Avitia, Executive Director

---

This document is not copyrighted. Readers may make additional copies of this report as needed. In addition, most State Auditor's Office reports may be downloaded from our website: <https://sao.texas.gov>.



In compliance with the Americans with Disabilities Act, this document may also be requested in alternative formats. To do so, contact our report request line at (512) 936-9500 (Voice), (512) 936-9400 (FAX), or 1-800-RELAY-TX (TDD); or visit the Robert E. Johnson Building, 1501 North Congress Avenue, Suite 4.224, Austin, Texas 78701.

The State Auditor's Office is an equal opportunity employer and does not discriminate on the basis of race, color, religion, sex, national origin, age, or disability in employment or in the provision of services, programs, or activities.

To report waste, fraud, or abuse in state government, visit <https://sao.fraud.texas.gov>.