Guide for State Department of Transportation Safety Data Business Planning

FHWA Safety Program

FHWA-SA-17-047
July 2017

U.S. Department of Transportation
Federal Highway Administration

Safe Roads for a Safer Future
Investment in roadway safety saves lives

http://safety.fhwa.dot.gov

Sources for cover images photos clockwise left to right: Getty Images, Cambridge Systematics, Inc., and Getty Images.

FOREWORD

The Federal Highway Administration (FHWA) has developed a Guide for State DOT Safety Data Business Planning. The Guide provides practical instructions for State DOTs to follow in developing and implementing a Safety Data Business Plan. The Guide focuses on safety data systems, which include crash, roadway, traffic, and railway-highway grade crossing data. A Safety Data Business Plan provides a roadmap for States to improve their safety data management and governance practices. These improvements provide better quality safety data to support safety decision-making and improved outcomes.

NOTICE

QUALITY ASSURANCE STATEMENT

The Federal Highway Administration (FHWA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

TECHNICAL DOCUMENTATION PAGE

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-SA-17-047	No.	

4. Title and Subtitle	5. Report Date
Guide for State Department of Transportation Safety Data Business Planning	July 2017
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Vandervalk, A., D. Snyder, J.K. Hajek	

9. Performing Organization Name And Address	10. Work Unit No. (TRAIS)
Cambridge Systematics, Inc. 4800 Hampden Ln #800 Bethesda, MD 20814	11. Contract or Grant No. DTFH61-10-D-00020

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Federal Highway Administration, Office of Safety 1200 New Jersey Avenue, SE Washington, DC 20590	Guide September 2014 – September 2017
	14. Sponsoring Agency Code FHWA

15. Supplementary Notes

The contract manager for this report was Stuart Thompson

16. Abstract

This Guide provides practical instructions for State DOTs to follow in developing, implementing, and maintaining a Safety Data Business Plan (DBP). A Safety DBP describes a State's data management challenges, vision and mission for safety data, framework for data governance, and actions for improving its State Safety Data System.

Data business planning is a relevant topic as State DOTs work to advance their capabilities for safety data collection, integration, and analysis to support program planning and performance management. Effective data management practices are necessary to integrate safety related data and make it readily available to support safety data analysis. However, State DOTs must coordinate with a variety of internal and external partners who manage safety data contributing programs. Data business planning provides a framework to enhance this coordination and to identify action items for improving safety data management processes.

The Guide describes steps, supporting actions, and key outcomes associated with each step in developing a Safety DBP. The steps in the Guide are flexible in implementation. States are encouraged to conduct the steps most relevant to their needs as they develop and implement their own Safety DBPs. States do not have to conduct all the supporting actions described in the Guide to achieve their goals.

17. Key Words	18. Distribution Statement
Safety data, roadway inventory data, traffic data, crash data, data management, data governance, data business plan	No restrictions

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	174	

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

Acronym	Term
DBP	Data Business Plan
DOT	Department of Transportation
EMS	Emergency Medical Services
ETL	Extract, Transform, and Load
FAST	Fixing America's Surface Transportation Act
FDE	Fundamental Data Element
FHWA	Federal Highway Administration
GIS	Geographic Information System
HSIP	Highway Safety Improvement Program
IT	Information Technology
LiDAR	Light Detection and Ranging
LRS	Linear Referencing System
MAP-21	Moving Ahead for Progress in the 21st Century Act
MIRE	Model Inventory of Roadway Elements
MMUCC	Model Minimum Uniform Crash Criteria Guideline
MPO	Metropolitan Planning Organization
NHTSA	National Highway Traffic Safety Administration
SSDS	State Safety Data System
TRCC	Traffic Records Coordinating Committee

INTRODUCTION

State Departments of Transportation (DOT), Metropolitan Planning Organizations (MPO), State Highway Safety Offices, and other transportation agencies are responsible for planning, designing, operating, and maintaining safe transportation facilities. High quality data used to document crash activity, roadway elements, and traffic volumes are essential to ensure a safe transportation system.

The Moving Ahead for Progress in the 21st Century Act (MAP-21) called for advancing the capabilities of States for safety data collection, integration, and analysis to support program planning and performance management and continued to allow data improvement activities as an eligible Highway Safety Improvement Program (HSIP) expense [23 U.S.C. 148 (a)(4)(B)(xiv)]. MAP-21 acknowledged the importance of using multiple data sources to understand highway safety problems and to make effective decisions regarding resource allocation for highway safety [23 U.S.C. 148 (c)(2)(A)]. To do this, State safety data systems should be sufficient to guide the HSIP and Strategic Highway Safety Plan (SHSP) processes, including analyses and evaluations identified in 23 U.S.C. 148 and 23 CFR Part 924. The Fixing America's Surface Transportation (FAST) Act continued the provisions of MAP-21 and added a provision related to data collection on unpaved roads. [23 U.S.C. 148(k)]

There are significant challenges when collecting, integrating, and analyzing data to support safety programming and performance management. Safety data management poses unique challenges within State DOTs because extensive coordination with external stakeholders is required. Stakeholders include law enforcement, departments of highway safety and motor vehicles, the State court system, departments of health, local agencies, MPOs, and a State's traffic records coordinating committee (TRCC).

Another challenge that affects a DOT's safety program is they are not the stewards of all the data required for their programs. Data for safety analysis are collected by many different entities, some internal and some external. For example, crash data are largely collected by law enforcement and then collated by another entity, typically other State offices, academia, contractors, or others. After a quality control check, the data may reside on a DOT system or "in the cloud" where the DOT has access to it. Roadway inventory data are typically collected by a non-safety business unit for State maintained roads. For local roads, the DOT may need to coordinate with local government agencies and MPOs to collect data needed to meet the all public roads requirement of the HSIP Final Rule shown in the Guidance on State Safety Data Systems (SSDS). FHWA Guidance on State Safety Data Systems, March 15, 2016. Available at:

(https://safety.fhwa.dot.gov/legislationandpolicy/fast/docs/ssds_guidance.pdf.) Traffic data are also collected and maintained in one or more non-safety business units. Finally, the common highway basemap component required to link safety data sources is rarely under the control or influence of the DOT Safety Program.

In a recent peer exchange, State DOT representatives identified data management as a challenge where the Federal Highway Administration (FHWA) could lend assistance. (Transportation Research Circular E-C196, Improving Safety Programs Through Data Governance and Data Business Planning, A Peer Exchange, March 3-4, 2015, Washington D.C. Available at: http://onlinepubs.trb.org/onlinepubs/circulars/ec196.pdf) FHWA has initiated a project on data business planning, which has proven effective in other industries and sectors of transportation in improving data access, quality, and management.

This Guide provides practical instructions for State DOTs to follow in developing, implementing, and maintaining a Safety Data Business Plan (DBP). A Safety DBP describes a State's management challenges, vision and mission for safety data, framework for data governance, and actions for improving their SSDS. Developing a DBP at a State level will lead to improved management and governance of safety data to support enhanced decision-making. Users may apply this Guide to develop a Safety DBP consistent with other enterprise (i.e., agency-wide) data management efforts.

A Data Business Plan:

- *Guides data management practices*
- *Contains vision, goals, objectives, and actions*
- *Focuses on data systems and business processes*
- *Improves business operations efficiencies*

This introduction documents the need for data business planning in the safety community, describes common terms, and includes a high-level description of the Guide.

SAFETY DATA BUSINESS PLANNING – WHY IS IT IMPORTANT?

Data or information business planning is a relevant topic within State DOTs as they work to advance their capabilities for safety data management, performance management, and asset management systems. Technology for managing data is constantly improving, offering greater chances for more informed decision-making and better targeted investments. Despite these opportunities, States continue to face legacy, 'silo' data systems, which results in technological and institutional challenges related to safety data system management.

Effective data management practices are necessary to integrate crash data with roadway and traffic volume data to investigate systemwide and site-specific conditions. State DOTs must coordinate with a variety of internal and external partners that manage data systems that support safety data analytics. Because data are collected by so many different programs, using different standards, and for different purposes, it is critical that data business planning spans the gaps between multiple data systems. Safety DBP efforts provide a framework to enhance this coordination.

Specific data challenges fall within three categories: **system** (for example, data collection, access, interoperability, quality of data, storage, and documentation); **technology** (for example, data tools, database design, system improvements, and system interfaces); and **institutional** (for example, data management and governance, ownership, coordination, knowledge management, training, and resource availability). State DOTs experience challenges within these categories:

System Challenges

- **Data Collection –** Budget restrictions may limit agencies' ability to collect data elements required for safety analysis on all public roads. Nationally accepted data guidelines such as Model Inventory of Roadway Elements (MIRE) – Fundamental Data Elements (FDEs) and Model Minimum Uniform Crash Criteria (MMUCC) provide criteria for a minimum set of roadway and crash data, respectively. The proposed tools and types of analysis will also dictate the required set of data.

- **Data Access –** Often, data is stored in unrelated systems and databases, or in legacy database systems. Due to current data storage methods, MPOs, local agencies, and other stakeholders may not have access to data or lack technical skills to use it in the native format. Organizations may lack staff with the skills to use existing data sources and data analytics tools. Another challenge relates to deciding which (possibly sensitive) data should be accessible by the public.

- **Data Interoperability –** Agencies may find it challenging to link its safety data systems due to differing database constructs. As noted in FHWA's Data Integration Primer, legacy systems may utilize flat file, network, or hierarchical database structures and contain data in many different formats. This creates challenges in performing the Extract, Transform, and Load (ETL) process to move data from their native systems into a common framework to support safety data analytics. It also reduces access to data across systems. Comprehensive,

enterprise-wide data collection and data quality standards are necessary to ensure data interoperability across disparate data systems.

- **Data Quality and Validation –** Inconsistent or undocumented data collection, varying location accuracy standards, reporting, and quality assurance techniques often compromise data quality. A crash record may also contain conflicting information (for example, number of non-motorists is none, while the contributing factor is a non-motorist action such as a jaywalking pedestrian). Regular verification of data quality, including temporal and spatial resolution, is essential to establish the integrity of input data and the subsequent analyses. Because safety data originate from disparate sources and are generated by distinctly different data collection programs, the originating program needs to assess and enforce data quality needs. However, the standards must be developed across all data collection programs. For example, if spatial and temporal resolution and accuracy do not match across all data sources, analytical results cannot be trusted. Developing data resolution and accuracy standards across all data sources and enforcing them in their native datasets is the only way to ensure data interoperability and integrity.

- **Data Storage and Delivery –** Comprehensive data collection methods require more storage for data; one example is the use of remote sensing technology. As more agencies move to the cloud to accommodate ever-increasing data, new challenges occur with storage, processing, security, and data sharing.

- **Documentation and Metadata** – Agencies may have poor or missing documentation for its safety data systems. This makes it difficult for users to interpret data correctly. Lack of system documentation could also result in a loss of knowledge as the workforce turns over. Time is a critical factor and is often overlooked. The disparate data systems that contribute to safety data analysis are often out of sync. For example, as roads are built and realigned, pavement, crash, and other data must reflect those changes. This can only be done if all the databases are tracking and documenting time.

Technology Challenges

- **Data Tools** – States may lack statewide data tools that allows users to access and analyze safety data on all public roads. Safety data analysis tools may be limited to state routes and only certain roadway elements. Data tools should be comprehensive in scope and provide: 1) data discovery, which allows users to access, prepare, and integrate safety data; 2) an ETL

process, which transforms data into the proper format for safety analysis; and 3) analytical tools to conduct safety data analysis on all public roads.

- **Data Reports –** All users need the ability to access, search, query, analyze, visualize, and generate reports from safety data. The ability to generate *ad hoc* customized queries and reports, as well as standard "canned" reports is important for all users. Many DOT and local agency users lack the technical training, resources, or time to manipulate data. Reports help standardize comparisons by ensuring use of consistent data definitions.

- **Database Design** – Database design is typically dictated by product vendors and consultants. With statewide Information Technology (IT) consolidation, database management is often controlled outside of the DOT. A service oriented architecture is the technical solution for accessing multiple data systems with different database designs. Using service oriented architecture; data systems can remain intact and just provide a web access point. This avoids costly DOT-specific vendor customization, data duplication, and other data management issues.

- **System Improvements** – Data systems may need improved functionality to support advanced analysis methods and to enable data sharing and reporting. Agencies must evaluate current systems and data structures to determine the investment needed to meet these requirements. Because existing data systems often adequately serve their business owners, there may be resistance by the business owners (whose programs fund these systems) to "improvements" to "their" systems, for someone else's use. A department-level DBP, employing service oriented architecture, and a strong DOT-level governance program can overcome this.

- **System Interfaces** – Many organizations are developing solutions to automate data discovery and ETL between data systems. This may require investment in new software and hardware. It will likely require updating business processes, and therefore, training and support services. Employing service oriented architecture allows States to avoid the cost of modifying and maintaining customized versions of existing systems. The interface can be designed to find and access existing data and move it into a form that new or existing analytical resources can consume. In States with statewide IT consolidation, system improvements are subject to standards and review by entities outside of the DOT. DOTs may be challenged to communicate their data needs to ITs for development and implementation.

- **Knowledge Management System** – Agencies may have poor or missing documentation for its data systems, they may not have it centralized in one place, or it may be "in the cloud." This makes it difficult for users to interpret data correctly. Lack of system documentation could also result in a loss of knowledge as the workforce turns over. In States with IT consolidation, system documentation may be controlled and maintained by personnel outside of the DOT. In these cases, DOTs may have little or no access to system documentation.

- **Statewide IT Consolidation** – Some States are consolidating IT resources at a statewide level rather than having individual IT offices within each Department. Statewide IT consolidation may take different forms in different States. Some DOTs have retained much of their pre-consolidation IT capabilities, and some have not. DOTs may not have control over the technology used to solve their information challenges.

Institutional Challenges

- **Data Management and Governance** – Roles and responsibilities for quality, access, and distribution of data are not always clear. Common concerns include firewalls, data silos, and trust issues between data owners and IT representatives.

- **Data Ownership** – Data "ownership" once processed or shared is often unclear. For example, in many States, the State Highway Patrol owns the official crash record for legal purposes, but DOTs process this data to improve its usefulness for engineering purposes.

- **Transmission, Sharing, and Exchange of Safety Data –** Formal data sharing agreements can facilitate sharing of safety data between offices within a DOT as well as with external stakeholders. Data standards, metadata, and data dictionaries are key to achieving consistency and facilitating integration of data from multiple data sources. Once these are implemented through a DBP, transmission, sharing, and exchange are solvable technical issues.

- **Training** – Training is essential to improve staff knowledge on data policies, procedures, processes, and tools for safety analysis and reporting. States should also train external safety stakeholders such as MPOs and local agencies as appropriate. Users of existing legacy systems may already have training on the use of those systems. Because safety data analytics require data from multiple sources, efforts should be made to utilize and build on existing training programs.

- **Funding** –Dedicated staff time is required to integrate safety data from multiple agencies. However, the benefit and cost of doing so is not always easy to determine. One pilot site noted that high level experts familiar with data integration needs and benefits find it difficult to clearly articulate to executives the scope of data issues or how safety data impact the enterprise. This makes it challenging to obtain ongoing commitment for safety data improvements, particularly when staff reductions and cuts in resources occur.

- **Resources –** The FHWA Office of Safety offers support to States to improve their capabilities in collecting, integrating, and analyzing data. Resources available to States include the Roadway Safety Data Program Toolbox, the MIRE, Highway Safety Information System, Crash Data Improvement Program, the United States Roadway Safety Data Capabilities Assessment, and the Roadway Data Improvement Program. (FHWA Office of Safety, Roadway Safety Data Program website, http://safety.fhwa.dot.gov/rsdp/.); (https://safety.fhwa.dot.gov/rsdp/mire.aspx.); (https://safety.fhwa.dot.gov/rsdp/rdip.aspx.) The Office of Safety is developing data management guides in these areas: State and local data integration, Safety Data Business Planning for Data Management, and State Traffic Records Coordinating Committee Noteworthy Practices. (https://safety.fhwa.dot.gov/rsdp/data_activities_state.aspx.); (https://safety.fhwa.dot.gov/rsdp/manage.aspx.); (https://safety.fhwa.dot.gov/rsdp/downloads/trcc_noteworthy.pdf.) These projects may include accompanying technical assistance.

State DOTs can apply data business planning to address data management and data governance challenges related to operations, asset management, and transportation planning. Several resources, including NCHRP 666, document this approach. This Guide adapts and customizes these proven approaches for safety data business planning. (NCHRP 666: Target-Setting Methods and Data Management to Support Performance-Based Resource Allocation by Transportation Agencies, Volume II: Guide for Target-Setting and Data Management, 2010.)

DATA BUSINESS PLANNING TERMS

NCHRP 666 defines data management and data governance as follows: (NCHRP 666: Target-Setting Methods and Data Management to Support Performance-Based Resource Allocation by Transportation Agencies, Volume II: Guide for Target-Setting and Data Management, 2010.)

> ***Data management*** *is the development, execution, and oversight of architectures, policies, practices, and procedures to manage the information lifecycle needs of an enterprise in an effective manner as it pertains to data collection, storage, security, data inventory, analysis, quality control, reporting, and visualization.*
>
> ***Data governance*** *is defined as the execution and enforcement of authority over the management of data assets and the performance of data functions. The management of data assets for an organization or state DOT is usually accomplished through a data governance board or council. This role is critical in successfully managing data programs that meet business needs and in supporting a comprehensive data business plan for the organization.*

Data governance is a critical element of data management and data business planning. It provides:

- A central focus to identify and control the collection, storage and sharing of data;
- Identification of stakeholder roles and responsibilities;
- Enterprise data standards, data dictionaries, and metadata;
- Standard data quality assurance processes;
- Knowledge management processes for sharing and retaining critical organizational knowledge related to data and information; and
- Alignment of data program investments with agency needs.

NCHRP 754 defines data, information, and knowledge as follows: (Cambridge Systematics, Inc. NCHRP Report 754: Improving Management of Transportation Information, Transportation Research Board, 2013. Available at http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_754.pdf.)

> ***Data*** *is a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or computers.*

Information *is data and documents given value through analysis, interpretation, or compilation in a meaningful form.*

Knowledge *is information combined with experience, context, and interpretation that make it possible to understand and draw implications from both data and information. Knowledge consists of data and information organized and processed to convey understanding, experience, accumulated learning, and expertise as they apply to a current problem or activity.*

Figure 1 shows the relationship between data, information, and knowledge.

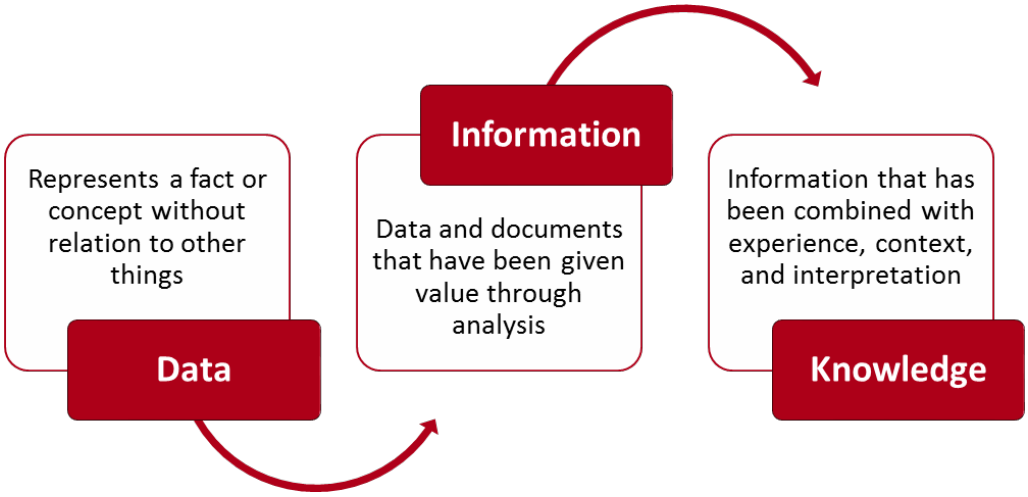


Figure 1. Flow chart. Data, information, and knowledge hierarchy.

Source: Adapted from Minnesota DOT Data Business Plan, 2008. Available at https://www.dot.state.mn.us/tda/databusinessplan.docx.

FHWA's Guidance on SSDSs defines a SSDS and safety data as follows:

As part of its State highway safety improvement program, a State shall have in place a ***safety data system*** *that can be used to perform analyses supporting the strategic and performance-based goals in the SHSP and HSIP. [23 U.S.C. 148 (c)(2)]. This section provides guidance on the capabilities a State's safety data system should have in order to support analyses and evaluations in 23 U.S.C. 148, including: 1) types of roadways, 2) types of data, 3) geolocation of safety data to a common highway basemap, 4) analysis and evaluation capabilities, and 5) the subset of Model Inventory of Roadway Elements (MIRE) to be collected.*

Types of Roadways: Consistent with the purpose and scope of the HSIP, a State shall have in place a safety data system to perform safety problem identification and countermeasure analysis. [23 U.S.C. 148 (c)(2)(A)]. The statute also specifies that a State shall advance the capabilities of the State for data collection, analysis, and integration in a manner that includes

all public roads, including non-State-owned public roads and roads on tribal land in the State. [23 U.S.C. 148 (c)(2)(D) and (D)(ii)]. Public road means "any road under the jurisdiction of and maintained by a public authority and open to public travel." [23 CFR 460.2(a)].

***Safety data** means crash, roadway, and traffic data on a public road, and, includes, in the case of a railway-highway grade crossing, the characteristics of highway and train traffic, licensing, and vehicle data. [23 U.S.C. 148 (a)(9)]. Data on rail-highway grade crossing train traffic are available through the Federal Railroad Administration crossing inventory. (http://safetydata.fra.dot.gov/OfficeofSafety/PublicSite/Crossing/Crossing.aspx.)*

Crash, roadway, and traffic data should be linkable by geolocation, i.e., a unique location identifier, on a highway basemap, which is defined as "a representation of all public roads that can be used to geolocate attribute data on a roadway." [23 U.S.C. 148 (a)(2)]. States should put in place methodologies to assure that the location of crashes, roadway elements, and traffic data are consistent with the most current basemap.

The FHWA Office of Highway Policy Information and Office of Planning, Environment, and Realty issued the Memorandum, Geospatial Network for All Public Roads on August 7, 2012. This Memorandum identified a Highway Performance Monitoring System (HPMS) requirement for States to update their Linear Referencing System to include all public roadways within the State by June 15, 2014, in accordance with the HPMS information collection approval from the Office of Management and Budget (2125-0028). To date, the majority of States have complied with this requirement. This Linear Referencing System is a means to geolocate all safety data on a common highway basemap that includes all public roads.

The FHWA developed the MIRE, a recommended listing of roadway and traffic elements critical to safety management, as a guide to help transportation agencies improve their roadway and traffic data inventories. MIRE was developed to enhance a State's ability to use advanced safety analyses such as presented in the Highway Safety Manual.

MAP-21 required the Secretary to establish a subset of the MIRE that are useful for the inventory of roadway safety and ensure that States adopt and use the subset to improve data collection. [23 U.S.C. 148(f)(2)]. The FHWA established a subset of the MIRE as part of the HSIP Final Rule changes to 23 CFR Part 924, effective April 14, 2016. This subset is referred to as the fundamental data elements (FDEs). The FDEs are categorized by roadway functional classification and surface type and include three tables, one each for non-local paved roads, local paved roads, and unpaved roads. They are further refined into subcategories of data elements for road segments, intersections and interchanges for non-local paved roads.

Figure 2 depicts how the required capabilities for a SSDS support analysis and evaluations for the SHSP and HSIP. Figure 3 illustrates how a State's crash, roadway, and traffic data are linkable through geolocation on a common highway basemap. Appendix A summarizes the MIRE FDE requirements for non-local paved roads, local paved roads, and unpaved roads.

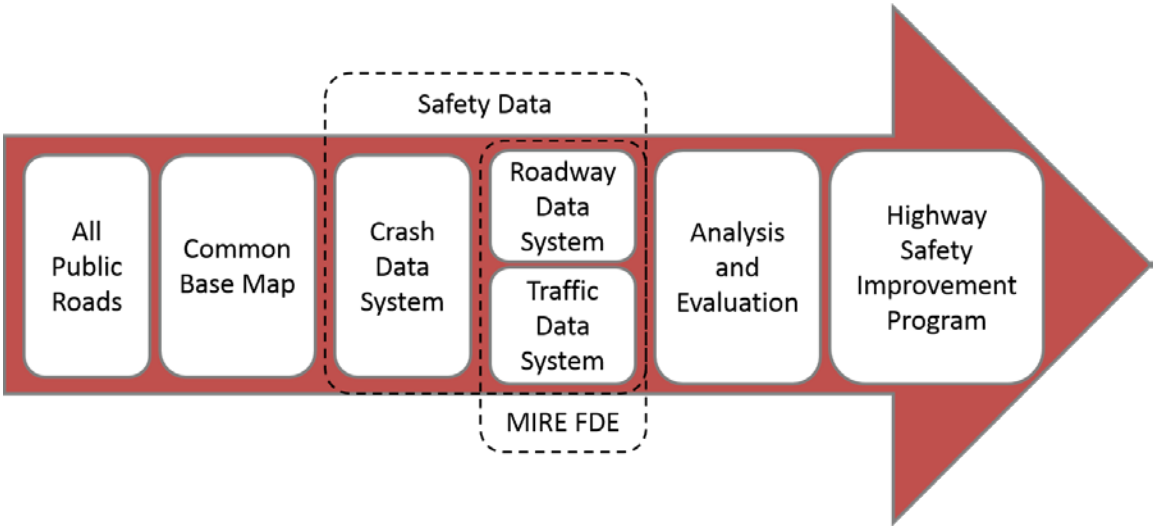


Figure 2. Flow chart. State safety data system capabilities.

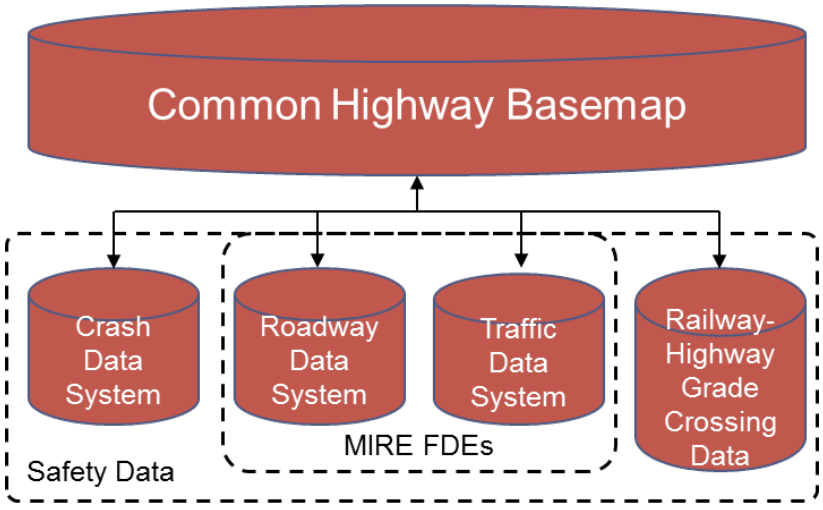


Figure 3. Flow chart. Linking of safety data.

AUDIENCE FOR THE GUIDE

This Guide assists States to develop a Safety DBP. The primary audience is the people leading safety data business planning efforts at State DOTs. This includes State safety engineers, safety program managers, IT professionals, planners, and data managers that use, collect, or manage

the various sources of data that contribute to safety data analysis and decision-making. Members of State TRCCs, local agencies, and MPOs will find its content useful to define data quality criteria and integration standards for traffic records data. This Guide targets State DOTs and uses the terms "State" and "State DOT" interchangeably.

A State may develop its Safety DBP in coordination with its TRCC. The TRCC has these responsibilities:

> *TRCC have specific review and approval authority with respect to State highway safety data and traffic records systems, technologies used to keep such systems current, TRCC membership, the TRCC coordinator, changes to the State's multi-year Strategic Plan, and performance measures used to demonstrate quantitative progress. It also charges a TRCC with considering; coordinating and representing to outside organizations the views of the State organizations involved in the administration, collection, and use of highway safety data and traffic records. (23 CFR 1200.22(b)(2))*

The Safety DBP does not supplant the requirement for a State traffic records strategic plan. The State should use its State traffic records strategic plan as a resource to develop the Safety DBP, and similarly, the State could identify potential traffic records improvement projects from the DBP recommendations.

Stakeholder involvement is critical throughout each step. The DBP development process is as important as the outcome itself. Developing a Safety DBP accomplishes the following:

- Helps everyone in the life-cycle of safety data, from data collection to data distribution, and decision-makers understand data management and governance processes. This includes roles and responsibilities at all levels, including analysts, managers, and technical staff;
- Helps business areas understand how they can leverage data across the enterprise to deliver their programs supporting the overall needs of the agency;
- Promotes collaboration with IT staff, leading to improvements in software and hardware capabilities that support crucial program areas;
- Identifies how each employee's responsibilities link to the agency's mission and goals, which helps them understand their role in the overall success of their program area and the DOT;

- Helps an agency identify risks associated with not having quality, timely data that they can use to demonstrate and justify the benefits of expending resources on its SSDS in the future; and

- Raises the perception that data is reliable and sufficient to support decision-makers and the agency's mission.

OVERVIEW OF THE GUIDE

This Guide documents each of the seven steps for developing and implementing a Safety DBP. The steps and their purposes are shown in Figure 4.

Table 1 summarizes supporting actions and key outcomes associated with each step in developing a Safety DBP. The work products of steps 1 through 5 culminate in the development of a Safety DBP in Step 6. A State implements the Safety DBP in Step 7.

The steps in the Guide are flexible in implementation. States are encouraged to conduct the steps most relevant to their particular needs as they develop and implement their own Safety DBPs. States do not have to conduct all the supporting actions described in the Guide to achieve their goals.

The Guide also documents the results of case studies and pilot projects conducted as part of the project:

- **Case Studies.** In the first phase of the project, the team researched State noteworthy practices in safety data management and governance. Four States – Alaska, Michigan, New Hampshire, and Utah – participated in detailed case studies documenting how their data management and IT practices have improved safety data systems and processes. Appendix B provides a summary of published case study results. The detailed case studies are available on the FHWA Roadway Safety Data Program web page at https://safety.fhwa.dot.gov/rsdp/safety_casestudies.aspx.
- **Pilot Studies.** FHWA selected two agencies – Kansas DOT and Washington State DOT – to participate in pilot studies to test the Guide concepts through the development of State Safety DBPs. Appendix C provides a summary of pilot study results.

Figure 4. Diagram. Process for developing and implementing a safety Data Business Plan.

Table 1. Process for developing a safety Data Business Plan.

Steps	Supporting Actions	Key Outputs / Work Products
 **Step 1 –** Plan for Safety Data Management and Governance	• Identify stakeholders for safety data systems • Engage stakeholders • Define safety data management challenges • Research State efforts in data management and governance • Establish vision and mission for safety data management • Develop outcome statement	• Stakeholder registry • Community of interest diagram • Stakeholder engagement plan • Survey instrument on safety data management challenges • Problem statement • Survey instrument on data governance initiatives • Vision and mission for safety data governance • Outcome statement for the Safety DBP
 **Step 2 –** Assess Current SSDS	• Identify data systems to include in the assessment • Document current business processes • Document spatial, temporal, and data resolution and accuracy standards in each data source • Research and summarize current and past assessment efforts • Update past assessments • Conduct capability maturity assessment	• Identification of data systems for the assessment • Use case diagrams and accompanying narratives on business processes and workflows for safety data systems • Summary of similarities and differences in data resolution and accuracy standards across all data • Summary of past assessment recommendations in matrix form • Update on State progress in implementing past assessment recommendations • Assessment tools • Assessment of current and desired levels of maturity for each dimension of the capability maturity model • Identification of actions needed to advance from current to desired capability

Table 1. Process for Developing a Safety Data Business Plan. (continuation).

Steps	Supporting Actions	Key Outputs / Work Products
 **Step 3 –** Establish a Governance Program	• Develop data principles • Develop a governance model • Establish roles and responsibilities for governance • Develop IT project governance • Develop governance documentation	• Core data principles • Governance model • Roles and responsibilities • IT project selection process • Data governance charter • Data governance manual • Data catalog • Business terms glossary • Common resolution and accuracy standards for linking data sources
 **Step 4 –** Identify Needs for Safety Tools and Technology	• Identify needs for improved technology • Develop plan for improved use of tools	• Summary of needs and weaknesses related to safety tools and technology • Plan for enhancing or replacing safety tools and technology • Tool training needs and opportunities defined
 **Step 5 –** Develop Action Plan	• Summarize gaps and improvements • Identify priorities • Develop action plan • Develop roadmap for implementation	• Summary of system, technology, and institutional gaps • Priorities for addressing gaps • Action plan • Roadmap for implementation
 **Step 6 –** Document the Safety DBP	• Document the Safety DBP	• Safety DBP

Table 1. Process for developing a safety Data Business Plan (continuation).

Steps	Supporting Actions	Key Outputs / Work Products
 **Step 7 –** Implement and Sustain the Safety DBP	• Assign roles and responsibility • Establish performance metrics • Implement the Safety DBP • Conduct training • Monitor progress • Communicate changes	• Designation of governance champion or small team to guide implementation • Performance metrics for measuring success • Implementation of the Safety DBP • Training program on data governance • Progress updates

STEP 1. PLAN FOR SAFETY DATA MANAGEMENT AND GOVERNANCE

The first step in safety data business planning is the initial design for data management and governance. This section guides a State to identify the data problems, challenges and issues, symptoms, root causes, and opportunities to improve safety data management. Key actions include identifying and involving stakeholders, defining safety data management challenges, researching other data governance initiatives, and establishing a vision, mission, and goals for data business planning. After completing this step, States will understand their current data management challenges, data governance efforts, and goals for managing and governing data.

IDENTIFY STAKEHOLDERS

Core Stakeholders

Initial planning involves identifying a core team of stakeholders willing to help champion the DBP effort. This team should consist of a small group of data managers or data owners whose daily tasks involve collecting, maintaining, or updating data elements needed for safety analysis. This team will help define challenges associated with managing, governing, and using safety data and complete the steps in this Guide.

Stakeholders for Safety Data

Next, the State should identify and document the stakeholders for safety data. A stakeholder is any internal or external person or organization that collects, owns, maintains, uses, interfaces with, accesses, or benefits from a safety data system. Stakeholders may include any internal or external agency statutorily required to collect, work with, or contribute to a safety data system. These stakeholders, collectively known as the Community of Interest, play a vital role in identifying needs and business uses for safety data from the perspective of their individual offices or agencies (if external to the State DOT). They typically dictate the policies, procedures, and business processes associated with a safety data system.

Internal stakeholders for a safety data system may include traffic safety engineers, safety program managers, asset managers, Highway Performance Monitoring System (HPMS) managers, design engineers, pavement management and bridge management engineers, planners responsible for statewide transportation improvement programs and long-range plans, and data managers from other offices that provide safety-related data. External stakeholders are also common users of safety data. These may include local and State law enforcement agencies,

MPOs, local government agencies (cities/counties), TRCC member agencies, the National Highway Traffic Safety Administration (NHTSA), FHWA, other Federal agencies, insurance companies, and university research entities. The following bullets briefly describe how some of these groups use safety data.

- State and local transportation agencies safety engineers and planners analyze safety data to identify safety problems, recommend appropriate improvements, evaluate the effectiveness of implemented improvements, track mandated performance measures, and conduct strategic planning to support the Strategic Highway Safety Plan and HSIP. Appropriate data management and governance practices are essential for a State to link safety data to a common LRS to support these activities.

- Local and State law enforcement agencies collect crash data and share it with the State DOT and other agencies. Law enforcement agencies may also use the data internally to determine the most effective methods for deploying law enforcement (based on NHTSA's Data Driven Approaches to Crime and Traffic Safety operational model) to improve traffic safety. (https://www.nhtsa.gov/staticfiles/nti/ddacts/811185_DDACTS_OpGuidelines.pdf.)

- Local government agencies may collect and maintain traffic volume, roadway inventory, and LRS data on local roads. They may provide the data to the State to maintain local roadway information in its statewide data system.

- State TRCCs help develop data definitions and data standards for the collection of traffic records data, including the State's crash, vehicle, driver, roadway, citation and adjudication, and injury surveillance data systems. This group does not necessarily use the data, but rather supports the State in improving the timeliness, accuracy, completeness, uniformity, integration, and accessibility of traffic records data to meet the needs of multiple safety program areas. The TRCC also develops a multi-year State Traffic Records Strategic Plan. This plan describes planned improvements for its core safety databases, provides an update on implementing traffic records assessment recommendations, and includes performance measures to demonstrate quantifiable and measurable progress.

Figure 5 illustrates a typical Safety Community of Interest. The shaded oval represents State DOT safety data managers who may serve on the Core Stakeholder Team. In planning for a Safety DBP, the State should develop a similar Community of Interest diagram that includes all stakeholders specific to their agency.

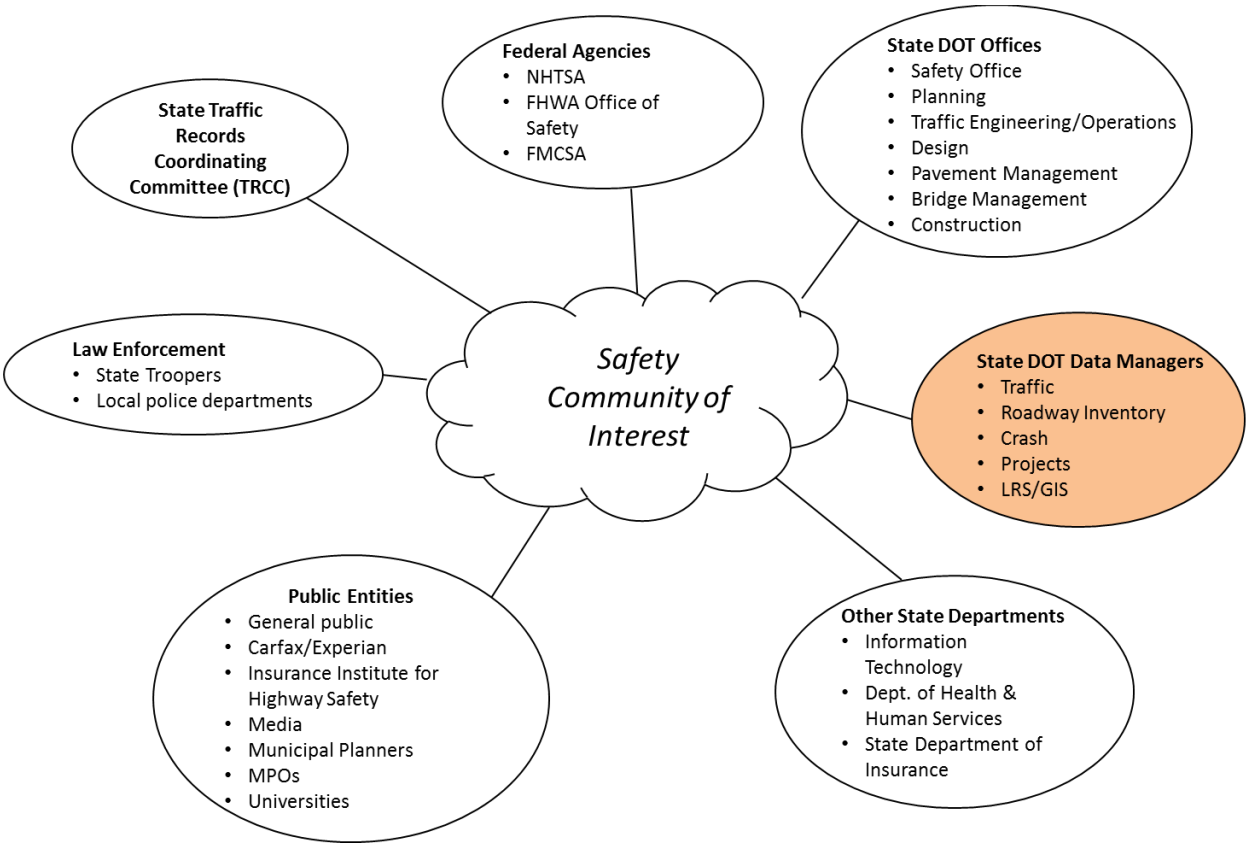


Figure 5.Web chart. Safety community of interest.

The State should develop a stakeholder registry that identifies the individual stakeholders involved in developing the Safety DBP, as shown in Table 2. The registry should document the stakeholder's organization, name, title, and contact information. The registry should also identify the stakeholder's role concerning safety data (for example, whether they are a system owner, data provider, or data user of a specific safety data system).

Table 2. Example stakeholder registry.

Agency	Stake-holder Name	Office	Title	Safety Data System	Role	Email	Phone
State DOT	Stakeholder 1	Office 1	Title 1	Data System 1	System Owner	Email 1	Phone 1
State DOT	Stakeholder 2	Office 1	Title 2	Data System 2	Data User	Email 2	Phone 2
…	…	…	…	…	…	…	…

Governance Stakeholders

Finally, the State should assemble a list of managers of other DOT business offices or divisions that may have data business planning or governance initiatives in place. This may include State DOT offices such as the safety office, planning, traffic engineering and operations, design, asset management, HPMS managers, pavement management, bridge management, maintenance, or construction. It may also include administrative and IT offices. These stakeholders will be critical in gathering information on governance initiatives underway in other business areas within the DOT.

ENGAGE STAKEHOLDERS

The State should involve stakeholders throughout all steps of developing the Safety DBP. The degree of stakeholder involvement will vary for each step of the Safety DBP development process. For example, during initial planning (Step 1), a State may engage a small group of stakeholders to identify data challenges and needs for safety data governance, making sure the group includes representatives from all safety data business areas. When the State is ready to move forward with other steps, the State should involve other internal and external stakeholders as needed.

The State should develop a stakeholder engagement plan that identifies the stakeholders involved in each step of the development process, the purpose of engaging stakeholders, and potential engagement mechanisms. Table 3 provides an example stakeholder engagement plan. The plan could also include details such as meeting dates, associated meeting materials, and how and when to distribute materials to stakeholders.

The plan should be tailored based on agency size and the resources and funding available for gathering feedback. Potential outreach mechanisms include the following:

- **Surveys:** Surveys are used to obtain feedback on how well individual data systems meet safety business needs, identify gaps in data systems or needs, and identify potential solutions to address gaps. Surveys provide an opportunity to assess data systems (agency wide or specific to the safety program area, depending on the scope of the DBP).

- **Focus Groups:** Focus groups engage stakeholders at a more detailed level. Focus groups may include data providers and data users of a specific data system. A State can conduct focus groups in person or via online webinar. Focus group topics could include identifying critical data gaps and issues in meeting safety business needs; documenting current business processes for safety analysis; and identifying short- and long-term improvements for the Action Plan. A State should designate a champion to lead the focus group and keep actionable items moving forward.

- **Workshops:** Workshops engage internal stakeholders such as IT staff, data program managers, and other agency staff who represent data providers and users. Workshops may capture needs for a group of data systems or a single data system. Potential topics include discussing specific data improvement strategies; identifying technology improvements; and collaborating on new data applications to integrate existing data into an enterprise model.

- **Research Studies:** Independent research studies help assess data system performance or identify the requirements for implementing specific analysis tools. Research studies offer an unbiased assessment of data systems and can identify best practices across both the public and private sectors.

- **Briefings:** Briefings engage larger stakeholder groups within the Community of Interest or senior management at a high level. The purpose of a briefing is to convey information, reach consensus and buy-in, or obtain dedicated resources (such as funding, personnel, and training) for safety data business planning efforts.

Table 3. Example stakeholder engagement plan.

Process Decisions	Supporting Actions	Relevant Stakeholders	Purpose of Stakeholder Engagement	Potential Stakeholder Engagement Mechanisms
Step 1 Plan for Safety Data Management and Governance	• Identify Stakeholders for Safety Data Systems • Engage Stakeholders • Define Safety Data Management Challenges • Research State Efforts in Data Management and Governance • Establish Vision and Mission for safety data management • Develop Outcome Statement	• State DOT Data Managers • State DOT Offices • Other State Departments (if relevant to the scope of the Data Business Plan)	• Obtain critical input on current data management and governance challenges and root causes • Identify needs and business uses for safety data from the perspective of their individual offices or agencies • Obtain information and supporting documentation on other State efforts in data management and governance • Obtain consensus on vision and mission to ensure they are realistic, specific to the agency, achievable over different periods of time, and linked to overall agency vision, mission, and goals • Obtain consensus on the outcome statement for the Safety DBP	• Surveys • Focus groups • Workshops • Research study

Table 3. Example stakeholder engagement plan (continuation).

Process Decisions	Supporting Actions	Relevant Stakeholders	Purpose of Stakeholder Engagement	Potential Stakeholder Engagement Mechanisms
Step 2 Assess Current SSDS	• Identify Data Systems to Include in the Assessment • Document Current Business Processes • Research and Summarize Current and Past Assessment Efforts • Update Past Assessments • Conduct Capability Maturity Assessment	• State DOT Data Managers • State TRCC	• Obtain input on relevant safety data systems to include in the assessment • Obtain input on current business processes and workflows for safety data systems • Obtain an update on progress made in implementing current and past assessments • Achieve consensus on current and desired maturity levels using the capability maturity model	• Focus groups • Workshops • Research study

Table 3. Example stakeholder engagement plan (continuation).

Process Decisions	Supporting Actions	Relevant Stakeholders	Purpose of Stakeholder Engagement	Potential Stakeholder Engagement Mechanisms
Step 3 Establish a Governance Program	• Develop Data Principles • Develop a Governance Model • Establish Roles and Responsibilities for Governance • Develop IT Project Governance • Develop Governance Documentation	• State DOT Offices • State DOT Data Managers • IT Office • Other State Departments (if relevant to the scope of the Data Business Plan)	• Obtain consensus on the data principles, Governance Model, data governance roles and responsibilities, and IT project governance • Obtain input on data governance documentation	• Focus groups • Workshops • Briefings to senior management
Step 4 Identify Needs for Safety Tools and Technology	• Identify Needs for Improved Technology • Develop Plan for Improved Use of Tools	• State DOT Data Managers • State TRCC • IT Office • Other State Departments (if relevant to the scope of the Data Business Plan)	• Obtain input on business needs for improved technology • Obtain technical input on IT requirements for software, hardware, system interfaces, compatibility, IT tools, and network requirements	• Workshops • Research study

Table 3. Example stakeholder engagement plan (continuation).

Process Decisions	Supporting Actions	Relevant Stakeholders	Purpose of Stakeholder Engagement	Potential Stakeholder Engagement Mechanisms
Step 5 Develop Action Plan	• Summarize Gaps and Improvements • Identify Priorities • Develop Action Plan • Develop Roadmap for Implementation	• State DOT Data Managers • IT Office	• Obtain input on action plan steps and priorities • Commit resources and assign responsibilities for plan implementation	• Workshops
Step 6 Document the Safety DBP	• Document the Safety DBP	• State DOT Offices • State DOT Data Managers • Other State Departments (if relevant to the scope of the Data Business Plan)	• Obtain feedback on the Safety DBP	• Briefings
Step 7 Implement and Sustain the Safety DBP	• Assign Responsibility • Establish Performance Metrics • Implement the Safety DBP • Conduct Training • Monitor Progress • Communicate Changes	• All stakeholders in the Community of Interest	• Obtain feedback on proposed revisions of the Safety DBP • Obtain feedback on training needs and plan effectiveness	• Surveys • Focus groups • Briefings

DEFINE SAFETY DATA MANAGEMENT CHALLENGES

In planning for safety data management, the State must document current challenges in managing and governing its safety data systems. The introduction section listed examples of common data challenges categorized by system, technology, and institutional. The State should use the following questions to help identify specific issues, symptoms, and root causes to address in the Safety DBP.

- **System:**
  - Are there gaps in required data elements needed for safety analysis? Are data elements consistent with national guidelines such as MIRE FDEs (summarized in Appendix C)?
  - Do current data collection efforts meet the State's business needs?
  - Are there redundancies in current data collection or data management efforts?
  - Is data easily accessible?
  - Can users find the data they need in the format they need?
  - Are there difficulties integrating safety data within the agency or across multiple agencies?
  - What are the challenges with integrating safety data (such as lack of geographical coordinates, differing segment identification, different data formats, varying temporal resolution)?
  - Are system owners entering data in a timely manner?
  - Is the available history of crashes adequate for safety analysis?
  - Is documentation complete and up-to-date?
- **Technology:**
  - Can users access the tools they need to conduct safety analysis?
  - Can users achieve consistent results when using safety analysis tools?
  - Do users need tools such as dashboards, scorecards, and data visualization to help with reporting, performance tracking, and analysis of safety data?

  - Do users need geospatial location capabilities to facilitate efficient visualization and analysis of data when using safety analysis tools?
  - Do users need additional functionality within applications such as enhanced modeling and reporting capabilities to help identify and prioritize safety improvements?
  - Can users generate customizable reports to support safety analysis?
  - Are safety related data sets stored in older legacy systems that require substantial investment to meet current and future business needs?
  - Do users need more streamlined access to data and information?
  - Are there data "silos," especially for critical data sets needed to support safety programs?
  - Can staff access the latest information about safety systems, data, policies, reports, tools, and training resources through a centralized knowledge management system?

- **Institutional:**
  - Is there a data governance structure for the SSDS?
  - Are roles, responsibilities, and processes for safety data governance formalized and documented?
  - Are formal data sharing agreements in place to facilitate data sharing between internal and external stakeholders?
  - What policies and procedures exist for collecting, maintaining, using, and updating safety data?
  - Do staff need training on safety data policies, procedures, and processes?
  - Do staff know how to use tools for safety analysis and reporting?
  - Are SSDS investments made at the functional (that is, within the safety program) or enterprise level?
  - Are overall agency needs for safety data optimized? How are safety data improvements prioritized with respect to improvements in other program areas?
  - Are safety data system needs coordinated with IT, local agencies, and MPOs?
  - Do data program investments align with business needs for safety data systems?

The State can gather this information through in-person interviews, group meetings, phone calls, emails, or an online survey instrument. The pilot studies used an online survey instrument

to outreach with safety stakeholders and the IT office. Appendix D provides an example online survey instrument used in the pilot studies. The end goal is to develop a statement defining the current situation regarding safety data management and governance.

RESEARCH STATE EFFORTS IN DATA MANAGEMENT AND GOVERNANCE

Next, the State should research other data management and governance efforts underway within the DOT by surveying managers of other business areas of the DOT to gather this information. Some example questions include:

- Does your office own, develop, or maintain any data systems or databases?
- Does your office have a data business plan in place that guides the way you manage or govern data systems or databases?
- Does your office regularly assess its data systems to identify needs for improvement?
- Have you assessed data governance maturity or capability within your business area?
- Does your office have formal policies and procedures in place for managing and governing its data systems or databases?
- Are the workflows and business processes for managing your data systems or databases documented?
- Has your office defined roles and responsibilities for data management and governance?
- Is there a governance board or working groups set up for data management and governance?

The State can gather this information through in-person interviews, group meetings, phone calls, emails, or an online survey instrument. Regardless of the format, it is important to introduce the reason for the questions, define key terms (such as a Data Business Plan), keep questions simple to answer, and make sure the process does not require too much staff time. Appendix E provides an example online survey instrument used in the pilot studies.

The intent of the survey is to determine where the DOT currently stands in its data governance efforts. The survey results could indicate one of the following scenarios:

1. No data management or data governance initiatives;

2. Other offices (non-safety) have embarked on efforts to better manage and govern data; or

3. There are enterprise-level efforts for data management and data governance.

The State must determine whether the Safety DBP is a stand-alone initiative or part of a larger governance program. If efforts have started in other business areas or at the enterprise level, the Safety DBP should complement those efforts and leverage any work already done (such as assessments of data management and governance maturity). If no efforts exist, the Safety DBP could be used as an example for developing an enterprise-wide initiative.

ESTABLISH VISION AND MISSION FOR SAFETY DATA MANAGEMENT

Finally, the State should establish the vision and mission for safety data within the organization. The vision and mission describe high-level opportunities for managing and governing safety data. They articulate the outcome of improved safety data collection, accessibility, security, cost effectiveness, and other data management attributes. The vision and mission support the State's broader safety goals by providing quality data for safety problem identification, countermeasure analysis, and target setting activities.

Vision

A vision statement is aspirational in nature and describes a future condition of a State's safety data system. It establishes the program's identity and guides future activities.

Effective vision statements are concise, yet provide enough content to clarify the preferred outcome. A vision statement for a safety data system could reference concepts such as performance management, data quality, integration of data across agencies, or providing information to the public. Some example vision statements are as follows:

- Quality data adheres to established data quality standards and supports safety decision-making.

- Users have access to quality safety data when, where, and in the form needed.

- **Kansas DOT:** The Kansas DOT and its safety data stakeholders will have a sound, comprehensive, and well-coordinated approach to managing, improving, and applying the State's safety data and analysis resources.

- **Washington State DOT:** WSDOT's business decisions will be supported by reliable, timely, accessible, and complete safety data.

Mission

In contrast to the vision, a mission statement is action-oriented. The mission may reference concepts from the vision statement, but it also emphasizes the role of the safety data system in achieving the vision. It highlights the need for collaboration with internal and external stakeholders. Some example mission statements are as follows:

- Provide reliable, timely, and accurate safety data and information. The information must be accessible, shared for cross-program analysis, and integrated into the agency's safety decision-making process.

- Maximize the efficiency and effectiveness of safety data resources, collection, management, analysis, and reporting.

- **Kansas DOT:** Achieve sound governance of safety data resources, enhance integration of safety data systems, continually improve the quality and usability of data, and promote user friendly and easily accessible data by our safety users and partners for their business analysis.

- **Washington State DOT:** WSDOT will have integrated safety data systems that are user friendly and easily accessible (as appropriate) by our safety users and partners for their business analysis.

DEVELOP OUTCOME STATEMENT

The outcome statement describes the results the Safety DBP will achieve. A Safety DBP has numerous possible objectives, but all States need data systems that support safety problem identification, countermeasure analysis, and target setting at a statewide level. States should relate the outcome statement to specific issues or gaps they want to address. For example, a State may want to improve its safety data systems to meet FAST Act requirements for data collection. A State may also want to implement a data governance program to improve its data management practices.

Some example outcome statements and objectives are as follows:

- **Minnesota DOT:** Provide a platform for stronger data management practices to: 1) increase transparency and accountability; 2) expand the reliability and utility of data to meet business decision-making needs; 3) create efficiencies in accessing, sharing, and using data and information; 4) standardize processes and systems that reduce redundancy and promote consistency of data; and 5) optimize new information management and spatial data tools and methods.

- **Kansas DOT:** The objectives of the Safety DBP are to: 1) develop a governance framework to help better manage safety data resources and assets; 2) develop a roadmap for improving safety data resources; and 3) create a communication and implementation plan.

- **Washington State DOT**: The Department wants to improve its data management and governance practices in order to integrate data and make it available to all State practitioners. The objectives of the Safety DBP are to: 1) demonstrate how safety data impacts the enterprise; 2) develop a roadmap to address safety data linkage, association, and management challenges; 3) establish a strong, sustainable vision for safety data; 4) implement a formal safety data governance process; and 5) ensure a sustainable safety data improvement process.

SUMMARY

Step 1: Plan for Safety Data Management and Governance, guides States in initial planning efforts to help them understand current data management challenges, data governance initiatives, and goals for managing and governing data. The important actions in this step are:

- **Identify stakeholders.** Stakeholders for safety data systems play a key role in identifying needs and business uses for safety data from the perspective of their individual offices or agencies. There are multiple stakeholder groups involved in the Safety DBP. A core team of stakeholders helps champion the Safety DBP effort. This team

KEY OUTPUTS AND WORK PRODUCTS

- ☐ Stakeholder registry
- ☐ Community of interest diagram
- ☐ Stakeholder engagement plan
- ☐ Survey instrument on data management challenges
- ☐ Problem statement
- ☐ Survey instrument on data governance initiatives
- ☐ Vision and mission statements for safety data governance
- ☐ Outcome statement for the Safety DBP

consists of data managers or data owners whose daily tasks involve safety data management. A larger group of stakeholders help define the policies, procedures, and business processes associated with a SSDS. This group includes any internal or external person or organization that collects, owns, maintains, uses, interfaces with, accesses, or benefits from a safety data system. Governance stakeholders include managers of other DOT business offices or divisions that may have data business planning or governance initiatives in place. States should document stakeholder groups in a stakeholder registry and Community of Interest diagram.

- **Engage stakeholders.** Engaging stakeholders throughout each step of the Safety DBP development process is crucial to its success. A stakeholder engagement plan identifies the stakeholder groups involved in each step, the type of feedback desired, and outreach mechanisms for obtaining feedback. Surveys, focus groups, workshops, research studies, and briefings are all potential outreach mechanisms for engaging stakeholders.

- **Define safety data management challenges.** Defining the current situation regarding safety data management and governance helps States identify specific issues to address in its Safety DBP. States can use the exploratory questions related to system, technology, and institutional challenges to understand specific issues, symptoms, and root causes.

- **Research State efforts in data management and governance.** States should survey business area managers to identify other governance initiatives underway at the DOT. This will determine whether the Safety DBP is a stand-alone initiative or part of a larger governance program. The State can also leverage work already done for these initiatives (such as assessments or best practices in data management and governance).

- **Establish vision and mission for safety data management.** The vision and mission describe high-level opportunities for managing and governing safety data. They articulate a vision for and the outcome of improved safety data collection, accessibility, security, cost effectiveness, and other data management attributes.

- **Develop outcome statement.** The outcome statement describes the results the Safety DBP will achieve. A Safety DBP has numerous possible objectives, but all States need data systems that support safety problem identification, countermeasure analysis, and target setting at a statewide level.

STEP 2. ASSESS CURRENT STATE SAFETY DATA SYSTEM

Once initial planning is complete, the State should assess the current status of its safety data system. This section guides a State to conduct this assessment and develop an appropriate improvement plan. Key actions include: identifying data systems to include in the assessment, documenting current business processes for safety data systems, researching and summarizing past assessment efforts, updating past assessments, and conducting a capability maturity assessment. After completing this step, the State will understand its current capabilities related to safety data collection, analysis, governance, and interoperability.

IDENTIFY DATA SYSTEMS TO INCLUDE IN THE ASSESSMENT

The State should include any datasets, data systems, and data programs critical for safety analysis and target setting. Although the focus is on safety data systems other programs such as asset management, HPMS, infrastructure, operations, or supporting administrative data may also support safety decision-making. Data systems should have a clear connection to and support the DOT's mission, core business services, and performance objectives related to improving traveler safety.

The following criteria may help identify critical safety data systems:

- Does the data system support safety analysis, performance measures, and targets?
- Does the State use the data system to meet Federal or State mandates?
- Are there critical risks associated with lack of access to the data system?

The State should document basic information for each data system in a data inventory. The inventory should include significance of the data to the Safety DBP, data ownership, and linkages to the crash data system. The inventory should also reference supporting documentation such as user's manuals, data dictionaries, and training manuals. Table 4 illustrates a simplistic approach to documenting this information.

Table 4. Inventory of safety data systems.

Data System and Content	Significance to Safety DBP	Data Owner	Crash Data Linkage
Crash Data • Crash location • Date • Collision type • Severity • Number of fatalities • Number of injuries • Relationship to junction • Initial travel direction • Maneuvers by involved vehicles	Essential data set for all safety analysis; common reference for other safety data sets	State Highway Patrol; State DOT crash data manager	N/A

Table 4. Inventory of safety data systems (continuation).

Data System and Content	Significance to Safety DBP	Data Owner	Crash Data Linkage
Roadway Data • Segment identifier • Route number • Route/street name • Federal aid and route type • Rural or urban designation • Surface type • Begin and end point segment descriptors • Segment length • Direction of inventory • Functional class • Median type • Access control • One vs. two-way operations • Number of through lanes • Type of governmental ownership	Physical inventory needed to identify roadway risk factors and support countermeasure development	State DOT roadway inventory manager, State DOT HPMS manager, MPO information services manager	Linear reference system

Table 4. Inventory of safety data systems (continuation).

Data System and Content	Significance to Safety DBP	Data Owner	Crash Data Linkage
Intersection Data • Unique intersection identifier • Location identifier for road 1 crossing point • Location identifier for road 2 crossing point • Intersection / junction geometry • Intersection / junction traffic control • Unique approach identifier • Rural or urban designation • Number of intersection legs	Inventory needed to identify roadway risk factors and support countermeasure development	State DOT roadway inventory manager; MPO information services manager	Linear reference system
Interchange / Ramp Data • Unique interchange identifier • Location identifier for roadway at beginning and ending ramp terminal • Ramp length • Roadway type at beginning and ending ramp terminal • Interchange type • Functional class • Type of governmental ownership	Inventory needed to identify roadway risk factors and support countermeasure development	State DOT roadway inventory manager; State DOT HPMS manager; MPO information services manager	Linear reference system

Table 4. Inventory of safety data systems (continuation).

Data System and Content	Significance to Safety DBP	Data Owner	Crash Data Linkage
Traffic Data • Annual average daily traffic • Annual average daily traffic for each intersecting road at intersection • Annual average daily traffic at ramp • Annual average daily traffic year • Vehicle/ Road User Mix	Allows for comparison of locations by crash rate and supports advanced analysis methods	State DOT traffic information manager	Linear reference system
Project Data • Project location • Project type • Project cost • Project implementation dates • Project-specific traffic volume estimates	Allows for ability to track project and program-level outcomes	State DOT project inventory manager	Linear reference system

DOCUMENT CURRENT BUSINESS PROCESSES

The State should document current business processes and workflows for safety data collection, processing, analysis, and reporting. One common method is to develop Unified Modeling Language use case diagrams and corresponding use case narratives. Use case diagrams are graphic depictions of the interactions among the following elements of a data system, as shown in Figure 6:

- Actors are represented by a person figure or disk symbol. These are users, external operators, or systems interfacing with safety data. The disk symbol may represent a database, data process, a data system, an agency, or a web application.
- Actions or business processes are depicted as ovals. These represent the functionality a system or service provides to users.
- The lines connecting data users and actions represent information flows.

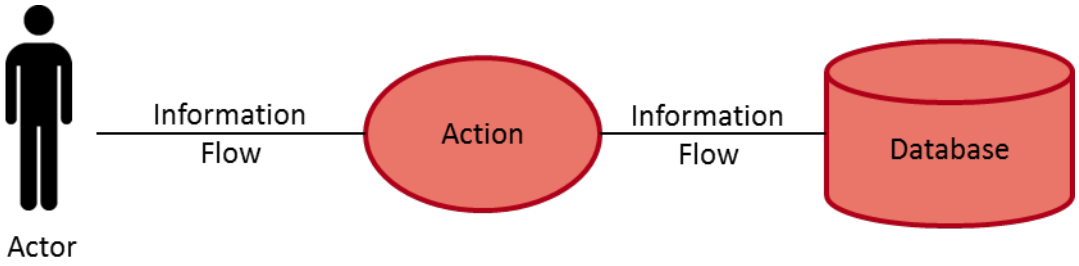


Figure 6. Diagram. Unified modeling language use case schematic.

Use case diagrams are helpful for visualizing and comparing business processes. The diagrams depict the full data management life cycle of a data system, including how data is collected, stored, analyzed, augmented, disseminated, and reported. The State should conduct extensive interviews with data system owners to document business processes and obtain supporting information such as user manuals.

The State can use tools such as Visio or Microsoft PowerPoint to develop the use case diagrams. Each element should include simple text descriptions to clarify business processes. Figure 7 shows an example use case diagram for regional traffic data collection.

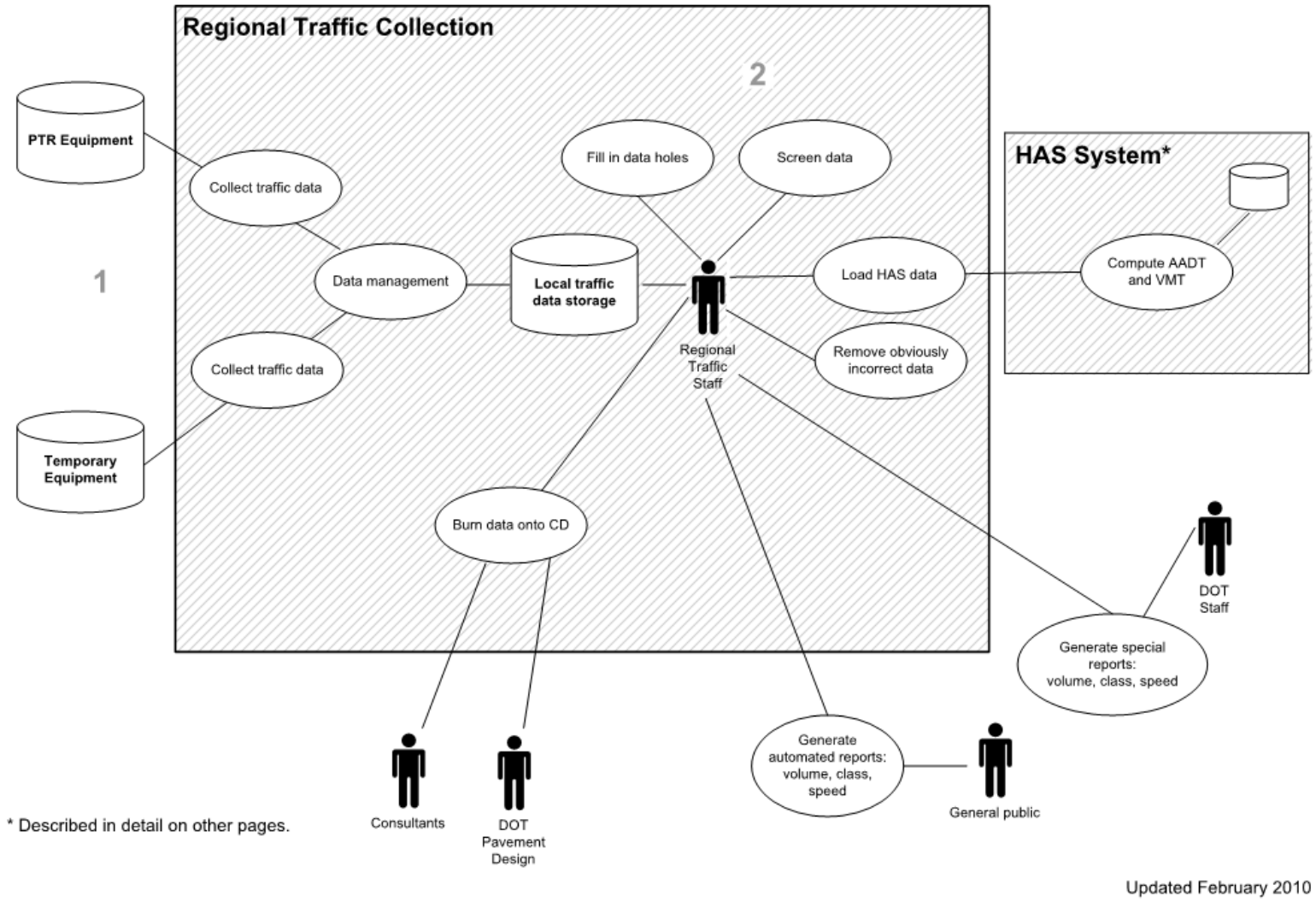


Figure 7. Diagram. Example use case diagram for regional traffic collection.

Source: Cambridge Systematics, Inc. Data Business Plan: Concept of Operations. Prepared for the Alaska Department of Transportation and Public Facilities, September 2005.

The State should develop an accompanying narrative to document each business process in detail. The narrative provides additional explanation of business processes not easily explained in the diagram (for example, defining acronyms or describing a particular software product). Figure 8 shows an example narrative for regional traffic data collection.

Documenting current business processes helps the State to maintain standards and consistency, train new hires, adhere to policy, and plan for data management improvements.

Regional Traffic Collection Processes

DOT regions perform the following steps to collect traffic data Highway Analysis System (HAS):

a. *Traffic collection is done by region with reports and data sent to Headquarters Traffic staff for Federal reporting. Two major process flows are in place: counter traffic collection and Weigh-in-motion. To meet Highway Performance Monitoring System requirements, the cycle of study is once every three years at a minimum. Results of traffic collection are stored locally. Access and individual files are used as the local repository. Peak's software is used where possible.*
b. *Data from permanent traffic recorders (PTR) are collected either via dial-up, Internet, or physically going out to site.*
c. *Temporary traffic counters are collected by going out to the site. Each study takes 1 to 3 weeks. Configuration varies by location and needs.*
d. *Regional Traffic staff review the data collected to accept, rerun and provide data to requestors. Corrected data is loaded into HAS for HPMS and other reporting.*
e. *Data in the form of reports are made available to other ADOT&PF staff including consultants and Pavement Design staff.*
f. *ADOT&PF staff and the general public request data. The process to provide the data is a manual process.*

Figure 8. Callout. Example use case narrative.

Source: Cambridge Systematics, Inc. Data Business Plan: Concept of Operations. Prepared for the Alaska Department of Transportation and Public Facilities, September 2005.

RESEARCH AND SUMMARIZE CURRENT AND PAST ASSESSMENT EFFORTS

The State should examine current and past evaluations of its data management and governance capabilities, as well as assessments of safety data quality. The DOT may have conducted these assessments as part of other projects to upgrade legacy data systems, implement safety analysis tools, plan for asset management, or conduct risk assessments. The State should include assessments from other business areas outside of safety as appropriate. For example, other business offices may have conducted assessments as part of ad hoc data governance initiatives.

The State should also examine results from national programs such as the Crash Data Improvement Program, Roadway Data Improvement Program, Roadway Safety Data Capabilities Assessment, Traffic Records Assessment, and others. These programs provide independent evaluations of the strengths and weaknesses of a State's data systems, as well as recommendations for the State's consideration. Descriptions of these programs are as follows.

Crash Data Improvement Program. The Crash Data Improvement Program is a NHTSA-sponsored technical assistance program that provides States an in-depth audit of their crash data systems and data quality. The evaluation team provides recommendations for improvement and performance measures that establish timeliness, accuracy, completeness, uniformity, integration, and accessibility to States that complete the program. NHTSA has updated the program and manual to reference new publications. The program incorporates a MMUCC mapping assessment that follows the new *Mapping to MMUCC* rules and leverages online data collection and analysis tools to enhance the process. (Mapping to MMUCC: A Process for Comparing Police Crash Reports and State Crash Databases to the Model Minimum Uniform Crash Criteria. DOT HS 812 184, July 2015, http://www-nrd.nhtsa.dot.gov/Pubs/812184.pdf.) Any State can request a full crash data audit or the MMUCC assessment by sending a letter to their regional NHTSA office.

Roadway Data Improvement Program. The purpose of the Roadway Data Improvement Program is to help State transportation agencies improve the quality of their roadway data to better support safety and other DOT initiatives. This resource is patterned after the Crash Data Improvement Program and supports the Roadway Safety Data Program goals of providing guidance to State DOTs to improve the quality of roadway data needed for safety analysis. The Roadway Data Improvement Program provides information and guidance on:

- Roadway data collected.
- Data collection tools and methods.
- Transportation planning and coordination.
- Data management and governance.
- Establishing the baseline roadway network.
- Roadway data quality measurement.
- Data interoperability between State and local agencies.

- Use of roadway data in safety analysis.

Roadway Safety Data Capabilities Assessment. As part of its Roadway Safety Data Program, FHWA conducted a capabilities assessment for each State, the District of Columbia, and Puerto Rico on the collection, management, and use of roadway safety data. (United States Roadway Safety Data Capabilities Assessment, FHWA-SA-12-028, July 2012, http://safety.fhwa.dot.gov/rsdp/downloads/rsdp_usrsdca_final.pdf.) FHWA used a five-level capability maturity model to assess each State's current capability in the following areas: 1) Roadway Inventory Data Collection and Technical Standards; 2) Data Analysis Tools and Uses; 3) Data Management; and 4) Data Interoperability and Expandability. States also used the maturity model to identify their desired capability levels. FHWA provided States with Safety Data Action Plans that identified Safety Data improvement goals and discussed how to reach them. The initial assessment was conducted in 2011-2012. FHWA will conduct a second assessment in each State in 2018 to gauge progress since the 2011-2012 assessment.

Traffic Records Assessment. A traffic records assessment is a NHTSA-sponsored, independent peer review of a State's traffic records systems that includes an examination of the six core traffic records data systems: crash, driver, vehicle, roadway, citation and adjudication, and injury surveillance. The evaluation also examines data integration processes and the characteristics of a State's traffic records system management, including the TRCC's strategic planning process, which sets the framework for improving all aspects of the traffic records system. States must undertake an assessment every five years as an eligibility requirement under MAP-21 to apply for §405(c) traffic data improvement grant funding. Evaluators assess a State's responses to the questions outlined in the Traffic Records Program Assessment Advisory, which describes the ideal traffic records system. (NHTSA, Traffic Records Program Assessment Advisory, http://www-nrd.nhtsa.dot.gov/Pubs/811644.pdf.) The final report provides the State a clear picture of its performance in comparison to the ideal and includes both broad recommendations and specific, actionable considerations. States seeking further assistance may request free technical assistance and training programs to augment the assessment.

If a State has already completed these assessments, it should start by summarizing the results.

UPDATE PAST ASSESSMENTS

The State should update past assessment results to reflect progress in implementing improvements since the assessment date. The core stakeholder team should meet to discuss and update the implementation status of recommendations. The team should note which

recommendations are complete and which are still outstanding. The team should also note recommendations that are no longer valid or that it does not plan to pursue.

The State may obtain this information from the custodial agency or from multi-agency groups. For example, the TRCC monitors progress in implementing traffic records assessment recommendations as part of its annual §405c grant application to NHTSA. Table 5 shows an example matrix summarizing the assessment program or source, relevant data system or assessment area, recommendation, and implementation status.

This process helps States identify future data needs and prioritize areas of concern to address in later steps of the Safety DBP. The State may wish to include outstanding items in its Action Plan for the Safety DBP.

Table 5. Current and past assessments.

Source	Data System	Recommendation	Implementation Status
Crash Data Improvement Program	Crash	Recommendation	Status
Roadway Data Improvement Program	Roadway	…	…
…	…	…	…
…	…	…	…

CONDUCT CAPABILITY MATURITY ASSESSMENT

After the State has updated past assessments, it should assess its capabilities for collecting, managing, governing, and using safety data. The assessment process includes these steps:

1. Select assessment tool;
2. Assess current level of capability maturity;
3. Determine target level of maturity desired; and
4. Identify gaps.

Select Assessment Tool

One common assessment tool is a capability maturity model. As defined in NCHRP 666, a capability maturity model "is used to assess how the roles of people, technology, and institutional arrangements help the agency to advance from an un-governed State to a governed State." (NCHRP 666: Target-Setting Methods and Data Management to Support Performance-Based Resource Allocation by Transportation Agencies, Volume II: Guide for Target-Setting and Data Management, 2010.) Because the model describes various levels of maturity and the characteristics of those levels, a State can use it to establish a baseline and identify next steps in moving towards its desired end State for data management and governance. The desired end State is to establish and maintain a governance program that supports safety problem identification, countermeasure analysis, and target setting.

The recommended maturity model is adapted from the United States Roadway Safety Data Capabilities Assessment. (Vanasse Hangen Brustlin, Inc., United States Roadway Safety Data Capabilities Assessment, FHWA-SA-12-028, July 2012.) The model defines levels of maturity for the following dimensions of capability.

- **Safety Data Collection and Technical Standards:** What safety data are collected? Are there gaps in MIRE FDEs? How well do safety data systems meet data quality standards for timeliness, accuracy, completeness, consistency, integration, and accessibility, as defined in Table 6? Is a five-year history of crash data available for all public roadways?

- **Data Analysis Tools and Uses:** How well does the SSDS support the roadway safety management process, including network screening, diagnosis, countermeasure selection, and evaluation? How well does the SSDS support advanced analysis methods using tools such as the Highway Safety Manual, the Interactive Highway Safety Design Model, or AASHTOWare Safety Analyst™.

Table 6. Data quality standards.

Data Quality Standard	Definition
Completeness	The degree to which data is available for the public roadway network in the State, as well as the degree to which there are no missing or blank fields for critical data elements in the data system.
Timeliness	The degree to which data values or a set of values are provided at the time required or specified. For safety data, timeliness is the number of days between the event occurrence and entry of data into the appropriate database, or the time from when the custodial agency receives the data to the point of data entry into the database.
Accuracy	The degree to which there are no errors in critical data elements. Accuracy reflects the degree to which data is error free, satisfies internal validity checks, and does not exist in duplicate within a single database.
Uniformity or Consistency	The degree to which records in a database are consistent with some independent standard or the degree of consistency in element definitions and codes across State and non-State files. Uniformity is the number or percentage of records that agree with nationally accepted guidelines and standards such as MMUCC and MIRE FDEs.
Integration	The extent to which data records are linked between two or more data systems using common or unique identifiers. For safety data, integration is the percentage of data elements or records in a safety database linked to another system or dataset.
Accessibility	The relative ease with which users can retrieve and manipulate data to meet their needs. Accessibility is measured in terms of a user's ability to obtain data and the timeliness of the response to their request.

Sources: Traffic Data Quality Measurement Final Report, FHWA, September 2004; NHTSA Model Performance Measures for State Traffic Records Systems, DOT HS 811 441, February 2011; The Six Primary Dimensions for Data Quality Assessment, DAMA UK Working Group on Data Quality Dimensions, October 2013

- **Data Management and Governance:** Is there a data governance structure for the SSDS? For example, are there formally defined roles, accountability, and core capacities for data governance? Is there a designated data governance board, data stewards, and data owners? What policies and procedures exist for collecting, maintaining, using, and updating safety data? Are technology and tools for safety data management and analysis consistent, standardized, and updated?

- **Data Interoperability and Expandability:** To what extent are linked data sets from roadway, crash, and others included in safety analysis? Are existing safety data systems expandable as new technologies and tools are developed?

Each dimension of capability has five distinct maturity levels as follows:

- **Level 1 – Initial or Ad Hoc.** The agency is not aware of the need for capability in a specific dimension, or activities and relationships are taking place but largely in ad hoc, informal, and champion-driven efforts. There is no plan for interoperability or expandability.

- **Level 2 – Repeatable.** The results of previous projects and the demands of the current project drive activities and actions. Individual managers decide what to do on a case-by-case basis during individual projects.

- **Level 3 – Defined.** The agency documents technical and business processes rather than on a per-project basis. The agency's standards relate to an adopted strategy, and this guidance determines project outcomes. However, there is limited accountability and uneven alignment with internal and external partners.

- **Level 4 – Managed.** The agency uses process management to initialize and supervise individual projects. Performance is measured, processes are predictable, and the organization can develop rules and conditions regarding the quality of the products and processes. Internal and external partnerships are aligned.

- **Level 5 – Optimized.** Safety data management and governance is a full, sustainable program priority, with top-level management support and formal partnerships in place. The whole organization focuses on continuous improvement. The organization possesses the means to detect weaknesses and to strengthen areas of concern proactively.

Appendix F provides a recommended capability maturity model for assessing a State's safety data system. Worksheets are provided for States to note strengths, weaknesses, current

maturity level, desired maturity level, and actions to advance to the desired maturity level for each assessment area. States may wish to assign a separate maturity level for different elements of their safety data system. For example, there may be portions of a State's system that are operating at a higher maturity level, while others are at a lower level. States may note specific areas within the element they wish to improve. For desired maturity level, it is acceptable for States to choose a lower maturity level if it is realistic for the organization.

FHWA expects to publish a revised version of the capability maturity model in 2018. NCHRP Report 814 provides an alternative method and spreadsheet tools for States to assess the value of their data programs and data management processes. (Spy Pond Partners, LLC. Data to Support Transportation Agency Business Needs: A Self-Assessment Guide. NCHRP Report 814. Transportation Research Board, Washington, D.C., 2015. Available at: http://www.trb.org/Main/Blurbs/173470.aspx.)

Assess Current Level of Capability Maturity

The State should conduct outreach with safety data system stakeholders to assess its current maturity for each dimension of the capability maturity model. States can use the worksheets in Appendix F or the spreadsheet tools available through NCHRP Report 814 to conduct the assessment.

Instruments for gathering feedback include surveys, focus groups, workshops, research studies, or current assessments conducted through NHTSA programs. For example, one pilot State convened a workshop in which participants discussed each dimension and agreed on consensus ratings with other team members. For the second pilot, workshop participants completed the ratings individually (at the workshop). The State determined the consensus ratings by averaging the individual ratings.

Determine Target Level of Maturity Desired

After identifying a current maturity level for each dimension of the capability maturity model, stakeholders should determine a target level of maturity desired.

Figure 9 illustrates example results for a capability assessment. A hollow circle (○) indicates current level of capability. The solid circles indicate the target level of capability, and they are color coded to reflect the degree of gap. For example, a green circle (●) indicates no gap, in which the desired level of capability is the same as the current level. A yellow circle (●) indicates a small gap, in which there is one level difference between current and desired levels

of capability. A red circle (●) indicates a large gap, in which there are two or more levels between current and desired levels of capability.

After identifying target maturity levels, the State may wish to incorporate them into the vision and mission statements established in Step 1.

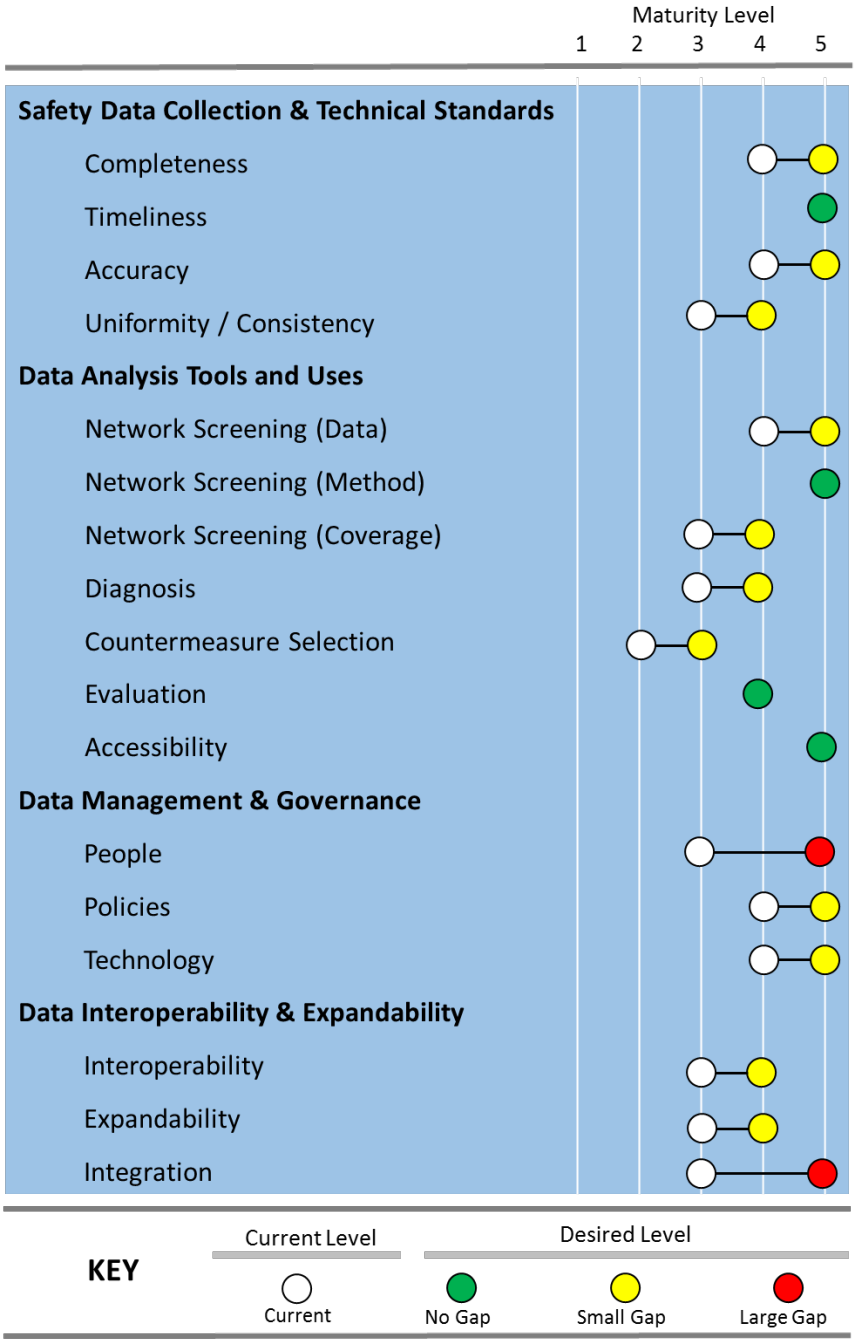


Figure 9. Graph. Capability assessment results.

Identify Gaps

The State should identify potential challenges or barriers preventing them from reaching the desired level. These could include: 1) needs and gaps within core business areas of the organization; and 2) needs and gaps based on primary job functions of the audience within the organization (for example, senior and mid-level managers, business data stewards, IT data stewards, users of data, data providers). They should also identify actions needed to advance from current to desired levels of maturity. These actions will help inform future steps in the Safety DBP development.

SUMMARY

Step 2: Assess Current SSDS, addresses the need for States to assess the current state of its safety data system and understand its current capabilities related to safety data collection, analysis, governance, and interoperability. The important actions in this step are:

- **Identify data systems to include in the assessment.** The State should include any datasets, data systems, and data programs critical for safety analysis and target setting. Although the focus is on safety data, other programs such as asset management, HPMS, infrastructure, operations, or supporting administrative data may also support safety decision-making. Data systems should have a clear connection to and support the DOT's mission, core business services, and performance objectives related to improving traveler safety.

KEY OUTPUTS AND WORK PRODUCTS

- ☐ Identification of data systems for the assessment
- ☐ Use case diagrams and accompanying narratives on business processes and workflows for safety data systems
- ☐ Summary of similarities and differences in data resolution and accuracy standards across all data
- ☐ Summary of past assessment recommendations in matrix form
- ☐ Update on State progress in implementing past assessment recommendations
- ☐ Assessment tool
- ☐ Assessment of current and desired levels of maturity for each dimension of the capability maturity model

- **Document current business processes.** Business process diagrams and accompanying narratives are helpful for visualizing and comparing business processes for safety data systems. The diagrams depict the full data management life cycle of a data system, including how data is collected, stored, analyzed, augmented, disseminated, and reported. The State

should conduct extensive interviews with data system owners to document business processes and obtain supporting information such as user manuals. Documenting current business processes helps to maintain standards and consistency, train new hires, adhere to policy, and plan for data management improvements.

- **Research and summarize current and past assessment efforts.** The DOT may have conducted assessments as part of other projects to upgrade legacy data systems, implement safety analysis tools, plan for asset management, or conduct risk assessments. The State should include assessments from other business areas outside of safety as appropriate. They should also examine results from national programs such as the Crash Data Improvement Program, Roadway Data Improvement Program, Roadway Safety Data Capabilities Assessment, Traffic Records Assessment, and others. These programs provide independent evaluations of the strengths and weaknesses of a State's data systems, as well as recommendations for their consideration. The State can organize the assessment recommendations in matrix form by agency, data system, assessment program/source, and recommendation.

- **Update past assessments.** States should update progress in implementing improvements since the assessment date. This helps identify future needs and prioritize areas of concern for the Safety DBP.

- **Conduct capability maturity assessment.** The State should assess its current capabilities for collecting, managing, governing, and using safety data using a capability maturity model. The recommended maturity model is adapted from the United States Roadway Safety Data Capabilities Assessment. It defines levels of maturity for safety data collection, analysis, management and governance, and interoperability. States should also determine a target level of maturity desired, as well as actions needed to advance from current to desired levels of maturity.

STEP 3. ESTABLISH A DATA GOVERNANCE PROGRAM

Once the assessment is complete, the State should establish a plan for improving data management through a Data Governance Program. Key actions include establishing core data principles, developing a Governance Model, defining data governance roles and responsibilities, and documenting the Data Governance Program. This section defines data management and data governance and then discusses these key actions in more detail. Appendix G provides additional information on data governance. After completing this step, the State will have a roadmap for improving data management with a Data Governance Program and documentation to support its implementation.

DATA MANAGEMENT AND GOVERNANCE DEFINED

Data management is the development, execution, and oversight of architectures, policies, practices, and procedures to manage the information lifecycle needs of an enterprise in an effective manner as it pertains to data collection, storage, security, data inventory, analysis, quality control, reporting, and visualization.

Data governance is the "execution and enforcement of *authority* over the management of data assets and the performance of data management functions." (NCHRP 666: Target-Setting Methods and Data Management to Support Performance-Based Resource Allocation by Transportation Agencies, Volume II: Guide for Target-Setting and Data Management, 2010.) The purpose of data governance is not to *manage* data, but rather to *guide* and *monitor* the proper management of data by establishing clear authority and policies for managing data at the agency-wide level. A Data Governance Program is one of the recommended tools for addressing safety data management in this Guide.

Figure 10 depicts data governance activities as follows:

- **Create and align rules.** Initially, the Governance Program establishes the policies and decision-making process for managing data. It also formalizes the roles and responsibilities of all stakeholders involved.

- **Enforce rules and resolve conflicts.** Next, the program ensures stakeholders are applying data management rules and processes correctly. It provides a forum for resolving conflicts if needed.

- **Provide ongoing support.** Finally, the program provides ongoing support to stakeholders who are applying data management rules and processes. It also identifies new opportunities for creating rules or adapting to existing ones, thus continuing the data governance lifecycle.

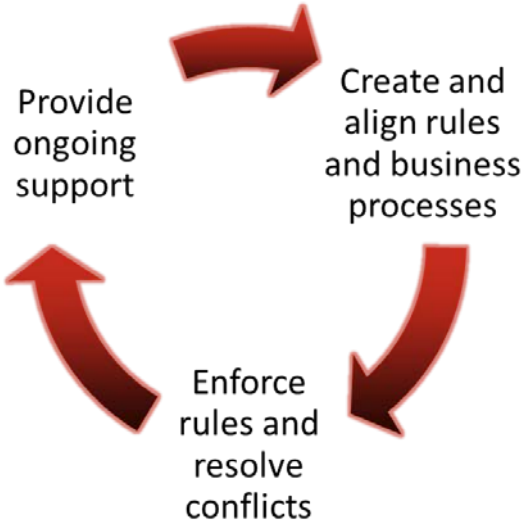


Figure 10. Flow chart. Data governance activities.

Source: C. Cabrera, "Data Governance Defined and Why It is Crucial to the Organization," April 15, 2009. http://www.element61.be/e/resourc-detail.asp?ResourceId=6.

A well-defined Data Governance Program is vital to ensure the integrity of safety (and all other) data analyses performed in a DOT. The Data Governance Program must:

- **Have executive buy-in and support.** Everyone in the organization needs to know the importance of, and commitment the agency has to data governance.

- **Be comprehensive in scope.** The entire data lifecycle, from collection through management, analytics, and distribution is subject to the agency's data governance program. Because data are collected by so many different programs, using different standards, and for different purposes, it is critical that data governance spans the gaps between data systems. Data are collected by specific DOT programs for their purposes (such as reporting, analytics, operations, planning, etc.) but are often required in the business processes of other programs in the DOT.

While the term "governance" may have negative connotations (due to new rules, regulations, and policies imposed on workflow processes and potential organizational changes), its benefits far outweigh any perceived negative impact. The benefits of data governance are evident from a policy, practical, and technical perspective as documented in NCHRP 666 as follows: (NCHRP

666: Target-Setting Methods and Data Management to Support Performance-Based Resource Allocation by Transportation Agencies, Volume II: Guide for Target-Setting and Data Management, 2010.)

> *From a policy standpoint, data governance promotes the understanding of data as a valuable asset to the organization and encourages the management of data from both a technical and business perspective.*
>
> *On a practical level, the use of a data governance model provides for access to data standards, policies, and procedures on an enterprise basis. It provides a central focus for identifying and establishing rules for the collection, storage, and use of data in the organization.*
>
> *From a technical perspective, use of data governance results in reducing the need to maintain duplicate data systems, improves data quality, and provides new opportunities to implement better tools for managing and integrating data.*

The benefits of data governance also extend to a State's data management practices. For example, it can help eliminate confusion over which offices are responsible for different data systems. Identifying the system of record in a data catalog provides a consistent source of information for addressing inquiries and producing reports. Finally, it can improve how States share data with the Community of Interest. Safety managers need to understand and communicate these benefits to upper management to obtain funding and resources for implementing data governance.

DEVELOP DATA PRINCIPLES

First, a State should develop data principles to guide governance practices at the DOT. The American Association of State Highway and Transportation Officials (AASHTO) recommend the following data principles: (AASHTO Subcommittee on Data, Data Subcommittee Efforts on Core Data Principles website, https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnx0cmJkYXRhc2VjdGlvbnxneDoxZDc3YjczNjUxZjlxZmM3.)

- **Principle 1 – VALUABLE: Data is an asset**—Data is a core business asset that has value and is managed accordingly.
- **Principle 2 – AVAILABLE: Data is open, accessible, transparent and shared**—Access to data is critical to performing duties and functions, data must be open and usable for diverse applications and open to all.
- **Principle 3 – RELIABLE: Data quality and extent is fit for a variety of applications**—Data quality is acceptable and meets the needs for which it is intended.

- **Principle 4 – AUTHORIZED: Data is secure and compliant with regulations**—Data is trustworthy and is safeguarded from unauthorized access, whether malicious, fraudulent or erroneous

- **Principle 5 – CLEAR: There is a common vocabulary and data definition**—Data dictionaries are developed and metadata established to maximize consistency and transparency of data across systems.

- **Principle 6 – EFFICIENT: Data is not duplicated**—Data is collected once and used many times for many purposes.

- **Principle 7 – ACCOUNTABLE: Decisions maximize the benefit of data**—Timely, relevant, high quality data are essential to maximize the utility of data for decision-making.

DEVELOP A GOVERNANCE MODEL

Next, the State should develop a safety data governance model (Governance Model) to establish the organizational framework and structure for governing its safety data system. Figure 11 illustrates a general governance model. The oval shapes represent various stakeholders, and the rectangles depict strategic goals, business processes, data systems, and governance components.

NCHRP 666 explains the hierarchy between the data management, data governance, and data stewardship components of a governance model: (NCHRP 666: Target-Setting Methods and Data Management to Support Performance-Based Resource Allocation by Transportation Agencies, Volume II: Guide for Target-Setting and Data Management, 2010.)

> *The data governance role primarily represents the individuals responsible for establishing overall policies, standards, and procedures that are to be followed by the organization. The data stewardship role represents the team of individuals throughout the organization who are responsible for enacting these policies and procedures on a daily basis. The data management program can be considered the umbrella overseeing all activities related to the management of core data systems.*

The management of data assets is usually accomplished through a Data Governance Board. The Data Governance Board, typically comprised of senior level managers across all business areas, is the authoritative body that serves in an oversight role for managing the data governance activities of an organization. This role ensures data programs are successfully managed to meet the business needs and help achieve the agency's strategic vision, mission, and goals for data. Data Stewards and Custodians manage the data systems used to support core business processes and functions of

the division, as well as the internal and external stakeholders who share a common interest as users of those data systems (also known as the Community of Interest).

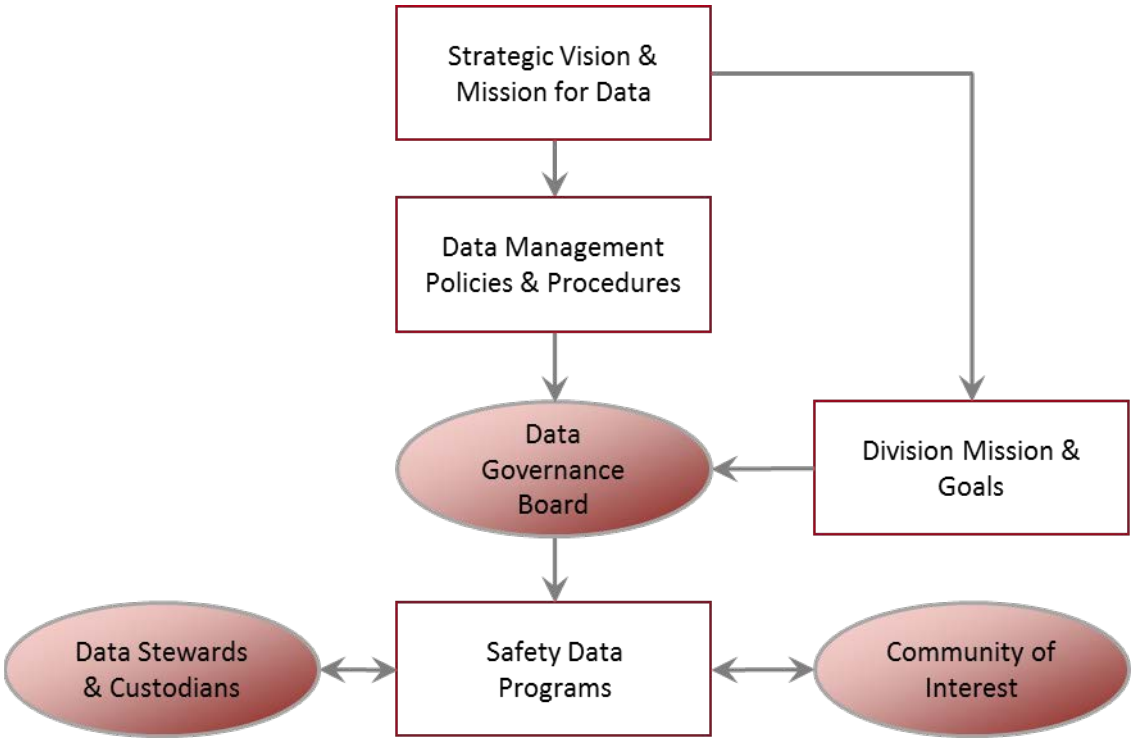


Figure 11. Organizational chart. General data governance model.

Source: Adapted from NCHRP 666, Figure 4.2, Overview of a general data governance framework.

Figure 12 illustrates an example Governance Model for Safety Data. The model identifies specific business processes, safety applications and tools, and safety data systems that the data governance program supports. An external department of public safety (or similarly named State agency) often houses the crash database. However, the DOT may maintain a copy for geolocating crash data, conducting safety analyses, and programming projects to improve safety as part of their HSIP.

State safety program managers are the most knowledgeable regarding their safety data systems and program needs; therefore, they play a critical role in developing a governance model that addresses those needs and provides maximum benefit to the Community of Interest.

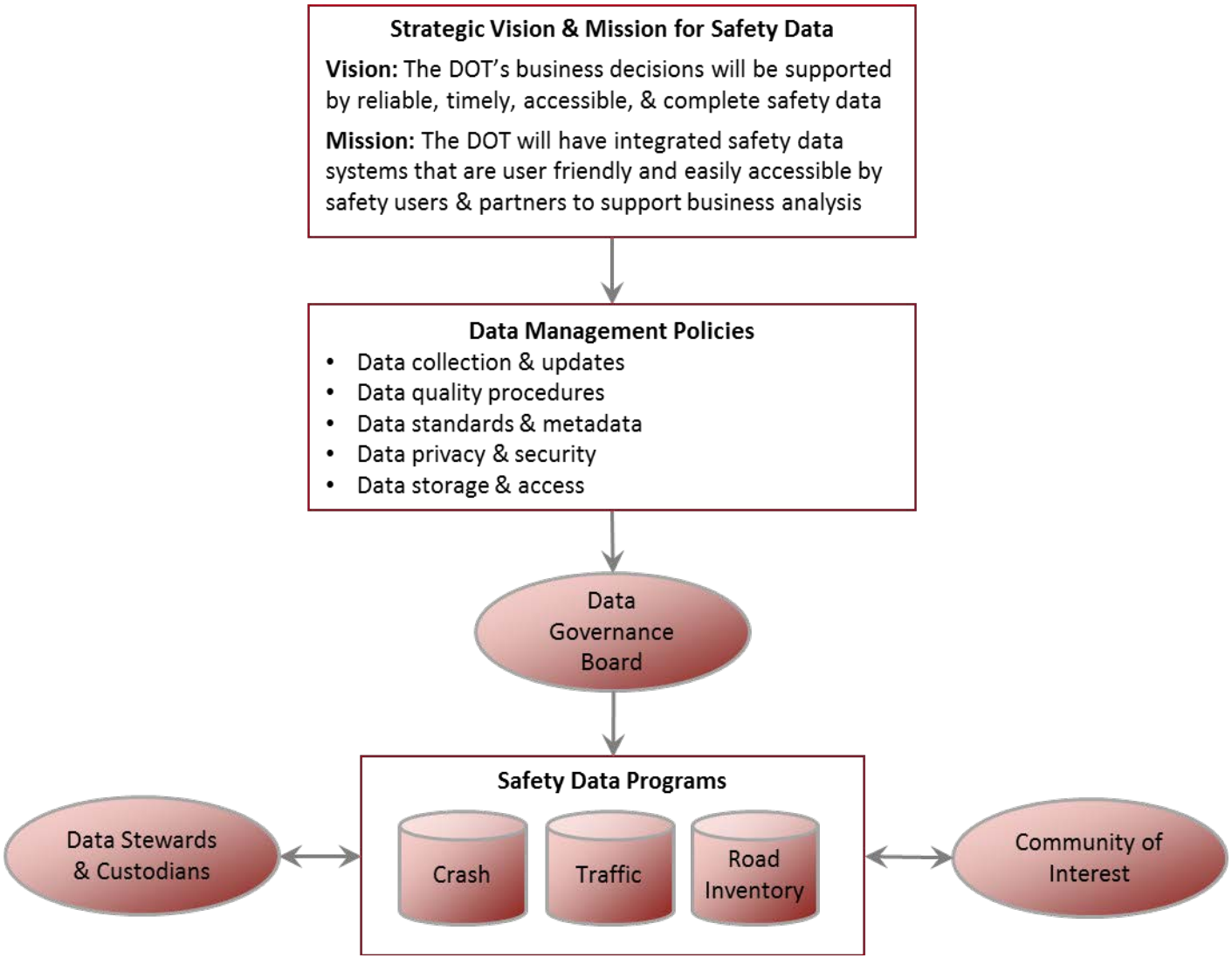


Figure 12. Organizational chart. Safety data governance model.

The governance model should consider the organizational structure of the DOT, with the understanding that some organization changes may be necessary to implement data management. The governance model should also reflect the status of data governance initiatives within the DOT as determined in Step 1:

- If there are no other management or governance initiatives underway, the State should implement safety data management and governance as stand-alone initiatives and reflect the needs of safety stakeholders within the DOT, as shown in Figure 12. The governance model should include coordination with the IT office and other business areas charged with collecting or managing safety related data.

- If management and governance initiatives are underway within one or two other offices, the governance model should complement those efforts while meeting the needs of safety stakeholders within the DOT. The Safety Data Governance Board should coordinate with other Boards to leverage applicable policies and decision-making processes for managing data.

- If management and governance initiatives are underway at the agency-wide level, State safety program managers should designate a representative on the Data Governance Board. If an agency-wide governance model exists, the safety program manager should work with the Board to incorporate the safety program's strategic goals, business processes, and data systems into the larger governance model. If there is no model in place, the State should develop a safety-specific governance model that fits within the context of the larger initiative.

ESTABLISH EOLES AND RESPONSIBILITIES FOR MANAGEMENT AND GOVERNANCE

Next, the state should establish roles and responsibilities for data management and governance. Establishing roles and responsibilities for data governance helps to embed these practices into the culture and day-to-day business operations. The State should reach out to other business areas responsible for safety data systems to help identify roles and responsibilities. Table 7 defines the roles and responsibilities recommended to support a governance model.

Although there are distinct roles defined, it is important to note the roles do not equate to distinct positions or people. Once the state has adopted these roles, they should develop a staffing plan to identify the positions or people who will fulfill the roles. They may need to identify new positions to support the Governance Program. The State should formalize and institutionalize governance roles and responsibilities by incorporating them into staff job descriptions, job duties, and performance plans.

Table 7. Data governance roles and responsibilities.

Role	Description	Responsibilities
Data Governance Board	Senior level managers across business areas of agency; typically includes director of the IT office or division. The Board may include representatives from external agencies charged with statutory authority for managing a specific data system.	• Implement policies and procedures for collecting, managing, and using data and information. Appendix G provides additional guidance on data management practices.
Chief Data Steward	An executive data steward who serves as the chair of the Data Governance Board and as the primary business champion of a data management program.	• Chair the Data Governance Board • Serve as primary champion of a data management program
Data Stewards	Individuals who ensure data is collected, updated, managed, and used in accordance with policies established by the Board. Data Stewards may be internal or external to the DOT, depending on the agency charged with statutory authority for managing a specific data system.	• Identify and manage metadata • Identify and resolve data quality issues • Determine business and security needs of data • Communicate data quality issues to individuals who can influence change • Provide input to data analysis
Data Business Owners	Individuals who establish business requirements for use of data in their business area. They also may approve access to data systems supported by their business area. Data Business Owners may be internal or external to the DOT, depending on the agency charged with statutory authority for managing a specific data system.	• Establish business rules for use of data in their business area • May approve access to systems supported by their business area
Data Custodians	Individuals who provide technical support for data systems. This may include IT staff such as network administrators, database administrators, server administrators, and IT security. This may also include application programmers and systems analysts who work in business areas other than the IT office or division.	• Ensure safety and integrity of data in custody of IT • Implement system and data access controls appropriate for security • Provide reasonable safeguards for information resources

Table 7. Data governance roles and responsibilities (continuation).

Role	Description	Responsibilities
Working Groups (sub-committees)	A group of people who collect and provide data and establish business rules and processes for a specific data system. Working Groups may include internal and external stakeholders.	• Provide recommendations to the Board regarding data products to meet business needs • Provide recommendations to the Board regarding standards and procedures for collecting, maintaining, and using data systems and products within the agency • Provide recommendations regarding technology tools to support data management at the agency
Community of Interest	Association of people comprised of internal and external stakeholders who share a common interest as users of a data system.	• Communicate with Data Business Owners regarding their business needs for data systems

Sources: NCHRP 666: Target-Setting Methods and Data Management to Support Performance-Based Resource Allocation by Transportation Agencies, Volume II: Guide for Target-Setting and Data Management, 2010.; Data Governance, Standards, and Knowledge Management, Alaska Department of Transportation and Public Facilities (ADOT&PF), 2009, Appendix B – Kansas Department of Education Roles and Responsibilities and Appendix C – Data Governance Manual; The DAMA Dictionary of Data Management, the Data Management Association (DAMA), 2nd Edition, 2011.

As with the governance model, the roles and responsibilities depend on whether there are other governance initiatives underway within the DOT, such as:

- If there are no other data management or governance initiatives underway, the roles and responsibilities should reflect the organizational structure of the safety program within the DOT. They may also include other program areas or external agencies statutorily authorized to collect or maintain safety related data.

- If data management or governance initiatives are underway within one or two other offices, the roles and responsibilities should complement those efforts as appropriate. If necessary, the State may define additional roles and responsibilities to meet the needs of safety stakeholders.

- If data management or governance efforts are underway at the agency-wide level, the Governance Program should integrate those efforts. The roles and responsibilities for safety data governance should complement those defined for the larger enterprise initiative.

The State should also determine the authority and organizational responsibility for data governance. Authority is often granted under a policy directive from executive management. Organizational responsibility should be a shared at the senior level via the Data Governance Board and at the individual office level with business area managers. The determination of organizational responsibility is unique for each DOT, as each has a distinct culture and characteristics in the way their data systems have evolved.

DEVELOP IT PROJECT GOVERNANCE

The IT office also plays an important role in the Governance Program, and the IT Director should participate on the Board. Traditionally, the IT office established the data standards, data dictionaries, and defining requirements for data applications. Now, individual business areas often help define requirements for data applications and customized software to meet their business needs. The partnership between the IT office and the business areas is vital for successful implementation of the Governance Program.

The IT office may have its own process for project development and prioritization that does not always align with safety business needs. States may need to revise their project selection process to balance safety data system improvements while accommodating the often-competing needs of other business units within the agency.

Appendix H documents key components of good practices for States to improve their IT project selection process. This includes the development and enforcement of consistent processes for IT project identification, prioritization, and selection criteria as follows:

- **Establish a formal process for submitting IT project requests.** States could conduct an annual (or more frequent) call for IT projects in which project sponsors are required to submit a project questionnaire describing the nature of the project, expected benefits and costs, and how it supports IT priorities. Project sponsors would obtain signatures from their division director to establish executive support for the proposed effort.

- **Establish a formal project prioritization and selection process.** States could appoint an IT Investment Selection Board to pre-review IT project requests. This group could discuss how proposals fit into overall agency priorities and explore alternate ways to handle project

requests. IT or Project Management Office staff could help develop project proposals and support the prioritization and selection process.

- **Establish criteria for IT project prioritization.** Example criteria include the following:
  - Ranking potential projects by value and benefits
  - Assessment of risks to determine investment priorities
  - Inventory of resource availability and allocation
  - Determination of an optimal or acceptable size of the project pipeline
  - Alignment of projects with the Department's strategic objectives, IT plan, and executive management input
  - Balancing different types of projects by purpose and benefit
  - Balancing opportunity, benefits, and risk
- **Use tools to support the IT project prioritization process.** This enables visibility, standardization, measurement, and continuous process improvement. Example tools include:
  - Spreadsheet tools
  - Software tools such as Decision Lens Software
  - Severity and risk assessment matrix
  - Project Portfolio Management tools
- **Engage executives in the IT project development and maintenance process.** The State's enterprise-wide data governance council (or executive steering committee) could review IT project requests and assess how they fit into larger priorities. This group would finalize project selections and determine budget and resource parameters. The governance council would coordinate with the IT Director on a regular basis to review prioritization and align new investment opportunities with business priorities.
- **Manage the IT pipeline.** The IT Department could maintain a database of current and potential projects. IT staff could periodically evaluate the status and performance of projects using Earned Value Analysis techniques and identify tasks outside of targets or thresholds. Staff could also make project continuation or termination decision at major project stages.

DEVELOP DATA GOVERNANCE DOCUMENTATION

Finally, the State should document data management plans in the form of a data governance charter, data governance manual, data catalog, and business terms glossary. While the Safety DBP provides a roadmap for developing data management in general, this supporting documentation provides accountability and rules of engagement for implementing the Governance Program. Therefore, they may develop and maintain this documentation separately from (and following implementation of) the Safety DBP. The following paragraphs briefly describe each of these documents.

- **Data Governance Charter:** The data governance charter is a high-level document that defines the authority of the Data Governance Council to oversee data management practices, policies, and procedures that support the Safety Program. The charter describes the business need, purpose, authority, goals, and membership of the Governance Program. The charter serves as a formal announcement for the initiative. It conveys there is active support from senior management, and there are resources assigned to fulfill the goals stated in the charter. The charter includes:
  - A high-level description of the business problem or safety data management challenge to establish the need for data management;
  - The purpose and authority for the Governance Program;
  - The vision, mission, and goals for governance;
  - The offices or business areas participating in the Governance Program; and
  - The effective date and duration of the Governance Program.
- **Data Governance Manual:** The data governance manual documents the State's policies, standards, roles, and responsibilities for managing safety data systems under the authority of the Governance Program. It also includes comprehensive, enterprise-wide data collection and quality standards, which are necessary to ensure data interoperability across disparate systems. Data interoperability promotes a single version of the truth and minimizes the problems created by different business units and programs drawing different conclusions based on their version of the data. The manual includes:
  - An introduction defining the goals for data governance, authority for the manual, and data governance principles that guide governance policies and actions;
  - The Governance Model illustrating the organizational structure and procedures for governing data systems;

  - Roles and responsibilities for governance, including members of the Data Governance Board, data stewards, data business owners, data custodians, working groups, and the Community of Interest;
  - The IT office's involvement in the safety program. This includes, but is not limited to, platforms used to warehouse safety data systems, protocols and IT tools used to link data from various sources, and mechanisms for sharing data both internally and externally;
  - The data systems included in the Governance Program;
  - Data management policies for data collection and updates, data quality procedures, data privacy and security, and data storage and access; and
  - Data standards defining naming conventions, metadata, reference and master data management, and disclosure and disposal policies.

- **Data Catalog:** The data catalog documents the safety data systems included in the Governance Program and the offices responsible for maintaining those systems. The data catalog can be included in the data governance manual or maintained as a separate document. It includes:
  - The system of record for specific safety data systems such as the State's road inventory database (as the primary source of roadway elements), or their traffic database (as the primary source of traffic data);
  - Contact information for the data stewards and data custodians who provide routine updates and maintenance of the databases and application systems; and
  - A data dictionary of all of the elements in the roadway or traffic database. This includes the element name, definition, attributes, file structure, coding conventions, and any metadata on how to use and interpret the data.
- **Business Terms Glossary:** The business terms glossary defines commonly used business terms for data stored in a safety data system. The glossary of terms can help safety professionals understand IT terminology and vice versa. It provides a single reference source for documenting how standard terms (such as "location") are defined and used across a DOT. For example, the term "location" may be defined as the point on a specific roadway identified somewhere between the beginning and end of a road or segment. Valid values for defining location may include mile point or latitude and longitude coordinates. A glossary also helps IT professionals define business terms correctly when developing or enhancing application systems to support the safety business area. Appendix I provides an example business terms glossary for safety data.

- **Data Sharing Agreements:** The State should implement formal data sharing agreements or memorandums of understanding as needed to facilitate data sharing between internal and external stakeholders. Data sharing agreements should identify data standards and file exchange protocols needed to facilitate data sharing, including:
  - Data definitions;
  - Data file structures;
  - Formats used for data transmission;
  - Frequency of transmission of data updates;
  - Names of individuals and offices who transmit and receive data updates;
  - Processes to secure the transmission of confidential data and information;
  - Standards and procedures to enable linking of data between data systems; and
  - Service level agreements for data quality areas such as timeliness and accessibility.

SUMMARY

Step 3: Establish a Data Governance Program, addresses the need for States to establish clear authority and policies for managing safety data. The important actions in this step are as follows:

- **Develop data principles.** Data principles are statements that help guide governance practices at the DOT. States may adopt AASHTO recommended data principles or develop their own.

- **Develop a governance model.** A governance model establishes the organizational framework and structure for governing data systems at a DOT. It includes a graphical representation of how various governance roles support the organization's safety data systems, business processes, and strategic vision and mission for data.

- **Establish roles and responsibilities for governance.** In this action, States define the roles and responsibilities needed to support the governance model. Potential governance roles at the DOT could include a Data Governance Council, data stewards, data business owners, data custodians, working groups, and the Community of Interest. It is important to note the roles do not equate to distinct positions or people. Once the State has adopted these roles, they should develop a staffing plan to identify the positions or people who will fulfill the roles. They also may need to identify new positions to support the Governance Program. Finally, they should determine the authority and organizational responsibility for data governance.

KEY OUTPUTS AND WORK PRODUCTS

- ☐ Core data principles
- ☐ Governance model
- ☐ Roles and responsibilities
- ☐ IT project selection process
- ☐ Data governance charter
- ☐ Data governance manual
- ☐ Data catalog
- ☐ Business terms glossary
- ☐ Common resolution and accuracy standards for linking data sources

- **Develop IT project governance.** The partnership between the IT office and the business areas is vital for successful implementation of the Governance Program. The IT Director should participate on the Data Governance Council. In addition, safety business areas should help define requirements for data applications and customized software to meet their business needs. The State may need to revise their project selection process to better accommodate safety business area needs. This action includes adopting best practices for IT project identification, prioritization, and selection criteria.

- **Develop data governance documentation.** The State should document its Data Governance Program in the form of a data governance charter, data governance manual, data catalog, business terms glossary, and data sharing agreements. While the Safety DBP provides a

roadmap for improving data management, this supporting documentation provides accountability and rules of engagement for implementing the Governance Program. The State may develop and maintain this documentation separately from the Safety DBP.

STEP 4. IDENTIFY NEEDS FOR SAFETY TOOLS AND TECHNOLOGY

In Step 4, the State should develop a strategy to improve its tools for safety data management. Key actions include identifying technology needs and developing a plan for improved use of tools. After completing this step, the State will understand its needs and weaknesses related to tools and will have a plan to enhance or replace these tools.

IDENTIFY NEEDS FOR IMPROVED TECHNOLOGY

The safety program often relies on data from other business areas, so technology that provides integration and sharing of data across business areas is critical for meeting the needs of the safety program. The State should review the assessment results from Step 2 to identify any technology challenges and needs. The State can use the following questions to identify additional gaps and areas for improvement:

- **Data Collection Technology**
  - Is there a need to improve roadway inventory data collection through innovative technology such as mobile laser scanning and remote sensing?
  - Is there a process for collecting and integrating data from non-state agencies?
  - Are law enforcement officials able to geolocate crashes in the field?
- **Data Tools**
  - Can the State meet the needs for the primary requirements of predictive analysis, systemic analysis, and data visualization?
  - Does the State's data tools provide: 1) data discovery, which allows users to access, prepare, and integrate safety data; 2) an ETL process, which transforms data into the proper format for safety analysis; and 3) analytical tools to conduct safety data analysis on all public roads?
  - Can users achieve consistent results when using safety analysis tools?
  - Do users need tools such as dashboards, scorecards, and data visualization to help with reporting, performance tracking, and analysis of safety data?
  - Do users need geospatial location capabilities to facilitate efficient visualization and analysis of data when using safety analysis tools?

  - Do users need additional functionality within applications such as enhanced modeling and reporting capabilities to help identify and prioritize safety improvements?
  - Can users generate customizable reports to support safety analysis?

- **System Improvements**
  - Do users need more streamlined access to data and information?
  - Are there data silos, especially for critical data sets needed to support safety programs?
  - Are State and non-state agencies data set compatible?

- **Knowledge Management**
  - Can staff access the latest information about safety systems, data, policies, reports, tools, and training resources through a centralized knowledge management system?
  - Are policies and processes properly documented?

- **Cost Management Solutions**
  - Do analysts need better tools to evaluate the best allocation of funding resources for safety projects?

- **IT Support**
  - Are IT staff involved in the planning process for safety data system improvements?
  - Are data stewards involved in the review of bids and purchases related to IT, software, and data management that support the applications managed by those stewards?
  - Are existing safety data systems expandable as new technologies and tools are developed?

The State should benchmark their practices against those of other States to identify additional gaps and ensure they are not overlooking any best practices. FHWA's Roadway Safety Data Program Toolbox has many resources available to support benchmarking. (FHWA Office of Safety, Roadway Safety Data Program website, http://safety.fhwa.dot.gov/rsdp/.)

DEVELOP PLAN FOR IMPROVED USE OF TOOLS

Once the needs are established, the State should develop a plan for enhancing or replacing safety tools and technology. For each of the following improvement areas, they should determine the level of effort and cost of each improvement and develop a prioritized list of actions for

implementing technology solutions. In some cases, they may already have initiatives underway to address the need for improved technology.

- **Data Collection Technology:** The State should identify opportunities for using innovative technology to improve safety data collection. For example, some States are using remote sensing technology such as Light Detection and Ranging (LiDAR) to collect a three dimensional model of roadway inventory and asset data, as shown in Figure 13. A State could add LiDAR to their existing data collection contracts for photo log and pavement condition imagery. They could then use the technology to automate extraction of roadway features such as pavement markings, curve and grade, lane widths, signs, and others. Other States are using web-based map technology to improve law enforcement's ability to locate crashes in the field. This technology combines a State's official road network or linear reference system with Global Positioning System data. It allows law enforcement officials to locate crashes in the field accurately and transfer data to the crash database electronically. This increases the accuracy of crash location and reduces the time needed to process crash data for use in planning and analysis. A State may benefit from using similar field-based data collection and transfer methods to obtain EMS and injury surveillance data from other State agencies.

- **Data Standards:** The State should implement comprehensive, enterprise-wide data collection and quality standards to ensure data interoperability across disparate systems. Data standards assure data quality is maintained at a consistent level as data is used and manipulated on an ongoing basis. FHWA's Data Integration Primer notes the following commonly used data standards: 1) the content and format for how data is stored in a database; 2) the protocols for how data are accessed and manipulated; and 3) the format in which data is transferred from its native system into another application or database.

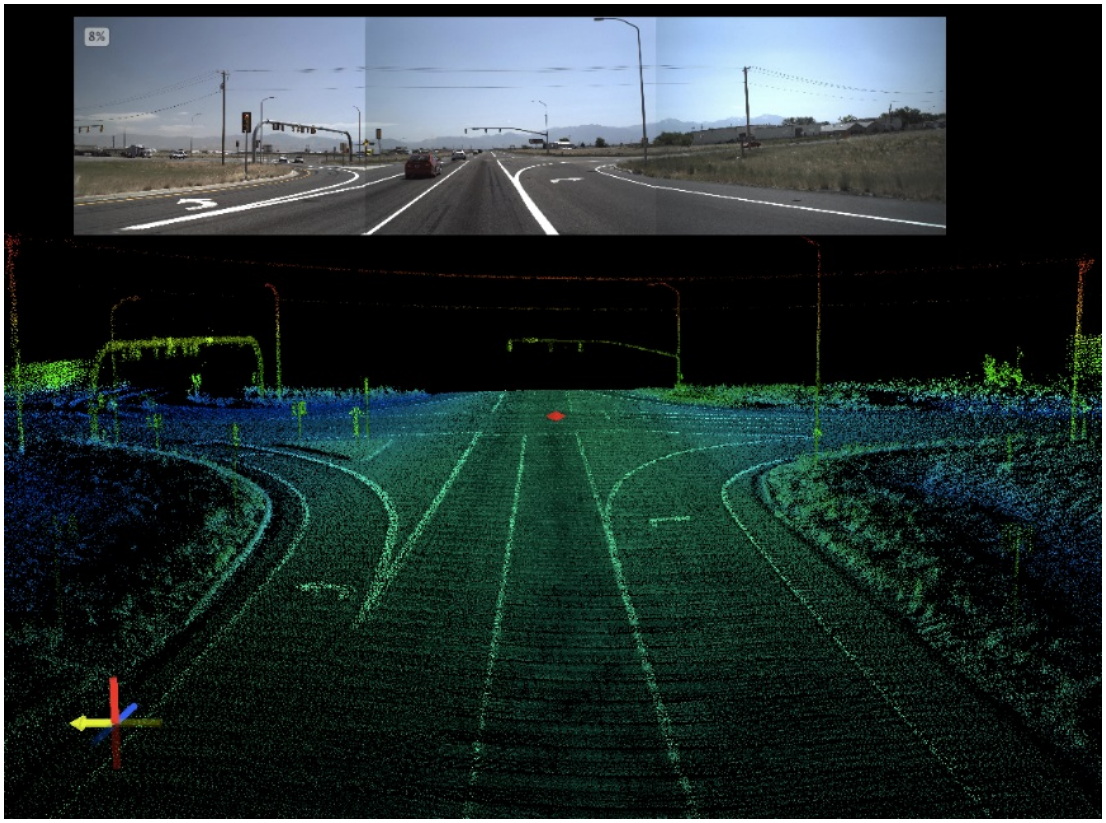


Figure 13. Photo. LiDAR imagery.

Source: Utah DOT Transportation Blog, Utah DOT Leveraging LiDAR for Asset Management Leap, February 25, 2013.

- **Data Tools:** The State should develop new data tools as needed to support advanced safety analysis. Data tools should provide the following capabilities:

  - **Data discovery.** Data discovery is the process by which users access, prepare, and integrate safety data for analysis. Data integration merges two or more data sources together. Geographic information systems (GIS) is one of the most commonly used tools for data integration. Because of the differences in native data sources, data management systems, and methods of data collection, geographic location is often the only common element that links these data. The location may exist: 1) as a latitude/longitude coordinate representation; 2) in the form of a linear referencing method that is applied to a LRS to give it spatial representation; and 3) a spatial feature in a GIS. GIS tools allow users to link safety datasets, visually view data inputs, make corrections if needed, and validate analytical tool outputs.

- **ETL Process.** Safety data may reside in one system or be drawn from their native "source" systems for the immediate purpose at hand (such as analysis, management, or reporting). The ETL process is necessary to move safety data from their native systems, transform it into the format required by the analytic software, and load the resulting file into the analytic software tool. ETL can be streamlined into a "one-button" application that automates the process. This allows States to conduct pre-processing of safety data routinely and consistently. However, specific IT skillset, as well as knowledge of the data, the source databases, and the analytics are required to perform the task properly and to ensure the integrity of the results.

> *"GIS is an essential technology to support quality assurance/quality control, ETL, and analytics necessary to perform and report safety data analyses."*
>
> *James Mitchell*
> *Louisiana Department. of Transportation & Development*

- **Analytical tools.** Safety analysis includes traditional safety analyses and advanced analyses as described in the Highway Safety Manual, or customized analyses that States might create for their own purposes. Analytical tools such as the Interactive Highway Safety Design Model and AASHTOWare Safety Analyst™ implement the methods shown in the Highway Safety Manual.

FHWA's Informational Guide for State, Tribal, and Local Safety Data Integration provides additional guidance on performing spatial data integration using GIS, performing the ETL process, and conducting safety analysis using integrated safety data. These capabilities must be implemented across different data systems to support advanced analysis. When procuring data tools, States should comply with State and Department IT architecture standards and requirements. The technology plan should include details on integration methods, standards, roles, responsibilities, training, and processes to support data quality.

- **System Improvements:** The State should enhance or replace legacy and silo safety data systems. In particular, they should focus on systems that support core safety business functions. The State should eliminate manual processes and migrate to newer systems that allow for improved functionality. These improvements will improve access to data and reduce data management costs associated with maintaining independent systems. The technology plan should leverage and improve upon tools, databases, and systems already working.

- **Knowledge Management System:** The State should implement a knowledge management system if one does not already exist. Knowledge management is a system for sharing and retaining critical organizational knowledge and business processes related to the creation,

capture, storage, and dissemination of safety data. For example, they could develop an online knowledge portal to exchange and share safety data and analysis tools with traffic safety professionals in the State. The portal could also contain instructions for accessing and using the data for safety analysis purposes. Figure 14 illustrates the relationships between knowledge management, data governance, and IT tools. While data governance provides the enforcement of authority regarding data management policies and practices, knowledge management ensures those policies and practices are kept current and accurate, stored in a manner where they can be easily retrieved, and made accessible to agency staff who need it to perform their duties. Knowledge management is also a vital tool for retaining organizational knowledge related to the design and development of application systems. A State can use best practices and lessons learned from similar projects to shorten the application development life cycle.

Figure 14. Venn diagram. Data governance and knowledge management.

Source: Adapted from Data Governance, Standards, and Knowledge Management, Alaska Department of Transportation and Public Facilities, 2009.

- **Cost Management Solutions:** The State should use cost management tools to allocate funding for safety projects. For example, one State developed a spreadsheet-based tool to assess the cost effectiveness of countermeasures using safety data from their data portal. The tool reports the economic benefits of implementing safety improvements based on crash statistics and the economic costs of certain crash types. The tool has helped them decide where to invest in safety improvements.

- **IT Support:** States must change their business processes and update data systems to meet their programs' business needs. However, data in older mainframe database systems is often not compatible with new technology such as GIS data management tools. Data governance is most successful when business offices and IT offices work as partners to ensure that: 1) business offices define their IT related needs, and 2) the IT offices procure the appropriate hardware and software to meet the agency's business needs.

  Before investing time and resources in technology improvements, the State should involve IT staff in the planning process and ensure all stakeholders understand the implications for both their business area and IT infrastructure. Similarly, the IT Department should involve data

stewards in the review of bids and purchases related to IT, software, and data management that support the applications managed by those stewards.

Lack of investment in technology and lack of coordination with IT can lead to significant operational problems. For example, one State invested significant resources to transition mainframe data to a new database structure and software. After dedicating significant resources to the effort, they discovered their IT infrastructure and standards were not adequate to support the new system. As a result, they were not able to share data with other business areas or the public as intended. In another case, a State invested in a robust data collection contract to meet Federal reporting requirements and the need for improved analysis capabilities in several program areas. As staff started receiving data from the contractor, they discovered there was inadequate space for storing the data on the existing infrastructure. As a result, data access is limited, and they are not able to use the data to its potential for supporting safety and other business area needs.

SUMMARY

Step 4: Identify Needs for Safety Tools and Technology, addresses the need for States to improve its tools for safety data management. The important actions in this step are:

- **Identify needs for improved technology.** States can use the assessment results from Step 2 to identify technology challenges and needs.

- **Develop plan for improved use of tools.** States should develop a plan for enhancing or replacing safety tools and technology. They should develop a prioritized list of actions for implementing technology solutions, and determine the level of effort and cost of each improvement. In some cases, States may already have initiatives underway to address the need for improved technology.

KEY OUTPUTS AND WORK PRODUCTS

- ☐ Summary of needs and weaknesses related to safety tools and technology
- ☐ Plan for enhancing or replacing safety tools and technology

STEP 5. DEVELOP ACTION PLAN

After the State identifies its technology needs, it should develop a plan for implementing the Safety DBP. Key actions include summarizing the challenges, issues, and gaps identified in previous steps, identifying priorities, and developing an action plan for improving safety data. After completing this step, the State will know its most critical deficiencies and have an action plan to address those deficiencies.

SUMMARIZE GAPS AND IMPROVEMENTS

First, the State should summarize the specific challenges, issues, and gaps identified in previous steps. The State should categorize gaps in the following areas:

- **System:** Gaps related to data collection, data access, data integration, data quality and validation, data storage, and documentation.
- **Technology:** Gaps related to data collection technology, data tools, database design, system improvements, system interfaces, knowledge management system, cost management solutions, and IT support.
- **Institutional:** Gaps related to data management and governance, data ownership, coordination across business areas, resource availability, and training needs.

The State should also identify improvements to address the gaps within each area. One approach is to compare the "current" situation to an ideal or future "desired" condition and identify the necessary improvements to close the gaps. For example, in the institutional area, the State may need to establish business rules to enable sharing of safety data between business areas. They can also use the business process diagrams and narratives from Step 2 to identify gaps, overlaps, and inefficiencies in business processes.

States can also leverage the resources in Table 8 to identify additional actions to resolve gaps. They should obtain input from data business owners or directives from senior management to determine critical gaps.

Table 8. Resources for identifying improvements.

Resource	Summary	Link
NCHRP Report 814: Data to Support Transportation Agency Business Needs	Appendix D contains resources for identifying potential data improvements.	http://www.trb.org/Main/Blurbs/173470.aspx
Improving Safety Data Programs Through Data Governance and Data Business Planning	Peer exchange summary that describes State practices in data governance and data business planning for safety applications.	http://onlinepubs.trb.org/onlinepubs/circulars/ec196.pdf
Informational Guide for State, Tribal, and Local Safety Data Integration	Provides guidance to States, Tribes, and local agencies on the steps and effective methods of safety data integration.	https://safety.fhwa.dot.gov/rsdp/downloads/fhwasa16118.pdf
FHWA Transportation Performance Management Toolbox	Provides guidance, self-assessment tools, and resources for States to enhance performance management practices.	https://www.tpmtools.org/

IDENTIFY PRIORITIES

Next, the State should prioritize the list of gaps to identify the most critical needs. One approach is to consider the risks associated with the gaps and their impact on achieving their safety program objectives. They may also consider the potential impacts of an interruption in critical business processes, as shown in Table 9.

Table 9. Example risk assessment.

Risk Statement	Negative Impact
If safety data are not collected…	Then the DOT could not evaluate and identify countermeasures for crashes
If there is a lack of a proper geospatial framework for data integration…	Then data could be stored in many different formats. Not having a single method of integration would affect the quality and availability of different data sources for analysis. Data collection efforts may be duplicated across divisions. There would be no ability to account for the changing nature of the roadway network over time. Decisions may be made with limited information.
If data systems are not maintained to modern standards…	Then the IT office might be unable to support the system, there might be difficulty integrating with modern systems; integration efforts may be fragmented, or there might be an inability to enhance or modify the system.
If there is no coordination across offices to exchange information between safety data systems…	Then there could be limits to analysis and reporting, and there could be disconnected data resources.
If resources for maintaining current safety data systems are reduced or eliminated…	Then there could be delayed application development, there could be delayed data publication, or there could be a reduced ability to address urgent safety business needs.
If staff have limited knowledge of safety analysis tools…	Then there could be inconsistent approaches to analysis, documentation, and increased time to review and correct work.
If there is distrust in the quality of data for safety analysis tools…	Then there could be hesitancy to use safety analysis tools. Staff avoiding using tools will revert to using crash rates and basic crash history. This requires greater investment of staff time in doing analysis because safety analysis tools can quickly produce summaries (analysis results that otherwise would take weeks to complete manually and in other cases would be impossible to do without the tool).

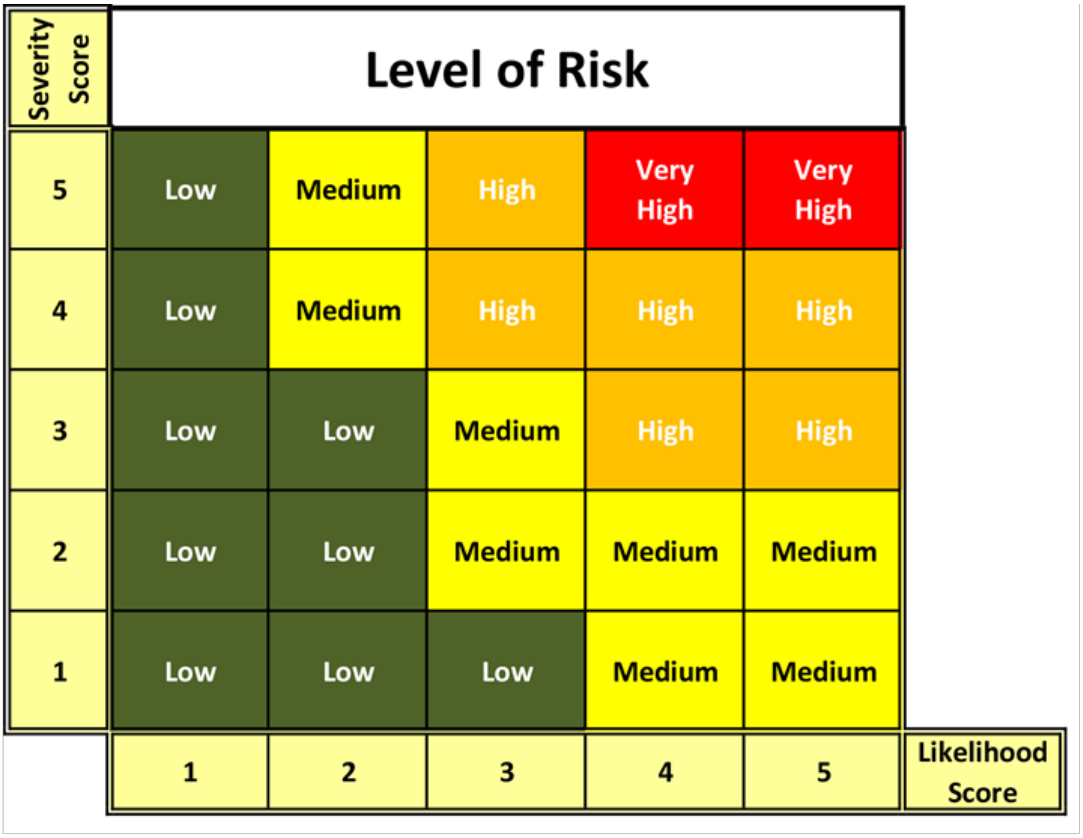
In its pilot study, Washington State DOT applied a four-step risk assessment process to identify, assess, and address risks for its safety data system as follows:

- **Risk Identification:** Collect and identify risks throughout the organization and develop a risk-list.
- **Risk Evaluation:** Determine the likelihood (frequency) and severity (degree of impact) for each risk.
- **Risk Analysis:** Rank and prioritize the risks, determine the level of risk (based on the likelihood and severity scores, as shown in Figure 15), and assign responsibility for management of risks.
- **Risk Response:** Determine the Risk Treatment Strategy and action to address risks; develop, implement, and monitor risk treatment strategies; and monitor and sustain mitigation best practices.

WSDOT's risk assessment process helped identify additional action items for their Safety DBP. The level of risk also helped prioritize the action plan recommendations.

Another approach is to assign a priority for filling gaps based on a general assessment of the required investment and resulting value to the agency as follows:

- Low priority – The required investment and resulting benefits do not add significant value to the agency;
- Medium priority – The agency should fill the gap as time and investment permits; however, safety analysis can proceed without filling this gap; and
- High priority – The agency should fill this gap as soon as possible as it is associated with high risks, it provides high value to the agency, or it is required for successful and accurate safety analysis.



Very High	The consequence requires intervention from **executive management, the Secretary of Transportation, or the Governor**; requires prompt action by the Secretary of Transportation to implement new **Departmental-level controls** to treat the risk.
High	The consequence affects the ability of WSDOT to carry out its mission and strategic plan - **existing controls** must be effective and requires additional action to be managed at the **executive management level**.
Medium	The consequence impacts completion of a critical WSDOT function - **existing controls** must be effective and possibly additional action implemented - action to be managed at **Division level.**
Low	The risk is managed within **current practices and procedures** - impacts are dealt with by **routine operations** at **Director/Office level** - monitor routine practices and procedures for effectiveness.

Figure 15. Matrix. Level of risk.

Source: Risk Management, Risk Assessment Process PowerPoint, Washington State Department of Transportation.

DEVELOP SAFETY DATA ACTION PLAN

The State should develop an action plan that summarizes the gaps, actions, and priorities for addressing the most critical gaps and needs. Table 10 provides an example format for a safety data action plan.

Table 10. Example safety data action plan.

Improvement Area	Gap	Action	Priority
System / Data Collection	**1. Gap** – Description of gap	**1. Action** – Description of solution	High
	2. Gap – Description of gap	**2. Action** – Description of solution	Medium
	…	…	…
Technology	…	…	…
Institutional	…	…	…

DEVELOP ROADMAP FOR IMPLEMENTATION

Finally, States should develop a roadmap for implementation by identifying key steps and priorities for each action in the Action Plan. They should also identify the offices or agencies responsible for each action, as well as the timeframe for implementation. The timeframe may include the short term (six months to one year), medium term (one to three years), or long term (beyond three years). The State should review the schedule and revise as needed to reflect any shifting priorities. Table 11 and Figure 16 show an example roadmap for implementation.

Table 11. Example roadmap for implementation.

Key Steps	Action	Priority	Responsibility	Timeframe
1. Examine and revise agency policies	a. Assign responsibility for implementing the Safety DBP.	High	DOT Transportation Information Group	6 months – 1 year
	b. Budget for implementation of the Safety DBP and dedicate staff resources	Medium	DOT Transportation Information Group	6 months – 1 year
2. Implement Safety Data Governance Process	a. Implement Data Governance Council	High	Data Governance Council	6 months – 1 year
	b. Formally adopt core principles for data and information management and incorporate them into governance policies, standards, and processes	High	Data Governance Council	6 months – 1 year
	c. Implement governance roles and responsibilities	High	Data Governance Council	6 months – 1 year
	d. Institutionalize governance roles and responsibilities by incorporating them into staff job descriptions and job performance review criteria	Medium / High	Data Governance Council	6 months – 1 year
	e. Develop data governance documentation, including a charter, manual, data catalog, and business terms glossary	Medium / High	Data Governance Council	1 – 3 years
	f. Adopt or revise policies (for example, stewardship, data security, database recovery, data retention)	High	Data Governance Council	1 – 3 years
	g. Adopt or revise standards (for example, metadata, naming conventions, data models)	High	Data Governance Council	1 – 3 years

Table 11. Example roadmap for implementation (continuation).

Key Steps	Action	Priority	Responsibility	Timeframe
3. Improve quality of safety data systems	a. Develop and implement crash validation business rules	Medium	State Highway Patrol	6 months – 1 year
	b. Ensure a 5+ year history of crash data is available for all public roadways	High	DOT Transportation Information Group	1-3 years
	c. Work with stakeholders and partners to develop methods for collecting and managing data on roadway features not currently available	Medium	DOT Transportation Information Group	1-3 years
	d. Identify and prioritize roadway inventory data attributes most important to traveler safety for vehicles, bikes, and pedestrians on State and local systems	Medium	DOT Transportation Information Group	1-3 years
	e. Identify opportunities to procure and use innovative technology to supplement current manual data collection methods or to capture data where needed for missing data items	Medium	DOT Transportation Information Group	1-3 years
	f. Develop and implement an automated reporting tool for performance measures established in the Strategic Highway Safety Plan	Medium	DOT Safety Office	1-3 years
	g. Replace legacy crash data system mainframe so it can be a reliable and effective source of crash data	High	DOT Transportation Information Group	3-5 years

Table 11. Example roadmap for implementation (continuation).

Key Steps	Action	Priority	Responsibility	Timeframe
3. Improve quality of safety data systems	h. Work with local law enforcement agencies to implement electronic crash reporting (provide grants for equipment purchase and technical support as needed)	High	State Highway Patrol	3-5 years
	i. Replace the roadway information system mainframe so it can be a reliable and effective source of roadway inventory data	Medium / High	DOT Transportation Information Group	3-5 years
4. Improve Tools for Safety Analysis	a. Develop specifications for exporting data for safety analysis tools	Medium / High	DOT Safety Office	6 months – 1 year
	b. Ensure data stewards and safety prediction experts are involved in critical decisions regarding segmentation criteria and testing of safety analysis results prior to release of safety analysis tool database updates.	High	DOT Safety Office	1-3 years
	c. Expand the use of safety analysis tools for systemwide analysis to identify systematic improvements needed to reduce fatalities and serious injury crashes	Medium	DOT Safety Office	1-3 years
	d. Obtain cross-functional user input to improve tools for safety analysis	Low	DOT Safety Office	1-3 years
	e. Establish feedback mechanisms among users, collectors, and data managers	Low	DOT Safety Office	1-3 years
	f. Develop a complete inventory and safety-project tracking mechanism for all public roads	Low	DOT Maintenance	3-5 years

Table 11. Example roadmap for implementation (continuation).

Key Steps	Action	Priority	Responsibility	Timeframe
5. Improve Data Integration and Collaboration	a. Implement a knowledge management system to increase safety data understanding for DOT staff	Medium	Data Governance Council	1-3 years
	b. Establish a Memorandum of Understanding to formalize data sharing agreements between the DOT and local agencies	Medium	DOT Transportation Information Group	1-3 years
	c. Develop process to geolocate crashes against State LRS for crashes on all public roadways		DOT Transportation Information Group	3-5 years
6. Initiate Training	a. Train staff on safety data policies, procedures, processes, and tools for safety analysis and reporting	Medium	DOT Safety Office	1-3 years
	b. Train external safety stakeholders such as MPOs and local agencies on use of safety data and tools	Medium	DOT Safety Office	1-3 years
	c. Require training of new staff and any staff who retrieve safety data. Create online training that staff can access on-demand. Require testing of concepts and certification of staff upon completion.	Medium	DOT Safety Office	1-3 years

Table 11. Example roadmap for implementation (continuation).

Key Steps	Action	Priority	Responsibility	Timeframe
7. Monitor Progress	a. Track progress in implementing the Safety DBP and governance program.	Medium	Data Governance Council	Ongoing
	b. Establish performance metrics to measure success.	Medium	Data Governance Council	Ongoing
	c. Report on progress to senior management.	Medium	Data Governance Council	Ongoing
	d. Update the Safety DBP to reflect new policies, procedures, or standards regarding data collection methods or equipment	Medium	Data Governance Council	Ongoing

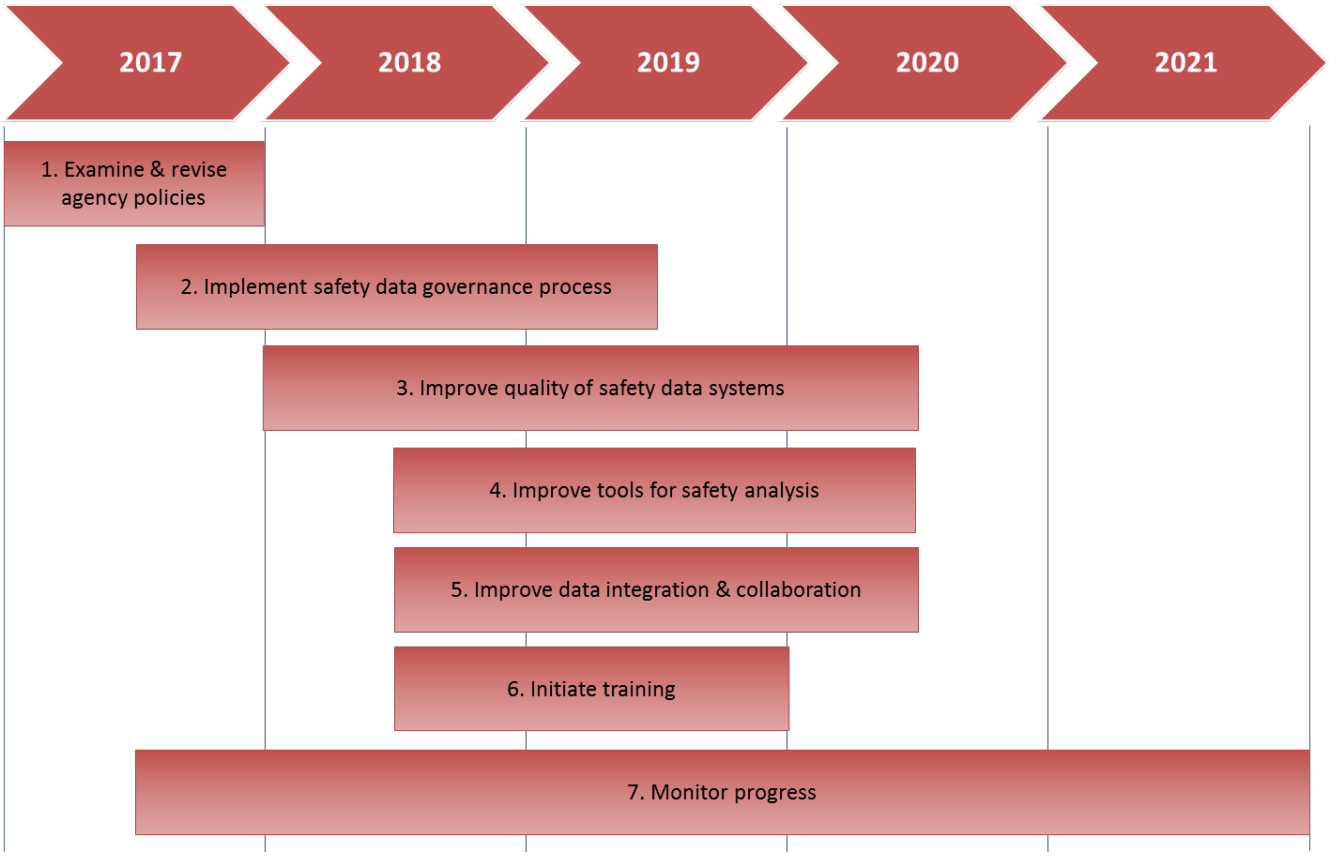


Figure 16. Gantt chart. Implementation roadmap.

SUMMARY

Step 5: Develop Safety Data Action Plan, addresses the need for States to develop a plan for implementing the Safety DBP. The important actions in this step are:

KEY OUTPUTS AND WORK PRODUCTS

- ☐ Summary of system, technology, and institutional gaps
- ☐ Priorities for addressing gaps
- ☐ Safety data action plan
- ☐ Roadmap for implementation

- **Summarize gaps and improvements.** The State should summarize the specific challenges, issues, and gaps identified in previous steps. They should also identify improvements to address the gaps within each area.
- **Identify priorities.** The State should prioritize the list of gaps to identify the most critical gaps and needs. One approach is to consider the risks associated with the gaps and their impact on achieving the State's safety program objectives. Another approach is to assign a priority for filling gaps based on a general assessment of the required investment and resulting value to the agency.
- **Develop safety data action plan.** The State should develop a plan that identifies actions to address the most critical gaps and needs. The plan should list actions for each safety data system in priority order. They should also identify the offices or agencies responsible for each action, as well as the timeframe for implementation.
- **Develop roadmap for implementation.** States should develop a roadmap for implementation by identifying key steps and priorities for each action in the Action Plan. The state should also identify the offices or agencies responsible for each action, as well as the timeframe for implementation.

STEP 6. DOCUMENT THE SAFETY DBP

In Step 6, the State should document the Safety DBP. The key action is to compile the results and documentation from Steps 1 through 5 into a single document. Having all the information in a single document makes it easier to distribute the Safety DBP to internal and external stakeholders.

DOCUMENT THE SAFETY DATA BUSINESS PLAN

The Safety DBP should include the following components:

1. **Introduction –** Document the Safety DBP objectives or outcome statement, and the vision and mission for safety data, as determined in Step 1.

2. **Plan for Safety Data Management and Governance –** Document current challenges in managing and governing safety data, stakeholders for safety data, and the stakeholder outreach process, as determined in Step 1.

3. **Assessment of Current SSDS –** Document business processes for safety data systems, status of current and past assessment recommendations, and overall management and governance capabilities of the agency, as determined in Step 2.

4. **Safety Data Governance Program –** Document core data principles, current and planned governance initiatives within the organization, the governance model describing the organizational structure and framework for governing a State's safety data system, and governance roles and responsibilities, as determined in Steps 1 and 3.

5. **Needs for Safety Tools and Technology –** Document current needs and weaknesses related to technology, as well as strategies for enhancing or replacing technology tools, as determined in Step 4. This section should also identify any high priority data systems in need of enhancement or replacement.

6. **Action Plan –** Document the actions, priorities, responsibilities, and schedule for improving the State's safety data systems, as determined in Step 5. This section should also document performance metrics to measure success, as determined in Step 7.

7. **Appendices –** Supporting documentation such as the data charter, data governance manual, data catalog, and business terms glossary.

SUMMARY

Step 6: Document the Safety DBP, guides States in assembling the Safety DBP. The important actions in this step are:

- **Document the Safety DBP.** The results and documentation from Steps 1 through 5 are compiled into a single document to form the Safety DBP.

KEY OUTPUTS AND WORK PRODUCTS

☐ Safety DBP

STEP 7. IMPLEMENT AND SUSTAIN THE SAFETY DBP

In the final Step, the State should implement and sustain the Safety DBP. Key actions include assigning responsibility, establishing performance metrics, implementing the Safety DBP and Governance Program, conducting training on data governance, and monitoring progress. Leadership and coordination are important for successful implementation. These actions will help the State implement its Governance Program while ensuring institutional support and buy-in at all levels.

ASSIGN RESPONSIBILITY

The State should assign clear responsibilities for monitoring implementation of the Safety DBP and Governance Program. For example, the State may designate a governance champion or small team to guide all activities in the plan initially. This provides a central point of responsibility for tracking progress and building momentum for the program. Once the program is self-sustaining, the Data Governance Board can assume responsibility for sustaining the program.

ESTABLISH PERFORMANCE METRICS

The State should define performance metrics to measure success. While the State's HSIP includes goals for improving safety, the DBP metrics should track how well data systems support the safety program. Performance metrics should reflect the Safety DBP objectives, business needs, and challenges. Table 12 provides example performance metrics. They can also monitor performance through its State Traffic Records Strategic Plan.

Table 12. Example performance metrics.

Example Objectives, Business Needs & Challenges	Example Performance Metric
Understand and promote the value of safety data as a Department-wide asset	Assessment of the value of data as a Department-wide asset conducted among senior management Number of executive briefings
Identify and address safety data gaps	Assessment of gaps in safety data systems based on MIRE FDEs

Table 12. Example performance metrics (continuation).

Example Objectives, Business Needs & Challenges	Example Performance Metric
Improve data quality management processes	Assessment of data quality (timeliness, accuracy, completeness, etc.)
Identify needs and opportunities to integrate safety data systems	Ongoing assessment of data interoperability and integration of safety data systems
Improve access to safety data	Assessment of stakeholder's satisfaction with and ability to access safety data Number of users accessing safety data
Identify and address safety data gaps	Assessment of gaps in safety data systems based on MIRE FDEs
Improve ability to track safety improvements	Development of tools to assess the cost effectiveness of countermeasures using safety data
Implement formal data governance structure	Level of engagement, participation, and influence the Safety Data Governance Council is having Extent to which stakeholder offices are implementing data standards in their data collection and management practices
Improve understanding and knowledge of safety data policies, procedures, processes, and tools for safety analysis and reporting	Development of annual training schedule Conduct scheduled training classes Percentage of employees who have attended training

IMPLEMENT THE SAFETY DBP

The State should implement the Safety DBP by conducting the activities in the Action Plan and Roadmap. It should also formalize the roles and responsibilities for governance as identified in the Safety Data Governance Manual developed in Step 3.

Implementation is not a one-time event, but rather the State should incorporate Safety DBP policies, standards, and procedures into day-to-day business practices. As such, they should continue to engage safety stakeholders beyond initial implementation of the Safety DBP. These individuals help inform and enforce safety data policies, procedures, and standards. They also provide input on development of tools for safety analysis.

Implementation support is available through the FHWA Office of Safety's technical assistance program. More information is available at https://rspcb.safety.fhwa.dot.gov/technical.aspx.

CONDUCT TRAINING

The State should develop and implement a training program to introduce the Safety DBP principles and practices to agency staff, partner agencies, and consultants. Training promotes the Governance Program. It helps stakeholders understand data management and governance processes and their responsibilities within those processes. Training is a critical step in institutionalizing the Governance Program throughout the offices responsible for the SSDS.

The State should train staff on safety data policies, procedures, processes, and tools for safety analysis and reporting. States should also train external safety stakeholders such as MPOs and local agencies as appropriate. Ongoing training is necessary to ensure the consistent use of data and to maintain data integrity over time.

MONITOR PROGRESS

The State should monitor implementation progress by tracking progress on action steps and assessing performance using the metrics defined above. Monitoring progress allows the State to adapt the program to changing priorities, and to capture knowledge and lessons learned from early governance efforts.

Initially, a State should report on progress at monthly meetings of the Data Governance Board. Discussion topics could include progress on action steps (such as tasks completed and tasks remaining) and any schedule impacts due to changes in DOT priorities, policies, standards, or legislative priorities. The State may need to adjust the timeline for implementing some of the recommendations. Once the program has gained momentum, the Board could meet on a semiannual or annual basis.

The TRCC may play a role in implementing some aspects of the Action Plan. Therefore, the State should also report on progress to the TRCC.

The State may need to revise the Safety DBP if there are new policies, procedures, or standards regarding data collection methods or equipment. The State may also need to update the DBP if they have implemented new IT tools or applications.

COMMUNICATE CHANGES

Finally, the State should provide relevant and timely progress updates to senior management and safety data managers and users. Topics for senior management briefings should include a high-level status update, successes achieved, new enhancements needed for existing systems, and recommendations for addressing issues. They should also report on cost savings and other benefits achieved through processes that are more efficient. This allows sufficient opportunity for senior managers to intervene and correct the course of the program, if needed.

States may communicate with safety data managers and users through email updates, a newsletter, or safety data business planning website. Potential topics include information on safety data management standards, processes, members of the Data Governance Board, contact information for key safety data staff, and progress in implementing the governance program. States may also provide a mechanism for users to provide feedback and report on safety data issues.

SUMMARY

Step 7: Implement and Sustain the Safety Data Business Plan, addresses the need for States to implement the Safety DBP and Governance Program. The important actions in this step are:

- **Assign responsibility.** A governance champion or small team should guide initial efforts to implement the Safety DBP and Governance Program. Once the program is self-sustaining, the Data Governance Council can assume responsibility for sustaining the program.
- **Establish performance metrics.** Performance metrics track how well data systems support the safety program. Metrics should reflect the Safety DBP objectives, business needs, and challenges.
- **Implement the Safety Data Business Plan.** The State should implement the Safety DBP by conducting the activities in the Action Plan. It should also formalize the roles and responsibilities for governance as identified in the Governance Program.

KEY OUTPUTS AND WORK PRODUCTS

- ☐ Designation of governance champion or small team to guide implementation
- ☐ Performance metrics for measuring success
- ☐ Implementation of the Safety DBP
- ☐ Training program on data governance
- ☐ Progress updates

- **Conduct training.** Training is a critical step in institutionalizing the Governance Program throughout the offices responsible for the SSDS. Ongoing training is necessary to ensure the consistent use of data and to maintain data integrity over time.

- **Monitor progress.** The State should monitor implementation progress by tracking progress on action steps and assessing performance using the metrics defined in this step. Monitoring progress allows the State to adapt the program to changing priorities, and to capture knowledge and lessons learned from early governance efforts. The State should report on progress at Data Governance Council and TRCC meetings as appropriate.

- **Communicate changes.** The State should report on progress to senior management, including successes achieved, new enhancements needed for existing systems, and recommendations for addressing issues. This allows sufficient opportunity for senior managers to intervene and correct the course of the program, if needed. The State should also communicate with safety data managers and users via a safety data business planning website or other means.

REFERENCES

References used to develop the Guide include the following:

- FHWA Guidance on State Safety Data Systems, March 15, 2016. Available at: http://safety.fhwa.dot.gov/legislationandpolicy/fast/ssds_guidance.cfm .

- Cambridge Systematics, Inc. NCHRP Report 666: Target-Setting Methods and Data Management to Support Performance-Based Resource Allocation by Transportation Agencies, Volume II: Guide for Target-Setting and Data Management, Transportation Research Board, 2010. Available at http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_666.pdf.

- Cambridge Systematics, Inc. NCHRP Report 754: Improving Management of Transportation Information, Transportation Research Board, 2013. Available at http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_754.pdf.

- Minnesota DOT Data Business Plan, 2008. Available at https://www.dot.state.mn.us/tda/databusinessplan.docx.

- Scopatz, R., J. Benac, and N. Lefler. Crash Data Improvement Program (CDIP) Final Report. FHWA-SA-14-001, January 2014. Available at http://safety.fhwa.dot.gov/rsdp/downloads/fhwasa14001cdip_final.pdf.

- Mapping to MMUCC: A Process for Comparing Police Crash Reports and State Crash Databases to the Model Minimum Uniform Crash Criteria. DOT HS 812 184, July 2015. Available at http://www-nrd.nhtsa.dot.gov/Pubs/812184.pdf.

- Cambridge Systematics, Inc. Data Business Plan: Concept of Operations. Prepared for the Alaska Department of Transportation and Public Facilities, September 2005.

- Vanasse Hangen Brustlin, Inc., United States Roadway Safety Data Capabilities Assessment, FHWA-SA-12-028, July 2012. Available at http://safety.fhwa.dot.gov/rsdp/downloads/rsdp_usrsdca_final.pdf.

- Vanasse Hangen Brustlin, Inc (VHB), Roadway Data Improvement Program: Informational Resource, June 2012. Available at http://safety.fhwa.dot.gov/rsdp/downloads/rdip_final061312.pdf.

- NHTSA, Traffic Records Program Assessment Advisory. Available at http://www-nrd.nhtsa.dot.gov/Pubs/811644.pdf.

- Battelle, Cambridge Systematics, Inc., and Texas Transportation Institute. Traffic Data Quality Measurement Final Report. FHWA, September 15, 2004. Available at https://ntl.bts.gov/lib/jpodocs/repts_te/14058.htm.

- NHTSA. Model Performance Measures for State Traffic Records Systems. DOT HS 811 441, February 2011. Available at http://www-nrd.nhtsa.dot.gov/Pubs/811441.pdf.

- DAMA UK Working Group on Data Quality Dimensions. The Six Primary Dimensions for Data Quality Assessment. October 2013.

- FHWA, Crash Data Improvement Program Guide, April 2010. Available at http://safety.fhwa.dot.gov/cdip/finalrpt04122010/finalrpt04122010.pdf.

- Vanasse Hangen Brustlin, Inc., Performance Measures for Roadway Inventory Data, FHWA-SA-12-036, February 2013. Available at http://safety.fhwa.dot.gov/rsdp/downloads/performancemeasures.pdf.

- C. Cabrera, "Data Governance Defined and Why It is Crucial to the Organization," April 15, 2009. http://www.element61.be/e/resourc-detail.asp?ResourceId=6.

- Cambridge Systematics, Inc. Data Governance, Standards, and Knowledge Management. Prepared for the Alaska Department of Transportation and Public Facilities, 2009.

- FHWA Office of Safety, Roadway Safety Data Program website, http://safety.fhwa.dot.gov/rsdp/.

- Vanasse Hangen Brustlin, Inc. United States Roadway Safety Data Capabilities Assessment. FHWA-SA-12-028, July 31, 2012. Available at http://safety.fhwa.dot.gov/rsdp/downloads/rsdp_usrsdca_final.pdf .

- Vanasse Hangen Brustlin, Inc. Model Inventory of Roadway Elements (MIRE), Version 1.0, FHWA-SA-10-018 (October 2010). Available at http://safety.fhwa.dot.gov/tools/data_tools/mirereport/mirereport.pdf.

- Cambridge Systematics, Inc., Safety Data Management Systems and Processes, Literature Review & Synthesis, FHWA-SA-15-061, March 2015.

- Cambridge Systematics, Inc. Safety Data Management Systems and Processes, Case Studies (Draft), May 2015.

- Transportation Research Circular E-C196, Improving Safety Programs Through Data Governance and Data Business Planning, A Peer Exchange, March 3-4, 2015, Washington D.C. Available at: http://onlinepubs.trb.org/onlinepubs/circulars/ec196.pdf.

- AASHTO Subcommittee on Data, Data Subcommittee Efforts on Core Data Principles website, https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnx0cmJkYXRhc2VjdGlvbnxneDoxZDc3YjczNjUxZjIxZmM3.

- Spy Pond Partners, LLC. Data to Support Transportation Agency Business Needs: A Self-Assessment Guide. NCHRP Report 814. Transportation Research Board, Washington, D.C., 2015. Available at: http://www.trb.org/Main/Blurbs/173470.aspx.

- Cambridge Systematics, Inc. Highway Enterprise System and Asset Management Analysis Assistance for the MassDOT Highway Division project, 2014.

- FHWA Data Integration Primer. Publication FHWA-IF-10-019, Federal Highway Administration, Washington, D.C., August 2010. Available online at: https://www.fhwa.dot.gov/asset/dataintegration/if10019/if10019.pdf.

- Scopatz, R., E. Goughnour, D. Abbott, E. Tang, D. Carter, S. Smith, and T. Salzer. Informational Guide for State, Tribal, and Local Safety Data Integration. Publication FHWA-SA-16-118, Federal Highway Administration, Washington, D.C., October 2016. Available online at: https://safety.fhwa.dot.gov/rsdp/downloads/fhwasa16118.pdf.

- Cambridge Systematics. Inc. U.S. DOT Roadway Transportation Data Business Plan (Phase 3): Data Business Plan Development for State and Local Departments of Transportation, May 2017. (Draft).

- The DAMA Dictionary of Data Management, the Data Management Association (DAMA), 2nd Edition, 2011.

- Lefler, N., F. Council, D. Harkey, D. Carter, H. McGee, and M. Daul. Model Inventory of Roadway Elements–MIRE, Version 1.0, Report No. FHWA-SA-10-018, October 2010. Available online at: https://safety.fhwa.dot.gov/tools/data_tools/mirereport/mirereport.pdf.

APPENDIX A. SAFETY DATA ELEMENTS

Table A.1. Summary of Model Inventory of Roadway Elements Fundamental Data Elements.

Model Inventory of Roadway Elements Fundamental Data Elements (Model Inventory of Roadway Elements Number) (The number in parentheses ( ) identifies the data element number in MIRE Version 1.0.)	Applicable Roadway Network		
	Non-Local Paved Roads	Local Paved Roads	Unpaved Roads
Roadway Segment			
Segment Identifier (12)	Yes	Yes	Yes
Route Number (8) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		
Route/Street Name (9) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		
Federal Aid/Route Type (21) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		

Source: Model Inventory of Roadway Elements–MIRE, Version 1.0, Report No. FHWA-SA-10-018, October 2010, https://safety.fhwa.dot.gov/tools/data_tools/mirereport/mirereport.pdf.

Table A.1. Summary of Model Inventory of Roadway Elements Fundamental Data Elements (continuation).

Model Inventory of Roadway Elements Fundamental Data Elements (Model Inventory of Roadway Elements Number) (The number in parentheses ( ) identifies the data element number in MIRE Version 1.0.)	Applicable Roadway Network		
	Non-Local Paved Roads	Local Paved Roads	Unpaved Roads
Rural/Urban Designation (20) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes	Yes	
Surface Type (23) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes	Yes	
Begin Point Segment Descriptor (10) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).	Yes	Yes	Yes
End Point Segment Descriptor (11) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes	Yes	Yes

Source: Model Inventory of Roadway Elements–MIRE, Version 1.0, Report No. FHWA-SA-10-018, October 2010, https://safety.fhwa.dot.gov/tools/data_tools/mirereport/mirereport.pdf.

Table A.1. Summary of Model Inventory of Roadway Elements Fundamental Data Elements (continuation).

Model Inventory of Roadway Elements Fundamental Data Elements (Model Inventory of Roadway Elements Number) (The number in parentheses ( ) identifies the data element number in MIRE Version 1.0.)	Applicable Roadway Network		
	Non-Local Paved Roads	Local Paved Roads	Unpaved Roads
Segment Length (13) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		
Direction of Inventory (18)	Yes		
Functional Class (19) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes	Yes	Yes
Median Type (54)	Yes		
Access Control (22) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		
One/Two-Way Operations (91) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		

Source: Model Inventory of Roadway Elements–MIRE, Version 1.0, Report No. FHWA-SA-10-018, October 2010, https://safety.fhwa.dot.gov/tools/data_tools/mirereport/mirereport.pdf.

Table A.1. Summary of Model Inventory of Roadway Elements Fundamental Data Elements (continuation).

Model Inventory of Roadway Elements Fundamental Data Elements (Model Inventory of Roadway Elements Number) (The number in parentheses ( ) identifies the data element number in MIRE Version 1.0.)	Applicable Roadway Network		
	Non-Local Paved Roads	Local Paved Roads	Unpaved Roads
Number of Through Lanes (31) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes	Yes	
Average Annual Daily Traffic (79) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes	Yes	
AADT Year (80) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		
Type of Governmental Ownership (4) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes	Yes	Yes

Source: Model Inventory of Roadway Elements–MIRE, Version 1.0, Report No. FHWA-SA-10-018, October 2010, https://safety.fhwa.dot.gov/tools/data_tools/mirereport/mirereport.pdf.

Table A.1. Summary of Model Inventory of Roadway Elements Fundamental Data Elements (continuation).

Model Inventory of Roadway Elements Fundamental Data Elements (Model Inventory of Roadway Elements Number) (The number in parentheses ( ) identifies the data element number in MIRE Version 1.0.)	Applicable Roadway Network		
	Non-Local Paved Roads	Local Paved Roads	Unpaved Roads
Intersection			
Unique Junction Identifier (120)	Yes		
Location Identifier for Road 1 Crossing Point (122)	Yes		
Location Identifier for Road 2 Crossing Point (123)	Yes		
Intersection/Junction Geometry (126)	Yes		
Intersection/Junction Traffic Control (131)	Yes		
AADT (79) [for Each Intersecting Road]	Yes		
AADT Year (80) [for Each Intersecting Road]	Yes		
Unique Approach Identifier (139)	Yes		
Interchange/Ramp			
Unique Interchange Identifier (178)	Yes		
Location Identifier for Roadway at Beginning Ramp Terminal (197)	Yes		
Location Identifier for Roadway at Ending Ramp Terminal (201)	Yes		
Ramp Length (187)	Yes		
Roadway Type at Beginning Ramp Terminal (195)	Yes		
Roadway Type at Ending Ramp Terminal (199)	Yes		

Source: Model Inventory of Roadway Elements–MIRE, Version 1.0, Report No. FHWA-SA-10-018, October 2010, https://safety.fhwa.dot.gov/tools/data_tools/mirereport/mirereport.pdf.

Table A.1. Summary of Model Inventory of Roadway Elements Fundamental Data Elements (continuation).

Model Inventory of Roadway Elements Fundamental Data Elements (Model Inventory of Roadway Elements Number) (The number in parentheses ( ) identifies the data element number in MIRE Version 1.0.)	Applicable Roadway Network		
	Non-Local Paved Roads	Local Paved Roads	Unpaved Roads
Interchange Type (182)	Yes		
Ramp AADT (191) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		
Year of Ramp AADT (192) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		
Functional Class (19) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		
Type of Governmental Ownership (4) (Highway Performance Monitoring System full extent elements are required on all Federal-aid highways and ramps located within grade-separated interchanges (that is, National Highway System (NHS) and all functional systems excluding local roads and rural minor collectors).)	Yes		

Source: Model Inventory of Roadway Elements–MIRE, Version 1.0, Report No. FHWA-SA-10-018, October 2010, https://safety.fhwa.dot.gov/tools/data_tools/mirereport/mirereport.pdf.

APPENDIX B. SUMMARY OF CASE STUDIES

MICHIGAN DOT SAFETY DATA PROCESSES AND GOVERNANCE PRACTICES, CASE STUDY FHWA-SA-15-059

Summary

Michigan DOT incorporates data governance into their standard business operations to improve their safety data systems and processes. This case study examines Michigan DOT's data governance practices from a policy and technical perspective.

Policy. Michigan DOT began implementing data management policies as part of their asset management program in the 1990s. These policies emphasize the value of data as an asset, with a goal to establish methods to collect data once for multiple uses. These practices have eliminated duplicate data collection, which has reduced costs associated with maintaining the same data in multiple data systems.

The DOT has a top-down data governance structure established by the State of Michigan Governor's office via an Executive Directive in 2013. In response, Michigan DOT established:

- A Data Governance Council, whose purpose is to establish policies for data governance and develop data dictionaries and metadata for all major systems and data sources. Membership includes representation from major business process areas and the IT Department;
- The role of Chief Data Steward, whose purpose is to implement data management within the Department and chair the Data Governance Council; and
- Data stewards, who are ultimately responsible for establishing and using business rules that govern data in each business area, including safety data systems.

Michigan DOT's current focus is on improving its data management practices, including developing data dictionaries and metadata. The DOT is migrating its capital programming and asset management definitions and metadata into a single tool maintained by IT staff. Once migrated, the DOT will expand data stewardship roles to include systems not previously governed. Many of these are safety data systems or data programs that support safety.

Technical. From a technical perspective, Michigan DOT is using tools supported by a centralized IT Department, including:

- An integrated Linear Reference System to maintain location data;

- AASHTOWare Safety Analyst™, the Highway Safety Manual, and GIS tools to support safety analysis.
- A work-order based maintenance system to maintain data on roadway safety features.

Applicability to Other States

Other States may develop and implement similar data governance practices for their safety programs as follows:

- Establish a Data Governance Council to oversee data management practices, policies, and procedures;
- Define data stewardship roles and responsibilities for governing data in each business area;
- Develop a data dictionary to help IT staff understand how commonly used terms (for example, location data) are used within individual business units;
- Involve the data stewards in the review of bids and purchases related to IT, software, and data management that support the applications managed by those stewards;
- Include the IT Department at all levels;
- Update job descriptions and classifications to include the roles of data stewardship and relate this concept to performance plans or job duties;
- Implement data governance using tools that are available and easy to understand; and
- Highway safety is a great starting point to implement data governance initiatives, since there is widespread interest in improving safety.

Link

https://safety.fhwa.dot.gov/rsdp/downloads/miDOT_casestudy_dm_final.pdf.

NEW HAMPSHIRE DOT SAFETY DATA SYSTEMS AND PROCESSES, CASE STUDY FHWA-SA-15-058

Summary

This case study examines how New Hampshire DOT has leveraged technology to support safety data management. NHDOT has invested in analytical, integration, and data sharing tools:

Analytical Tools. NHDOT uses the Highway Safety Manual, AASHTOWare Safety Analyst™, the Interactive Highway Safety Design Model, and safety analysis spreadsheets to support safety analysis. Implementation and usage of these tools necessitated a review of data elements to determine gaps. They also used their safety datasets to calibrate the safety performance functions in Safety Analyst™ to local conditions. These processes required collaboration between the safety group and IT and demonstrated the need for institutionalizing methods outlined in the Highway Safety Manual.

Integration Tools. NHDOT uses an integrated LRS that provides a common link between safety data sets, including crash, traffic, and road inventory data. Their use of GIS applications helps to improve overall data quality by providing a method for visualization of data on maps and identification of data errors for correction, prior to their use with analytical tools.

Data Sharing Tools. Investments in data sharing technology are critical for sustaining and enhancing NHDOT's safety program. Data sharing maximizes the potential to locate and correct errors reported by data users, which ultimately leads to improved data quality. Data sharing methods include providing quarterly snapshots of GIS data to regional planning agencies, providing GIS data to an online statewide GIS data warehouse, and providing GIS web maps online. NHDOT is also working on an initiative to share crash data with the New Hampshire Department of Safety within a relational database environment.

Applicability to Other States

Other States may learn from NHDOT's experiences in leveraging technology to improve develop their safety programs as follows:

- State DOT business areas, including safety program managers, should partner with IT offices to understand technology available to support business operations;
- Safety Office staff should have a basic understanding of (or work with people who do) how IT products can improve access to, integration of, and sharing of safety data;

- Think long-term about how technology fits into an overall safety data management and governance strategy. Technology that provides integration and sharing of data across business areas is critical for meeting the needs of the safety program;
- Ensure analytical tools support the needs of the safety program;
- Prioritize data collection efforts to focus on required data elements rather than optional data elements;
- Use a common LRS as the foundation for safety data integration and analysis; and
- Coordinate data collection efforts with other agencies (including local) to expand data available for safety analysis.

Link

https://safety.fhwa.dot.gov/rsdp/downloads/nh_case_study.pdf.

UTAH DOT SAFETY DATA PROCESSES AND GOVERNANCE PRACTICES, CASE STUDY FHWA-SA-15-060

Summary

This case study examines Utah DOT's use of innovative technology to support safety data management and analysis. In addition to highlighting forward-thinking strategies for safety data management, data analysis, and reporting, the case study documents the need for a formal data business plan and data governance.

Data Collection. UDOT's data collection program is coordinated among multiple business areas to meet as many needs as possible. This includes incorporating advanced imagery (hi-resolution photo and LiDAR), data extraction of specified inventory, and pavement data imaging and tools for analysis. This innovative approach has vastly improved procedures for managing assets and roadway inventory.

Data Management. UDOT manages and shares data in a centralized data system that supports many tools and applications for planning, safety data analysis, target setting, and performance management. They consolidate all of their data (including those that support safety) in a centralized data portal called UGate. Data in UGate is integrated, downloadable, and accessible. Most information is available to the public. At UDOT, data is available for viewing and analysis using web-based applications and online maps. Data is also available for download in various formats. UGate supports many data-driven tools used by traffic and safety engineers for project prioritization, planning, analysis, and reporting.

Data Governance. Currently, there is no formal data business plan for safety or enterprise data. However, the expansion of technology has made data governance and data business planning a high priority need for the Department. UDOT is in the process of organizing a data governance board to review technology expenditures, stewardship roles, and other data governance matters.

Interagency Partnerships and Collaboration. UDOT uses an external department for technology delivery to handle technical details such as data item definitions and physical database locations, storage, and structures. Although the service comes at a cost, UDOT found it is helpful to have IT professionals handle the system architecture and database functionality so UDOT staff can focus on improving data collection and analysis capabilities to support program areas.

Safety Data Analysis Tools. UDOT utilizes multiple tools to support safety analysis, planning, and decision-making

- **UPlan.** UPlan is a web-based decision support, mapping, and informational tool to support complex planning and project development tasks. In the UPlan Portal for Zero Fatalities,

UDOT links safety data to performance measures. Roadway segments link to statistics such as severe crash rate, crash rate per mile, and safety ratings.

- **Linear Bench.** Linear Bench is a tool used to view and analyze data internally. UDOT staff can select a roadway segment and data sets to generate a straight-line diagram, tabular report, or map display with the selected characteristics. The tool allows users to view multiple data sets to support detailed analysis, decision-making, and reporting needs. For example, a user can view crash scores, traffic volume, and pavement data together and assess the need for a site visit to check pavement surface condition.

- **Report Auto Generator.** This tool allows users to generate a bid estimate for roadway improvements (for example, guardrail, overlay or mill and fill, or pavement repair) based on roadway segment data. The tool allows users to notify other interested parties (internal or external to the Department) regarding the project. This reduces overlap and allows for coordination of work efforts.

- **Crash Data Analysis Tool.** This tool allows users to combine crash location, damage value estimates, and asset inventory data to identify the need for safety improvements. The tool is currently in spreadsheet format, but there are plans to transition to an online dashboard to support both user-defined and network level analysis.

Applicability to Other States

Other States may benefit from the following lessons learned:

- Collect data once for use by many groups;

- Involve all interested parties in data management and make sure the right people are involved in decision-making;

- Develop central applications to share/distribute data;

- Consolidate tools, reports, and data in central locations and ensure they meet as many needs as possible; and

- Track and share cost savings achieved (or the return on investment) through more efficient processes.

Link

https://safety.fhwa.dot.gov/rsdp/downloads/utah_case_studyFinal.pdf.

APPENDIX C. SUMMARY OF PILOT STUDIES

KANSAS DOT DATA BUSINESS PLAN EXECUTIVE SUMMARY

The Kansas Department of Transportation (KDOT) is responsible for building and maintaining a modern, safe, and sustainable transportation network for all Kansans. KDOT and its partners maintain a broad range of safety data systems and work together closely to promote and strive for safer transportation in the State. However, the Department needs to improve its data resources, data management, and governance practices to integrate safety data and make it available to all State practitioners. To address these concerns, KDOT developed a Safety Data Business Plan (DBP) to guide its safety data management practices.

Objectives

- Develop a governance framework to better manage safety data resources and assets
- Develop a roadmap for improving safety data resources
- Create a communication and implementation plan

"Safety Data" in this DBP refers to crash, roadway inventory, and traffic volume data on public roadway and includes, in the case of a railway-highway grade crossing, the characteristics of highway and train traffic, licensing, and vehicle data. The DBP also includes ancillary data systems that support safety analysis.

- **Vision:** The Kansas DOT and its safety data stakeholders will have a sound, comprehensive, and well-coordinated approach to managing, improving, and applying the State's safety data and analysis resources.
- **Mission:** The Kansas DOT's mission with respect to safety data management is to achieve sound governance of safety data resources, enhance integration of safety data systems, continually improve the quality and usability of data, and promote user friendly and easily accessible by our safety users and partners for their business analysis.

KDOT developed the DBP through participation in the FHWA Safety Data Management and Governance Processes project. KDOT pilot tested the *Guide for State DOT Safety Data Business Planning*, which provides a seven-step approach to assist States in developing and implementing a Safety DBP. The following steps provide an overview of KDOT's Safety DBP based on the FHWA guide.

Step 1
Plan for Safety Data Management/Governance

Through discussions with its safety data stakeholders, KDOT identified several system, technical, and institutional challenges and issues to address in its Safety DBP. A stakeholder engagement plan identifies the stakeholders involved in each step of the DBP, the purpose of engaging stakeholders within that step, engagement mechanisms, and timeframe for engagement. KDOT also developed a vision, mission, and outcome statement for safety data management.

Step 2
Assess Current State of Safety Data Program

In this step, KDOT identified existing data systems in place for collecting, managing, storing, and reporting safety data; identified business processes associated with safety data systems; summarized current and past assessment efforts; and assessed their current capabilities related to safety data collection, analysis, governance, and interoperability.

Step 3
Establish a Safety Data Governance Program

In this step, KDOT established core data principles; documented current and planned governance initiatives; developed a Governance Model; and defined governance roles and responsibilities. **Figure C-1** depicts a formal structure for KDOT to govern its safety data system. The governance model depicts the relationship between safety data programs, the various individuals responsible for implementing data governance, and the stakeholders for the data programs.

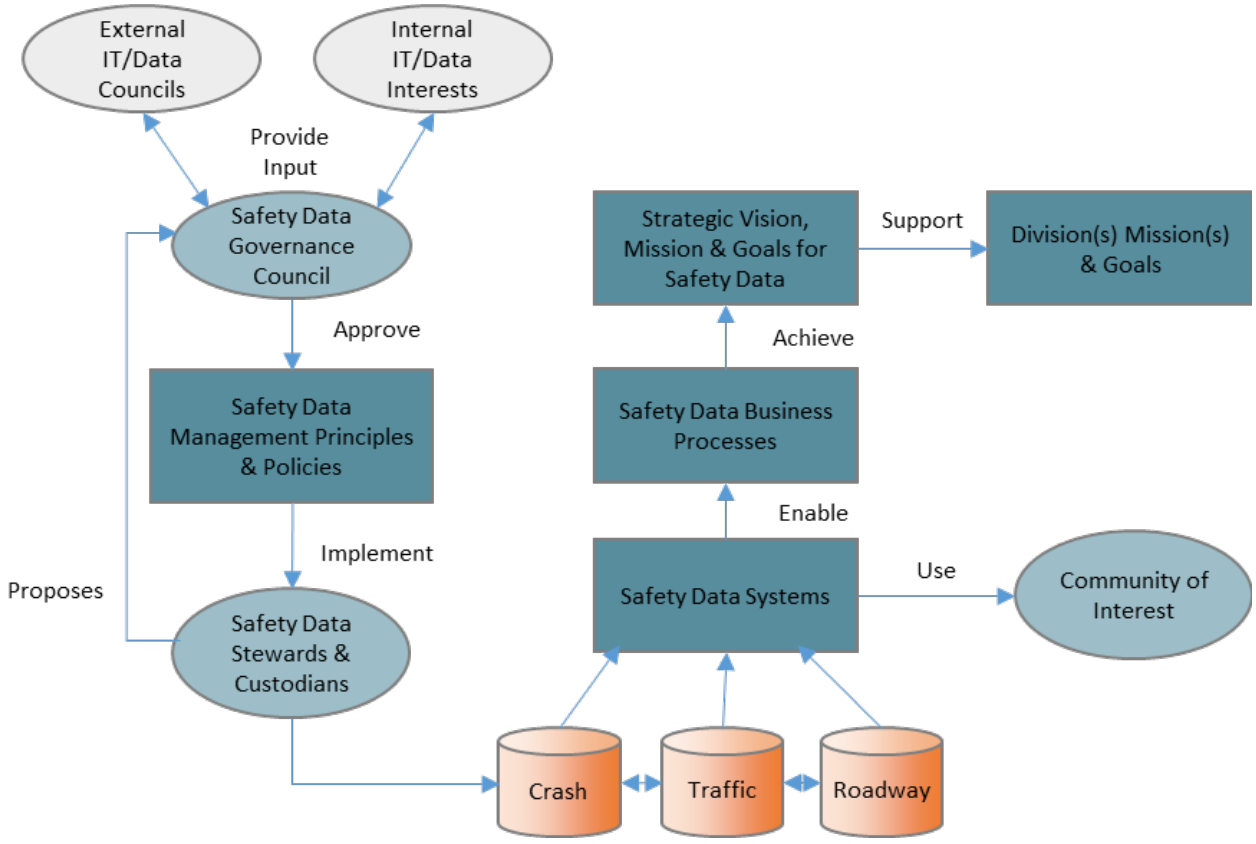


Figure C-1. Diagram. Kansas Department of Transportation Safety Data Governance Model.

Step 4
Develop Tools and Technology for Safety Data Management

In this step, KDOT identified technology needs and developed a plan for improved use of tools. Recommendations are categorized into the following categories – data collection, data tools, knowledge management, system improvements, training, and cost management. KDOT is implementing many of the recommendations through the K-HUB and Crash Data Portal initiatives.

Step 5
Develop an Action Plan

This step provides an action plan for improving KDOT's safety data based on the challenges, issues, and gaps identified in previous steps. Recommendations are organized into the following improvement categories:

- **System:** Recommendations related to data systems, data collection, data access, data integration, data quality, data storage, and documentation;

- **Technology:** Recommendations related to software, hardware, system interfaces, IT compatibility, business intelligence tools, analytical tools, knowledge management, and network issues; and
- **Institutional:** Recommendations related to data management and governance, business rules and processes, coordination across business areas, IT support, resource availability, and training needs.

KDOT obtained stakeholder input to prioritize the recommendations.

Step 6
Develop an Implementation Plan

Successful implementation of the Safety DBP will require continued work and dedication of resources over the next few years, as well as a cultural shift in how safety data assets are managed in the Department. KDOT should designate a governance champion or small team to oversee the recommendations in the action plan and lead initial safety data governance efforts. Once the governance program is self-sustaining, responsibility should transition to the Safety Data Governance Council. A roadmap for implementation is depicted in **Figure C-2**.

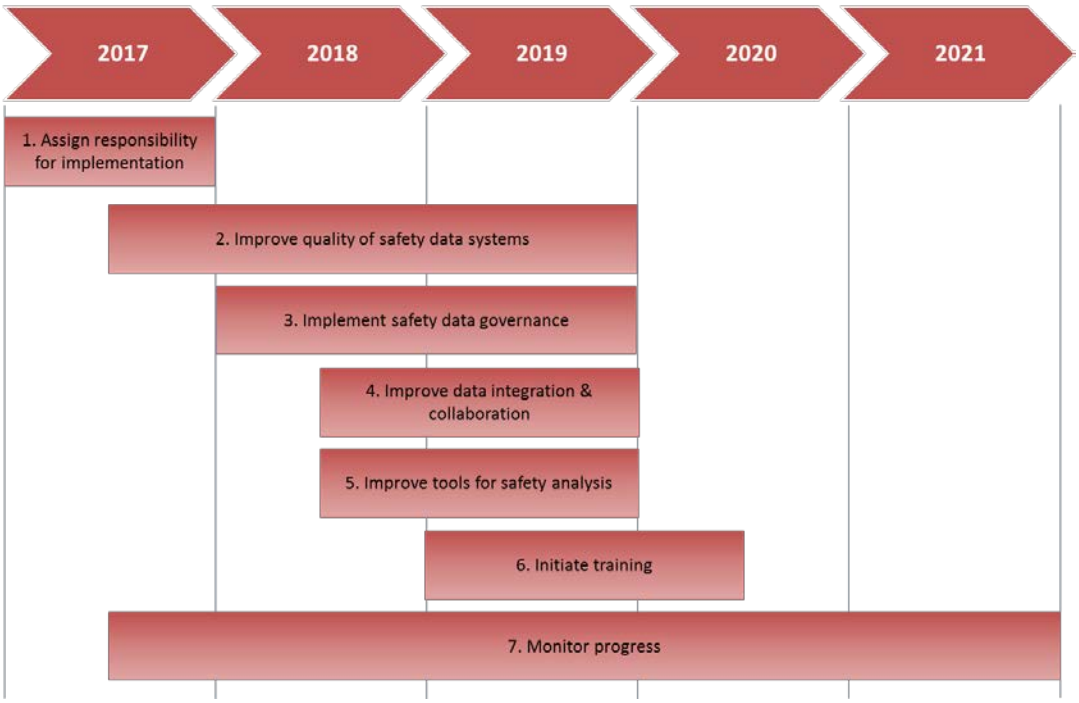


Figure C-2. Gantt chart. Implementation roadmap.

WASHINGTON STATE DATA BUSINESS PLAN EXECUTIVE SUMMARY

Washington State Department of Transportation (WSDOT) is the steward of a multimodal transportation system and is responsible for ensuring people and goods move safely and efficiently. Washington's State Strategic Highway Safety Plan: Target Zero, sets a zero goal for fatalities and serious injuries by 2030. WSDOT's 2014-2017 Strategic Plan also includes a goal to reduce the number of fatal and serious injuries for all transportation modes. Meeting this goal requires the ability to assemble and analyze safety data. WSDOT maintains safety data systems for these activities. However, the Department needs to improve its data management and governance practices to integrate data and make it available to all State practitioners. To address these concerns, WSDOT developed a Safety Data Business Plan (DBP) to guide its safety data management practices.

Objectives

- Demonstrate how safety data impact the enterprise
- Develop a roadmap to address safety data linkage, association, and management challenges
- Establish a strong, sustainable vision for safety data
- Implement a formal safety data governance process
- Ensure a sustainable safety data improvement process

- **Vision:** WSDOT's business decisions will be supported by reliable, timely, accessible, integrated, and complete safety data.
- **Mission:** WSDOT will manage and maintain integrated safety data systems that are user friendly and easily accessible (as appropriate) by our safety users and partners for their business analysis.

WSDOT developed this DBP through participation in the FHWA Safety Data Management and Governance Processes project. WSDOT pilot tested the *Guide for State DOT Safety Data Business Planning*, which provides a seven-step approach to assist States in developing and implementing a Safety DBP. The following steps provide an overview of WSDOT's Safety DBP based on the FHWA Guide.

Step 1
Plan for Safety Data Management and Governance

Through discussions with its safety data stakeholders, WSDOT identified several system, technical, and institutional challenges and issues to address in its Safety DBP. Stakeholders cited institutional challenges as the number one risk to WSDOT. A stakeholder engagement plan identifies the stakeholders involved in each step of the DBP, the purpose of engaging the stakeholders within that step, engagement mechanisms, and timeframe for engagement. WSDOT also developed a vision, mission, and outcome statement for safety data management.

Step 2
Assess Current State of Safety Data Program

In this step, WSDOT identified existing data systems in place for collecting, managing, storing, and reporting safety data; summarized current and past assessment efforts; and assessed their current capabilities in safety data collection, analysis, governance, and interoperability.

Step 3
Establish a Safety Data Governance Program

In this step, WSDOT identified core data principles; documented current and planned governance initiatives; developed a Governance Model; and defined governance roles and responsibilities. **Figure C-3** depicts a formal structure for WSDOT to govern its safety data system. The governance model depicts the relationship between safety data programs, the various individuals responsible for implementing data governance, and the stakeholders for the data programs.

Step 4
Develop Tools and Technology for Safety Data Management

In this step, WSDOT identified technology needs and developed a plan for improved use of tools. Recommendations are categorized into the following categories – data collection technology, data tools, database design, knowledge management, system improvements, training, and cost management.

Step 5
Develop an Action Plan

This step provides an action plan for improving WSDOT's safety data based on the challenges, issues, and gaps identified in previous steps. Recommendations are organized into the following improvement categories:

- **System:** Recommendations related to data systems, data collection, data access, data integration, data quality, data storage, and documentation;
- **Technology:** Recommendations related to software, hardware, system interfaces, IT compatibility, business intelligence tools, analytical tools, knowledge management, and network issues; and
- **Institutional:** Recommendations related to data management and governance, business rules and processes, coordination across business areas, IT support, resource availability, and training needs.

WSDOT prioritized the recommendations based on the results of a Risk Management Assessment.

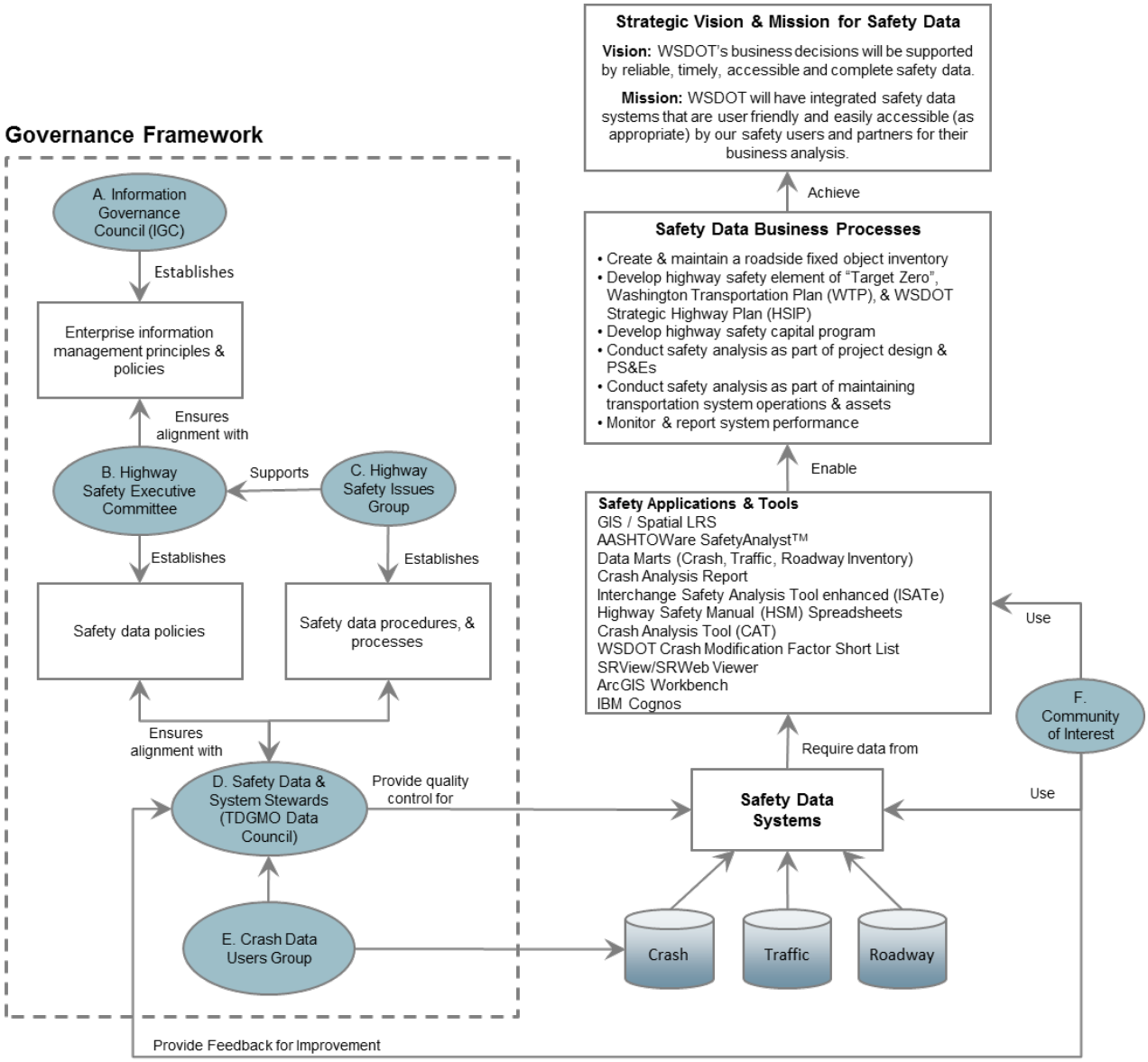


Figure C-3. Diagram. WSDOT safety data governance model.

Step 6
Develop an Implementation Plan

Successful implementation of the Safety DBP will require continued work and dedication of resources over the next few years, as well as a cultural shift in how safety data assets are managed in the Department. The Highway Safety Executive Committee and Highway Safety Issues Group should assume responsibility for overseeing the recommendations in the Action Plan and leading initial safety data governance efforts. Once the enterprise governance program is self-sustaining, responsibility should transition to the Information Governance Council. A roadmap for implementation is depicted in **Figure C-4**.

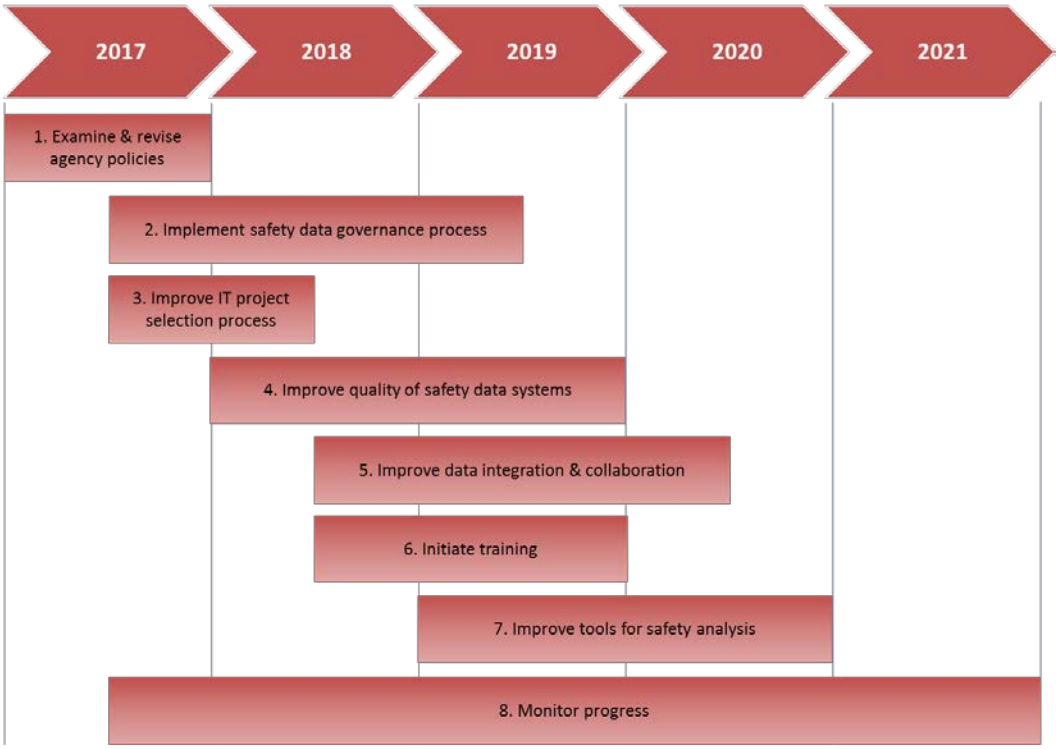


Figure C-4. Gantt chart. Implementation roadmap.

APPENDIX D. EXAMPLE SURVEY INSTRUMENT ON SAFETY DATA CHALLENGES

Who to Survey: State DOT Safety Data Managers, Safety Data Providers, Safety Data System Owners, Safety Data Users

Purpose: **<AGENCY NAME>** is conducting a safety data business planning initiative to improve the management and governance of our safety data, which, for the purposes of this project, is defined as crash, traffic volume, roadway feature inventory, or other transportation/safety related location data. An initial step is to gather more information on current challenges the DOT is facing with regard to the management, governance, and use of safety data by stakeholders. To assist us in the process, please respond to the survey below by **<DATE>**. We appreciate your assistance.

Survey Questions (using Survey Monkey or similar online tool)

1. Please identify the organization or DOT division under which you are employed, and what your title is.
    a. Organization: <text box>
    b. Title: <text box>
2. Do you directly collect, develop, or maintain any safety data for which your organization or division is responsible? For the purposes of this study, safety data is defined as crash, traffic volume, roadway feature inventory, or other transportation/safety related location data.
    a. Yes (if yes, survey will continue to Q3)
    b. No (if no, survey will continue to Q13)

Questions for Data Owners and Stewards:

3. Please list the safety data for which you are responsible. (select all that apply)
    a. Traffic volume data
    b. Crash data
    c. Roadway features inventory data
    d. Linear referencing data
    e. Other (please specify)

4. Where is this data stored? (select all that apply)
    a. On individual desktop computers
    b. As hard copy maps or drawings
    c. In a centralized, enterprise database management system such as Oracle or Microsoft SQL server
    d. Within a specialized software application
    e. Other (please specify)
5. How frequently are the data records updated? Please list your data items in the appropriate box.
    a. Updated continuously <Text box>
    b. Updated yearly <Text box>
    c. Updated monthly <Text box>
    d. Updated weekly <Text box>
    e. Updated daily <Text box>
    f. Updated as needed <Text box>
6. Are the databases shared with, or available for use by: (Select all that apply)
    a. Other divisions or organization units within the DOT?
    b. Other agencies outside of the DOT?
    c. General public?

    If yes, in what format are the databases shared with other entities?

    d. Copies of the raw database
    e. Summary tabulations
    f. Periodic reports
    g. Other (please specify)
7. Do the majority of users know how to properly query and perform analysis with your safety data? If not, why do users face challenges accessing and/or using your data? (Examples: Yes, a data dictionary is provided with our data so that users will understand

what exactly the data represents and how to use it. No, our data has a lot of codes and information that only those that generate the data know about.)

   a. <Text box>

8. What current challenges do you and/or other data users face in merging the safety data you manage with other data?

   a. Lack of geographical coordinates

   b. Differing segment/location identification

   c. Different data formats

   d. Varying temporal resolution

   e. Other (please specify)

9. Which of the following types of improvements would you like to see for the DOT's safety data systems? Please rank them in priority order, with one being the most important and four being the least important.

   a. A "one stop shop" for all data at the Department instead of data storage on multiple network connections.

   b. A web based system where users can search, view, and query up-to-date data.

   c. Data about the data. Data dictionaries or "how to use this data" directions associated with all data.

   d. Other (please specify)

10. Do you receive requests from users for additional data elements needed for safety analysis that are not currently being collected? Is so, what types, and how often/important are the requests?

   a. Yes (please specify)

   b. No

11. Are your data management responsibilities formalized and documented as part of your job description or office standard operating procedures?

   a. Yes

   b. No

c. Not sure

12. Which of the following types of additional resources would be helpful for managing and maintaining your safety data? Please rank them in priority order, with one being the most helpful and seven being the least helpful.

    a. Staffing

    b. Funding

    c. Training

    d. Data dictionaries

    e. Guidance

    f. Software/tools

    g. Other (please specify)

Questions for Data Users

13. Do you require or regularly use safety data maintained by another organizational unit or outside agencies?

    a. Yes (If yes, survey will continue to Q14)

    b. No (If no, survey will continue to Q24)

14. Please list the safety data that you use on a regular basis. (Select all that apply)

    a. Traffic volume data

    b. Crash data

    c. Roadway features inventory data

    d. Linear referencing data

    e. Other (please specify)

15. For what are these data being used? (select all that apply)

    a. Identify safety needs and recommend safety improvements

    b. Evaluate the effectiveness of implemented improvements

    c. Track mandated performance measures

d. Conduct strategic planning to support development of the Strategic Highway Safety Plan or HSIP

e. Develop safety-related maps, documents, or publications

f. Other (please specify)

16. In what format are the data obtained? (select all that apply)

    a. Direct access to a shared database

    b. Copies of the database

    c. Summary reports

    d. Other (please specify)

17. How frequently do you obtain updates of the data?

    a. Updates obtained continuously

    b. Updates obtained yearly

    c. Updates obtained monthly

    d. Updates obtained weekly

    e. Updates obtained daily

    f. Updates obtained as needed

18. Please describe any issues or difficulties you have in obtaining or using the data. (Examples: cumbersome data request procedures, data quality issues, restrictions on use, data is always located in a different place when I need to use it again, there is no one to tell me how to get to it or use it, sometimes the data is named differently than when I used it before)

    a. <Text box>

19. Do you have a need for additional safety data elements that are not currently being collected? Is so, what types and for what purpose?

    a. <Text box>

20. How easy or difficult is it to merge safety data with other data needed to conduct safety analysis or perform your job functions?

    a. Very easily, the data are provided in the same format as our data.

b. Easily, the data are provided in a format that can be easily transformed to be in the same format as our data.

c. Moderately, the data require some manual labor to get them into a usable format.

d. Difficult, the data require extensive manual labor to get them into a usable format.

e. Not at all, the data are unusable in the current format they are submitted in and cannot be transformed into a usable format.

f. Other (please specify)

g. Does not apply

21. What software or tools do you use to conduct safety analysis? (select all that apply)

a. Advanced safety analysis tools such as AASHTOWare Safety Analyst™

b. Highway Safety Manual spreadsheets

c. GIS Systems

d. Statistical Analysis Software (SAS)

e. Microsoft Excel

f. Microsoft Access

g. Other (please specify)

h. Does not apply

22. Are you able to achieve consistency in analysis methods and results?

a. Yes

b. No

c. Sometimes

d. Does not apply

23. Which of the following types of additional support would be helpful for conducting safety analysis as part of your job function? Please rank them in priority order, with one being the most helpful and seven being the least helpful.

a. Funding

b. Training

c. Data dictionaries

d. Format requirements

e. Guidance

f. Software/tools

g. Other (please specify)

Concluding questions (all respondents)

24. Please provide your contact information for follow-up if we have questions regarding your response.

    a. Name: <Text box>

    b. Email: <Text box>

    c. Phone: <Text box>

APPENDIX E. EXAMPLE SURVEY INSTRUMENT ON GOVERNANCE INITIATIVES

Who to Survey: Managers (or designated representatives) from other DOT business offices or divisions

Purpose: **<AGENCY / DIVISION NAME>** is conducting safety data business planning initiative to improve the management and governance of our safety data, which, for the purposes of this project, is defined as crash, traffic volume, roadway feature inventory, or other transportation/safety related location data. The data business plan will describe our vision, goals, objectives, and actions related to improving the way we manage safety data within the agency.

An initial step is to gather more information on data management or governance initiatives underway in other business areas within the DOT. To assist us in the process, please respond to the survey below by **<DATE>**. We appreciate your assistance.

Survey Questions (using Survey Monkey or similar online tool)

1. Please identify the DOT division or office under which you are employed, and your job title.
    a. Name: <text box>
    b. Division/Office: <text box>
    c. Title: <text box>
2. Does your office own, develop, or maintain any data systems or databases? If yes, please identify the names of the data systems or databases.
    a. Yes (please explain) <Text box> <If yes, survey continues to Q3>
    b. No <If no, survey ends>
3. Does your office have a data business plan in place that guides the way you manage or govern your data systems or databases (or is one planned)?
    a. Yes, a data business plan is in place and being implemented within our business area
    b. Yes, a data business plan is in place, but has not been implemented yet
    c. We are in the process of developing a data business plan
    d. No, we don't have a data business plan, but one is planned or we recognize the need for one

e. No, we don't have a data business plan in place, nor is one planned

f. Other (please specify)

4. Does your office regularly assess its data systems or databases to identify needs for improvement? If yes, how often is the assessment conducted?

    a. Yes (please explain) <Text box>

    b. No

5. Have you done any assessments of data governance maturity or capability within your business area? If yes, please provide a brief explanation.

    a. Yes (please explain) <Text box>

    b. No

6. Does your office have formal policies and procedures in place for managing and governing its data systems or databases?

    a. Yes, we have formal standards, policies, and procedures in place for the way we manage and govern our data

    b. Yes, we have procedures in place, but they are not standardized or incorporated into policy, or our procedures differ each time we need to reconcile or correct data.

    c. No, we have no defined standards, policies, and procedures in place

    d. Other (please explain)

7. Are the workflows and business processes for managing your data systems or databases documented? If yes, please provide a brief explanation.

    a. Yes (please explain) <Text box>

    b. No

8. Are there clear roles and responsibilities (e.g., data stewards, data business owners, and data custodians) defined for data management and governance activities?

    a. Yes, roles and responsibilities are formalized and documented as part of our employees' job descriptions

b. Yes, there are clear roles and responsibilities, but they are not formalized or incorporated into job descriptions

c. No, we do not have defined roles and responsibilities

d. Other (please explain)

9. Is there a governance board or working groups set up for data management or governance?

    a. Yes, there is a governance board or working groups within our business area

    b. Yes, our office is part of a larger agency-wide governance board or working group

    c. No

    d. Other (please explain)

10. Please provide your (or a designated representative's) contact information for follow-up if we have questions regarding your response.

    a. Name: <Text box>

    b. Email: <Text box>

    c. Phone: <Text box>

APPENDIX F. STATE SAFETY DATA SYSTEM CAPABILITY MATURITY MODEL

The capability maturity model is adapted from the United States Roadway Safety Data Capabilities Assessment. (Vanasse Hangen Brustlin, Inc., United States Roadway Safety Data Capabilities Assessment, FHWA-SA-12-028, July 2012.) It defines levels of maturity for each of the following dimensions of capability:

- **Safety Data Collection and Technical Standards:** What safety data is collected? How well do safety data programs meet data quality standards for timeliness, accuracy, completeness, consistency, integration, and accessibility?

- **Data Analysis Tools and Uses:** How well does the SSDS support the roadway safety management process, including network screening, diagnosis, countermeasure selection, and evaluation? How well does the SSDS support advanced analysis methods using tools such as the Highway Safety Manual, the Interactive Highway Safety Design Model, or AASHTOWare Safety Analyst™?

- **Data Management and Governance:** Is there a data governance structure for the SSDS? For example, are there formally defined roles, accountability, and core capacities for data governance? Is there a designated data governance board, data stewards, and data owners? What policies and procedures exist for collecting, maintaining, using, and updating safety data? Are technology and tools for safety data management and analysis consistent, standardized, and updated?

- **Data Interoperability and Expandability:** To what extent are linked data sets from roadway, crash, and others included in safety analysis? Are existing safety data systems expandable as new technologies and tools are developed?

There are five distinct levels of capability for each of the dimensions:

- **Level 1 – Initial or Ad Hoc.** The agency is not aware of the need for capability in a specific dimension, or activities and relationships are taking place but are largely ad hoc, informal, and champion-driven. There is no plan for interoperability or expandability.

- **Level 2 – Repeatable.** The results of previous projects and the demands of the current project drive activities and actions. Individual managers decide what to do on a case-by-case basis during individual projects.

- **Level 3 – Defined.** The agency documents technical and business processes rather than on a per-project basis. The agency's standards relate to an adopted strategy, and this guidance determines project outcomes. However, there is limited accountability and uneven alignment with internal and external partners.

- **Level 4 – Managed.** The agency uses process management to initialize and supervise individual projects. Performance is measured, processes are predictable, and the organization can develop rules and conditions regarding the quality of the products and processes. Internal and external partnerships are aligned.

- **Level 5 – Optimized.** Safety data management and governance is a full, sustainable program priority, with top-level management support and formal partnerships in place. The whole organization focuses on continuous improvement. The organization possesses the means to detect weaknesses and to strengthen areas of concern proactively.

FHWA expects to publish a revised version of the capability maturity model in 2017.

The following tables provide detailed descriptions of maturity for each dimension and element of the capability maturity model. The tables are provided in worksheet format for States to note strengths, weaknesses, current maturity level, desired maturity level, and actions to advance to the desired maturity level for each assessment area.

States may wish to assign a separate maturity level for different elements of their safety data system. For example, there may be portions of a State's system that are operating at a higher maturity level, while others are at a lower level. States may note specific areas within the element they wish to improve. For desired maturity level, it is acceptable for States to choose a lower maturity level if it is realistic for the organization.

AREA 1: SAFETY DATA COLLECTION AND TECHNICAL STANDARDS

Element 1A: Completeness

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	The State maintains low-level of detail (i.e., limited elements) for critical safety data elements for some or all State-owned roads. There is a moderate to large amount of missing or blank fields.	The State maintains either a high or a moderate level of detail for critical safety data elements for all State-owned roads. The records have no more than a moderate amount of missing or blank fields.	The State maintains high-level detail (maximum elements) for critical safety data elements for all State-owned roads. The records have few missing or blank fields (i.e., less than 5%)	The State maintains high-level detail (maximum elements) for all State-owned roads and moderate level of detail for some data elements for some non-State road mileage. The records have few missing or blank fields (i.e., less than 5%)	The State maintains high-level detail (maximum inventory elements) for critical safety data elements for all public roads in the State. There are few missing or blank fields (i.e., less than 5%).
Current					
Desired					
Actions to Advance to the Next Level					
•					

Note: States may wish to assess their crash, roadway, and traffic data systems separately.

Element 1B: Timeliness

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	The State has no standardized procedure for updating safety data files. Changes to the files are made only when they come to the attention of the file maintainer.	The State's process for updating is based on volunteer reporting by field personnel. This leads to a moderate number of cases where no report is made. For changes reported, the updates made to the database normally take six months or longer.	The State updates its safety databases on an annual (or less often) basis. The new data are entered into the computerized files within three months of data collection.	The State continually updates all safety databases. The data are updated to the computerized file within 2-3 months of completion of data collection.	The State continually updates all safety files and there is a documented process in place. The data are updated to the computerized file within one month of completion of data collection.
Current					
Desired					
Actions to Advance to the Next Level					
•					

Note: States may wish to assess their crash, roadway, and traffic data systems separately.

Element 1C: Accuracy

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	The State has no measure of the accuracy of their safety data systems and the accuracy is felt to be low. There is no external verification with field data and no internal verification with checks for reasonableness.	The State has some subjective judgment of accuracy indicating a moderate level of accuracy across the safety data systems they maintain. The measure of accuracy is generally judgment based on maintainer or user familiarity with the data. There is no external verification with field data and no internal verification with checks for reasonableness.	The State has a moderate level of accuracy in their safety data systems across all categories they maintain. The data are believed to be moderately accurate, but the State does not conduct any kind of external verification process. The State also has developed and uses a computerized set of internal verification checks for data reasonableness.	The State has a moderate to high level of accuracy in their safety data systems across all categories they maintain. The level of existing accuracy is verified by occasional external verification with field data collection. The State also has developed and uses a computerized set of internal verification checks for data reasonableness.	The State has a high level of accuracy in their safety data across critical data elements. The existing values are accurate as determined by frequent systematic external verification process. The State has developed and uses a computerized set of internal verification checks for data reasonableness.
Current					
Desired					
Actions to Advance to the Next Level					
•					

Note: States may wish to assess their crash, roadway, and traffic data systems separately.

Element 1D: Uniformity or Consistency

Strengths		Weaknesses			
•		•			
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	The State has a low level of uniformity and consistency with national standards. Data coding is not consistent across all State or non-State files. There are no procedures in place to ensure coding is consistent across multiple years.	The State has a moderate level of uniformity and consistency. Data coding is consistent across all State files except non-State files. Procedures are in place to ensure coding for most elements is consistent across multiple years, but procedures are not in place to ensure particular locations on roadways tracked across multiple years.	The State has a moderate level of uniformity and consistency. Data coding is consistent across all State files except non-State files. While procedures are in place to ensure particular locations on roadways tracked across multiple years, procedures are not in place to ensure coding for all elements is consistent across multiple years.	The State has a moderate to high level of uniformity and consistency. Data coding is consistent across all State files except non-State files. Procedures are in place to ensure coding is consistent for all elements across multiple years and locations on roadways can be tracked across multiple years.	The State has a high level of uniformity and consistency in element definitions and codes based on national standards. Data coding is consistent across all State and non-State files. Procedures are in place to ensure coding is consistent across multiple years.
Current					
Desired					
Actions to Advance to the Next Level					
•					

Note: States may wish to assess their crash, roadway, and traffic data systems separately.

AREA 2: DATA ANALYSIS TOOLS & USES

Element 2A: Network Screening (Data)

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	Solicited Input – severe lack of crash data, must rely on input from district, county, or local staff or citizen complaints to identify sites for improvement.	Crash-Based – based on crash data only (or fatal crash only). Does not link traffic or roadway inventory data.	Crash-Based Plus – based on crash data with traffic or roadway inventory linked. Difficult to identify "zero-crash" locations	System Analysis –based on roadway inventory data (for example, ability to screen all curves or intersections of a certain type to determine sites with most promise), incorporating traffic volume data and crash data (for example, use of AASHTOWare Safety Analyst™).	System Plus Analysis – based on roadway inventory data, incorporating traffic volume data and crash data, along with citation, driver, or injury outcome data.
Current					
Desired					
Actions to Advance to the Next Level					
•					

Element 2A: Network Screening (Method)

Strengths		Weaknesses			
•		•			
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	Judgment – relies solely on input and judgment of State and local transportation staff.	Simple Methods –ability to use traditional screening tools such as crash frequency, crash rate, or crash severity indices. Does not account for regression-to-the-mean and does not set a performance threshold.	Traditional Methods – ability to use traditional screening tools such as crash rate or crash severity indices. Accounts for mean exposure. Does not set a performance threshold or account for regression-to-the-mean and is misled by the non-linearity of rate (crash and traffic volume).	Traditional Methods Plus – ability to use traditional screening tools such as crash rate or crash severity indices. Accounts for mean exposure and sets a performance threshold. Does not account for regression-to-the-mean and is misled by the non-linearity of rate (crash and traffic volume).	Advanced Methods – ability to employ state-of-the-art methods for network screening. Accounts for regression-to-the-mean, exposure, and sets a performance threshold (for example, uses a Safety Performance Function to determine the "expected" level of safety. Compares the relative safety of sites with similar characteristics (i.e., ability to identify specific groups of sites for screening).
Current					
Desired					
Actions to Advance to the Next Level					
•					

Element 2B: Diagnosis

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	Limited ability to generate statistics for any portion of the network. State may have difficulty generating a collision or condition diagram. Must rely heavily on site visits to assess potential safety issues.	Ability to generate a portion of the relevant statistics listed above for a portion of the network. State also has the ability to generate a collision or condition diagram.	Ability to generate relevant statistics and summaries for a portion of the network. Statistics include total crashes for a given study period by type, severity, time of day, day of week, date, road condition, lighting condition, weather condition, and driver impairment. Summaries include the ability to generate a condition diagram and a collision diagram. Some of the data for the condition diagram may have to be measured in the field or obtained from aerial imagery.	Ability to generate a portion of the relevant statistics listed above for any specific site or corridor (includes all public roads). Ability to generate a collision and a condition diagram, although some of the data for the condition diagram may have to be measured in the field or obtained from aerial imagery.	Ability to generate relevant statistics and summaries for any specific site or corridor (includes all public roads. Statistics include total crashes for a given study period by type, severity, time of day, day of week, date, road condition, lighting condition, weather condition, and driver impairment. Summaries include the ability to generate a condition diagram and a collision diagram. Can calculate over-representation of crashes – similar to AASHTOWare Safety Analyst™. Roadway data should be sufficient to generate a reliable condition diagram without site-specific field measurements. Roadway data for the condition diagram may include lane width, shoulder width, lighting presence, traffic control, signal phasing, posted speed, etc.
Current					
Desired					
Actions to Advance to the Next Level					
•					

Element 2C: Countermeasure Selection

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	Limited ability to determine existing safety-related infrastructure attributes for any portion of the network. Must rely heavily on site visits to assess potential safety issues.	State has the ability to determine a portion of the existing safety-related infrastructure attributes for a portion of the network. May require a site visit or use of aerial imagery to determine certain attributes.	State has the ability to determine all existing safety-related infrastructure attributes for a portion of the network. Includes peripheral safety databases such as sign inventory, lighting presence and condition, pavement condition, presence and condition of pavement markings, etc. for the network.	State has the ability to determine a portion of the existing safety-related infrastructure attributes for any specific site or corridor (includes all public roads). May require a site visit or use of aerial imagery to determine certain attributes.	State has the ability to determine all existing safety-related infrastructure attributes for any specific site or corridor (includes all public roads) without a site visit. Includes complete roadway data for intersections, curves, tangents, interchanges, and at-grade rail crossings. Also includes peripheral safety databases.
Current					
Desired					
Actions to Advance to the Next Level					
•					

Element 2D: Evaluation (Project-Level)

Strengths	Weaknesses
•	•

Level	1 – Initial	2 – Repeatable	3 – Defined	4 – Managed	5 – Optimizing
Criteria	Ability to conduct a simple before-after or anecdotal project level evaluation. Does not account for regression-to-the-mean, traffic volume trends, or temporal trends (i.e., changes over time other than the treatment or project of interest). Installation and crash data are available for the treatment site(s) of interest, but not for a reference or comparison group (i.e., non-treatment sites).	Ability to conduct a simple before-after project-level evaluation. Accounts for traffic volume changes, but does not account for regression-to-the-mean or temporal trends. Installation, crash, and traffic volume data are available for the treatment site(s) of interest, but not for a reference or comparison group (i.e., non-treatment sites).	Ability to conduct cross-sectional project-level evaluations. The State has crash, traffic volume, and roadway data for specific projects. An empirical Bayes analysis is not possible because either the State does not track the specific installation date OR there are fewer than 5 years of historical data available for analysis (not enough years to develop stable estimates of expected crashes in the before and after period).	Ability to conduct a rigorous before-after project-level evaluation, accounting for regression-to-the-mean, traffic volume trends, and temporal trends. State has the ability to perform this type of evaluation for some projects (i.e., requires data on a subset of roads in the State). This type of evaluation is carried out by applying the empirical Bayes before-after observational study. Requires installation data and 5+ years of historical crash and respective annual traffic volume data for treatment and non-treatment sites, and will develop SPFs for the evaluation study.	Ability to conduct a rigorous before-after project level evaluation, accounting for regression-to-the-mean, traffic volume trends, and temporal trends. State has the ability to perform this type of evaluation for any project (i.e., requires data on all roads in the State). This type of evaluation is carried out by applying the empirical Bayes before-after observational study. Requires installation data and 5+ years of historical crash and respective annual traffic volume data for treatment and non-treatment sites, and will develop SPFs for the evaluation study.
Current					
Desired					

Actions to Advance to the Next Level
•

Element 2D: Evaluation (Program-Level)

Strengths	Weaknesses
•	•

Level	1 – Initial	2 – Repeatable	3 – Defined	4 – Managed	5 – Optimizing
Criteria	Anecdotal program level evaluation. Data are not available to support specific program evaluations.	Crash data are available for at least all State-maintained roads to evaluate the overall performance of the State, but not at the project level to determine the effectiveness of a specific program.	Project-level data are available, but incomplete. May not include cost data, exposure data, or may not have 5+ years of crash data available for analysis.	Ability to evaluate the effectiveness of specific programs, including the cost and potential benefit. Requires project level data to identify the number of projects by type (so projects can be associated with a specific program), the cost of projects by type, and the relative timeframe of installation. Also requires crash data on a statewide basis with information on specific crash types and contributing factors. One of the following is also available: 1. Exposure data (for example, vehicle-miles traveled) are available to account for changes over time. 2. 5+ years of crash data are available to account for other time trends.	Ability to evaluate the effectiveness of specific programs, including the cost and potential benefit. Requires project level data to identify the number of projects by type (so projects can be associated with a specific program), the cost of projects by type, and the relative timeframe of installation. Also requires crash data on a statewide basis with information on specific crash types and contributing factors. Exposure data (for example, vehicle-miles traveled) are available to account for changes over time and 5+ years of crash data are available to account for other time trends.
Current					
Desired					

Actions to Advance to the Next Level
•

Element 2E: Accessibility

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	Few individuals within the State are granted access to the data.	State has an informal process for requesting data and the ability to provide data to some safety partners.	State has a formal process for requesting data and the ability to provide data to some safety partners within a defined timeline.	State has an informal process for requesting data and the ability to provide data to all safety partners.	State has a formal process for requesting data and the ability to provide data to all safety partners, including the public, within a defined timeframe.
Current					
Desired					
Actions to Advance to the Next Level					
•					

AREA 3: DATA MANAGEMENT AND GOVERNANCE

Element 3A: People

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	The State is not aware of the need for an institutional arrangement or organizational structure to support data governance. Management and staff do not recognize a specific need for a data management program to support performance management. The State does not have strong executive level support for data governance. No management input or buy-in on data quality problems. Executives are unaware of data problems or blame IT entirely. Success depends on the competence of a few individuals. Organization relies on personnel who may follow different paths within each effort to reconcile and correct data.	Success depends on a group of database administrators or other employees. Individuals create useful processes for data quality initiatives, but no standard procedures exist across functional areas. Some personnel in the State are aware of the need for a formal data management program and processes to support performance management but are not involved in developing such a program. Business analysts do not participate in from development of data quality rules. Work teams have been identified in several offices across State agencies to participate in the development and implementation of a data management program. Little corporate management buy-in to the value of data or to an enterprise-wide approach to data quality or data integration.	Data stewards emerge as the primary implementers of data management strategy and work directly with cross-functional teams to enact data quality standards. Some personnel in the IT (or similar) office of an agency currently participate in the development and implementation of a data management program for the State. Staff across the State are aware of the data management program and use the program routinely for the collection and use of data within the State. Executive-level decision-makers begin to view data as a strategic asset. Management understands and appreciates the role of data governance – and commits personnel and resources.	The State has strong executive and senior management support for data governance. Data governance has executive-level sponsorship with direct Chief Executive Officer support. Business users take an active role in data strategy and delivery. A data quality or data governance group works directly with data stewards, application developers, and database administrators.	A data governance council or data governance board exists at the State to direct the data management activities of the State (This is in addition to a TRCC – the TRCC would report to this governance council or board). Data champions have been identified in each business area of the State. Organization has "zero defect" (i.e., corrected immediately) policies for data collection, use, and management. People in the State are fully engaged in continuous improvement related to data management and performance measures. Staff across the State are actively involved in recommending changes for data management policies, standards, and procedures, as business needs change and new performance management goals are identified. Communities of interest, which are comprised of internal and external users and stakeholders for core data programs, have been defined.
Current					
Desired					
Actions to Advance to the Next Level					
•					

Element 3B: Policies

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 - Repeatable**	**3 - Defined**	**4 – Managed**	**5 - Optimizing**
Criteria	The State does not have a Data Business Plan in place to support management of core data programs. The State does not have defined roles, such as data stewards, stakeholders, business owners (of data), and communities of interest, to support a data governance framework. Data quality is non-existent, with no defined data quality processes	Data quality is project focused only, with limited defined data quality processes. "Firefighting mode." Address problems as they occur through manually driven processes. Most data management processes are short-range and focus on recently discovered problems. Data and data processing operate as silos–systems operate independently. Resources are not optimized due to redundant, outdated data. State senior management recognizes the need for a Data Business Plan to manage critical data programs; however, a plan has not yet been developed or the State is developing a Data Business Plan to support management of strategic data programs.	Rules for data governance emerge, but the emphasis remains on correcting data issues as they occur. Within groups and departments, tasks and roles are standardized. Data governance processes are built. Many State agencies have implemented a Data Business Plan to manage the core data programs for their area. Data metrics are sometimes measured against industry standards to provide insight into areas needing improvement.	Goals shift from problem correction to prevention. Real-time activities and preventive data quality rules and processes emerge. A service oriented architecture encapsulates business rules for data quality and identity management. Data metrics are measured against industry standards to provide insight into areas needing improvement. An enterprise Data Business Plan has been developed to support management of core data programs across the agency and has been incorporated into the overall State strategic plan. The State has developed and published a Data Governance manual or handbook, which identifies the roles and responsibilities of staff in the State to support data governance operations. It has developed a data catalog with data definitions, standards, policies, and procedures for the collection and use of data in the organization. The catalog is available on an enterprise basis electronically.	New initiatives are approved after careful consideration of how the initiatives will affect the existing data infrastructure. Automated policies are in place to ensure data remains consistent, accurate, and reliable throughout the enterprise.
Current					
Desired					
Actions to Advance to the Next Level					
•					

Element 3C: Technology

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	The State does not have any IT tools in place to support data management. No data profiling, analysis, or auditing is used.	Data cleansing and standardization occurs only in isolated data sources. Data improvement is focused on single applications. Agencies have delegated the responsibility to a specific office, such as IT, to determine what tools are needed to support data management across the agency. Most data are not integrated across business units; some departments attempt isolated integration efforts. Agencies have implemented some IT tools, including GIS, data models, data repositories, data dictionaries, etc., to support data management in certain offices of the agency.	Database administration tactics emerge. Tactical data quality tools are often available. Applications utilize data quality technology. The State uses IT tools on a widespread basis, including such applications as an enterprise data warehouse, GIS systems that integrate business data from various offices, and dashboards and scorecards delivered through a web-enabled interface for access statewide.	A data stewardship group maintains corporate data definitions and business rules. Data quality and data integration tools are standardized across the organization. All aspects of the organization use standard business rules created and maintained by designated data stewards. More real-time processing is available and data quality functionality is shared across different operation modes. The State uses Service Oriented Architecture as the enterprise standard and Open Database Connectivity in the development of new applications to support future integration of applications.	Data are continuously inspected – and any deviations from standards are resolved immediately. Ongoing data monitoring helps the data stewards maintain data integrity. The use of technology and tools in the State improves the overall management of programs in the State, in accordance with the strategic mission, goals, and targets. Data models capture the business meaning and technical details of all corporate data elements. Performance management tools, such as dashboards and scorecards, are used in every involved office of the State to monitor the progress of State programs in meeting the State mission and goals. Performance measures and targets are adjusted as needed and displayed on the State dashboard, or similar mechanism, to maintain peak program performance across the State.
Current					
Desired					
Actions to Advance to the Next Level					
•					

AREA 4: DATA INTEROPERABILITY AND EXPANDABILITY

Element 4A: Interoperability

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	There are few or no examples of safety analysis using merged datasets. The reliability of linkage between roadway and crash data is problematic.	Safety analysis using merged roadway and crash data is performed for some, but not all roadway types. Other examples of analyses using merged datasets are rare and not well used in support of safety decision-making.	Safety analysis using merged data from roadway and crash records is common, but other analyses (for example, using injury surveillance data) are rare.	Safety analysis supports using linked datasets from roadway, crash and at least one other traffic records data source. Though not a standard feature of all safety analyses in the State, such analyses of merged data are not uncommon or difficult to find.	Safety analysis uses linked data sets from sources including roadway, crash, injury surveillance, citation, and others. The linked data sets are considered reliability for supporting decision-making. Analysis of merged data is a regular feature of safety analysis.
Current					
Desired					
Actions to Advance to the Next Level					
•					

Element 4B: Expandability

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	The majority of safety data sources are stand-alone systems, of varying vintage, design, and software. Adding new data elements usually is not done. Linkage to external (outside the DOT) sources is not generally possible. Use of GIS in safety analysis is limited, not covering a significant portion of the public roads, crashes, or other key data	Within the State DOT, a few systems are modern, and the rest are considered legacy. Adding new data elements or additional roadway miles or segments is difficult and piecemeal. The plans for replacement of older components are "long term," not currently funded, or stalled. Data linkage is difficult requiring many different "mappings" among location coding schemes and system designs. Much of the work is manual or simply not performed. Spatial display of data is limited and not well integrated into safety analysis efforts.	Within the State DOT, system components are of mixed vintage, built to different standards, and separately maintained. Adding new data elements or additional roadway miles/segments is possible, but will have been done separately for some system components. Movement is toward a common standard for software and database, but the implementation of full integration, enterprise-wide solutions is several years in the future. Some data linkage is automated, but some is manual and labor intensive. Expansion of the older systems is considered too expensive and not worth the effort given, their eventual replacement is planned. For critical expansions, a minimal design to get the job done is the standard. Newer systems are easily expandable. Spatial data are just used in visualization of layers in the GIS – no (or limited) spatial analysis capabilities	Within the State DOT, systems are written in modern languages with modern database structures. Adding new data elements or additional roadway miles or segments is generally easy, but may have been done separately for some system components. There are common platforms, but not a single system for enterprise-wide databases or software. Data linkage generally is automated among the DOT's main systems, but some data sources require manual effort to convert to a common location-coding scheme. Analytic tools (including GIS) exist and some capability for spatial analysis exists. Expansion of systems would be difficult, but not impossible to coordinate.	Within the State DOT, modern database design and enterprise-wide planning mean adding coverage or data elements is built into systems and thinking about system improvements. Data transfers among agencies (esp. local and State) are electronic and automated as fully as possible. Linkage among systems is accomplished in an automated fashion. Analytic tools are integrated and provide "seamless" access to users. Full spatial analysis capabilities are available.
Current					
Desired					

Actions to Advance to the Next Level
•

Element 4C: Integration

Strengths			Weaknesses		
•			•		
Level	**1 – Initial**	**2 – Repeatable**	**3 – Defined**	**4 – Managed**	**5 – Optimizing**
Criteria	There is little or no linkage between safety data systems. Linkage to external Location coding is not standardized or accurate.	Most of the safety data systems are not linked. Multiple incompatible location coding methods are used.	Some key safety data sources are not linked. More than one location coding method is used and there are some incompatibilities among them.	The major safety databases are linked. While more than one location coding method is used, the translation among methods is automated and works well.	All of the key safety databases are linked. A single method of location coding is used.
Current					
Desired					
Actions to Advance to the Next Level					
•					

Note: States may wish to identify desired maturity levels for different time horizons (e.g., 1-year, 3-year, and 5-year).

APPENDIX G. DATA GOVERNANCE 101

This appendix provides an overview of data governance.

DATA MANAGEMENT LIFE CYCLE

Because data is a valuable asset, a State should manage it over its entire lifecycle. The lifecycle encompasses the time from collecting data to the time it is archived or updated/refreshed. Figure G.1 depicts the elements and stakeholders typically involved in each phase of the data management life cycle.

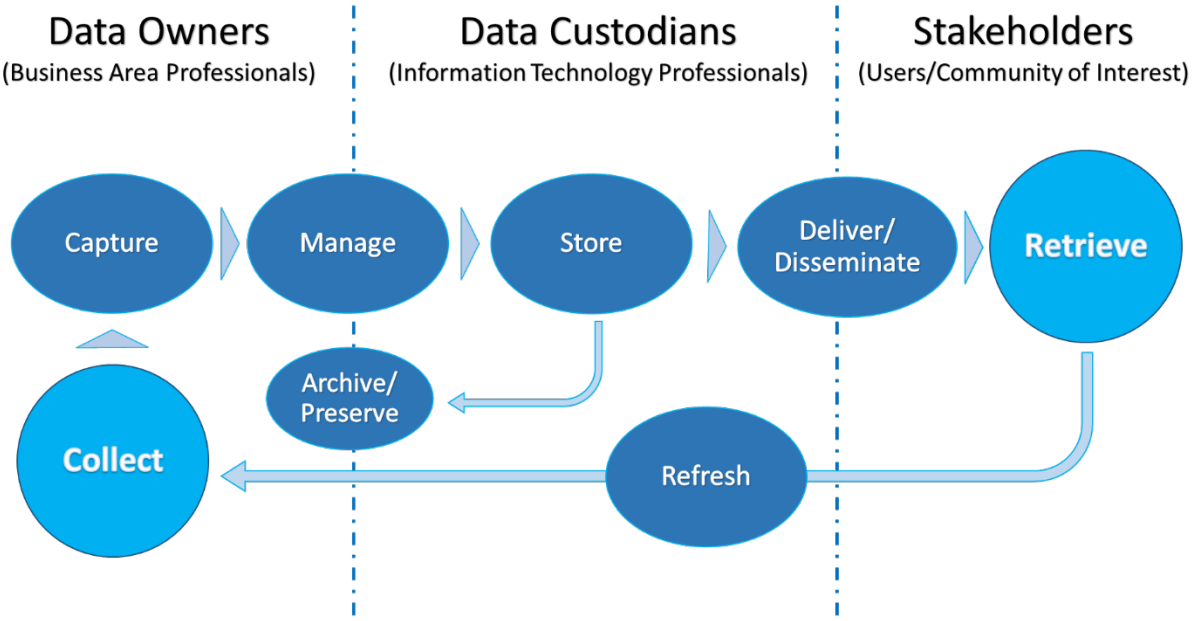


Figure G-1. Flow chart. Data management life cycle.

Source: NCHRP Report 754: Improving Management of Transportation Information, Transportation Research Board, 2013.

Data governance principles apply to each phase of the data management life cycle to ensure data is trusted and understood:

- **Collect:** Standards should exist for the recording of asset name, location, and descriptive attributes. The data collected for each asset and attribute must reflect the requirements of each successive phase of the life cycle.

- **Capture:** Data capture involves the transfer of records from the collection mechanism to a system-of-record. This is the phase to verify geographic completeness to ensure data exists for all division and regions or, where appropriate, for each individual asset statewide.

- **Manage:** Manage involves any processing or validation of data within the system-of-record to improve ease-of-use. This includes performing quality assurance and quality control processes on data. Standards must exist for each individual data element.

- **Store:** Data storage using systems with contemporary architecture to ensure data is serviceable by data managers. Procedures should exist for identifying the people from both the business and technical sides of the DOT responsible for maintaining the database.

- **Archiving and Preservation:** Archiving, preserving, or destroying data is subject to significant regulation, particularly where sensitive financial or personal information is concerned. Decisions around this phase of data management are subject to Department or State standards and are made under the authority of data owners and data custodians.

- **Deliver and Disseminate:** Much like archiving, the delivery and dissemination of data is subject to legal restriction and regulations. Data delivery is a distinct and separate function from data capture, since the data owner plays a gatekeeper role.

- **Retrieve:** Data should be accessible to all users within the Community of Interest through well-publicized retrieval methods, ad hoc queries, or formal reports. Users may retrieve data, but they should not alter it or add to the system-of-record without the permission and possible assistance of data owners.

- **Refresh:** Data custodians must understand user needs and obtain feedback on tools and data to make appropriate revisions or corrections.

States can easily customize the data management lifecycle to show roles and responsibilities for data governance in their organization, but the basic elements are the same for almost any application.

IDENTIFYING THE NEED FOR DATA MANAGEMENT AND DATA GOVERNANCE

This section helps States establish a need for data governance and obtain buy-in from executives and decision-makers.

Identify and Document Needs

Most States realize a need for data governance when they encounter issues within a specific program area or when complying with Federal or State requirements related to funding, reporting, or accessibility. This usually leads to small groups discussing issues with managers in an attempt to

solve problem. These small groups of data managers and stakeholders are exactly the ones who are best equipped to lead initial data management efforts in coordination with managers who will get them the support they need to do their jobs.

A good way to get started on identifying safety data governance needs is to coordinate a focus group that includes (at a minimum) representatives from the traffic, crash, and roadway data business areas. The group should meet to discuss general data needs and requirements of their program areas and to identify opportunities for improvement.

Demonstrate Return on Investment through a Governance Model

After needs are identified and documented, the next step is to relate improvements in safety data management to a return on investment (ROI) in planning processes, performance measures, target setting and prioritization of resources.

One method is to show how safety data links to planning, performance measures, and target setting processes. A State should design and implement a data governance model to assist with this. A data governance model is a diagram that visualizes the connection between a Department's mission, vision and goals, data governance practices, and the program areas. The need for governance is established by illustrating how individual programs provide information critical for decision-making. Figure G.2 shows an example data governance model.

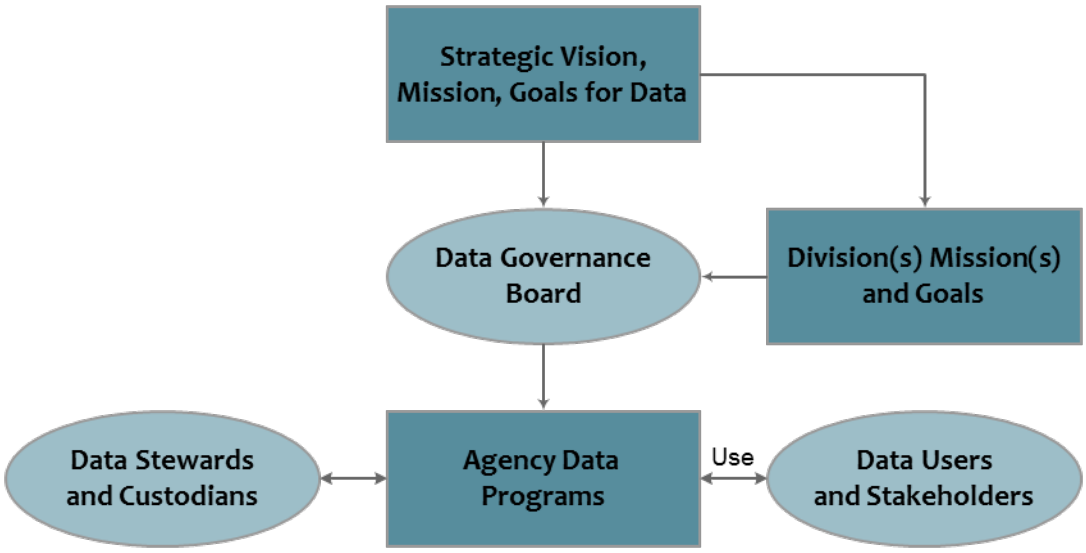


Figure G-2. Organizational chart. Example data governance model.

Source: Adapted from NCHRP 666, Figure 4.2, Overview of a general data governance framework.

States can use information from the initial assessment and group discussion to customize a model for their DOT. This exercise fosters collaboration between business areas and leads to a better awareness of how specific data programs help managers make informed decisions.

Data governance leads to improved data within individual program areas, which provides management with quality analysis tools, applications, and reports to support data-driven decision-making.

Data governance can help improve the following data concepts:

- Traceability – Data governance helps align programs with DOT needs;
- Performance Measures – Improved data allows for better target setting and performance tracking;
- Risk Assessment – Starting a data governance program requires a DOT to assess risks associated with data management;
- Value of Data Programs – Part of data governance is demonstrating value of data programs to those who authorize investment in them; and
- Knowledge Management – This system enables documentation and sharing of lessons learned and experiences pertaining to data management.

Communicate the Need to Stakeholders

After the focus group has made some progress in documenting needs and developing a governance model, they should share the findings with colleagues, managers, decision-makers, and other stakeholders to obtain buy-in and support for improvement. The presentation of needs will depend on the group, but in general should be simple, focused, and demonstrate the benefits of governance. One approach is to target a problem a manager or colleague might face that is solvable through better data and tools. For example, in one State, a director needed a way to show legislators funded projects in their district so they could ensure fairness in resource allocation. This required getting data from several sources and manually compiling it to produce a table of results for a specific district. Better data integration and management could support an interactive tool that allows managers (or even legislators) access to do this type of analysis on the fly. The return on investment is reduced staff time (and expense) in manually building the report, more accessible data, and better decision-making regarding the allocation of resources.

Obtain Agreement on Need

A good practice is to share findings and the agreement on the need (if any) back to business areas supporting the effort. This is a good opportunity to get more staff and stakeholders involved in the planning process to ensure all needs for safety data management are included in the data business plan.

After high-level managers and executives agree there is value in pursuing data governance, they will need a detailed plan to move forward and can proceed with the steps in the Guide for State DOT Safety Data Business Planning.

DATA MANAGEMENT PRACTICES

Effective data management practices are necessary for a State to collect, update, describe, standardize, analyze, store and protect safety data to ensure its usability. States should consider the following aspects of data management: (Cambridge Systematics. Inc. U.S. DOT Roadway Transportation Data Business Plan (Phase 3): Data Business Plan Development for State and Local Departments of Transportation, May 2017. (Draft).)

- **Data collection.** Define responsibilities for the collection, update and maintenance of data; identify where duplicate data collection and storage exist; address data ownership and user rights; investigate new data acquisition methods.

- **Data quality.** Define data quality per governance standards; adopt data quality standards and metadata for the collection, processing, use, and reporting of safety data; document data quality procedures for each data system, with instructions on how to process data errors; and develop validation rules and allowable values for coded fields in data systems and repositories.

- **Data standards.** Define metadata standards for each type of safety data set (for example, roadway, crash, traffic, project), data dictionaries and descriptive information for data products; develop metadata guidelines to indicate update frequency, age of data, and integration with other data sources; and coordinate with applicable data standards. Note that metadata standards are different from data format standards.

- **Data privacy and security.** Ensure data privacy and security related to safety data in accordance with Federal and State legislative requirements and limitations.

- **Data storage and access.** Define business requirements for data access, analysis and reporting; define responsibilities for data storage, hosting, data retention (archive), and disposal; define data ownership and dissemination rights; and explore methods to enhance access to data. This includes developing web portals that internal and external stakeholders can use to obtain data and information as needed.

APPENDIX H. STATE PRACTICES FOR IT PROJECT PRIORITIZATION AND SELECTION

This appendix presents best practices for IT project identification/selection process. The information is based on brief research of IT practices at Michigan, Montana, New Mexico, Pennsylvania, and Texas DOTs conducted as part of another project. (Cambridge Systematics, Inc. IT Project Selection Criteria. Research conducted as part of the Highway Enterprise System and Asset Management Analysis Assistance for the MassDOT Highway Division, 2014.)

PROCESSES FOR SUBMITTING IT PROJECT REQUESTS

Annual Call for Projects (Michigan DOT)

DOT-specific software procurement at Michigan DOT is managed at the department level. In an annual call for IT projects, different divisions submit their needs for a two-year budget cycle. The Call for Projects Memo includes background information on existing IT priorities to provide some context for incoming projects. Requestors coordinate with their automation manager (AM) to submit a MDOT Call for IT Projects Questionnaire Template. The AM vets the questionnaire with the requestor and with the bureau management. (These move no further if the bureau/management does not support it). The questionnaires are sent to MDOT's Project Management Office, which assembles all of them, distributes them, and then schedules a prioritization meeting.

IT Strategic Plan (Texas DOT)

In accordance with Legislative mandate, TxDOT develops the agency Strategic Plan, which includes the IT strategic plan, each biennium. To develop the IT strategic plan, the Technology Service Division (TSD) Business Services Section gathers IT information regarding technology needs, plans and alignment to agency strategic goals from each district, division, office, or region (D/D/O/R). TSD section directors review the resulting list of needs to identify potential overlaps and to assess high-level future infrastructure requirements to support the needs, and then compile them into the IT strategic plan. TSD also answers standard statewide questions about agency plans for technology consolidation, IT managed services, security and privacy and green IT. Director, TSD submits this plan to Administration.

PROJECT PRIORITIZATION AND SELECTION PROCESS

Pre-Review of IT Project Requests and Prioritization Meeting (Michigan DOT)

MDOT AMs collectively meet at prioritization meetings to discuss how the proposals fit into priorities and any alternative ways to handle the requests. Sometimes project requests are turned into maintenance requests; other times they will spawn a small project to satisfy the requests outside of the major project category. MDOT sets aside funding to handle these smaller requests.

MDOT technical staff also review the project scope in preparation for the prioritization meetings.

IT staff (who report to the CIO) participate in the project prioritization and selection process to ensure projects are consistent with current activities and priorities. The priorities for prioritizing projects in that particular year are established ahead of time and made available in the Call for Projects Questionnaire. While there is a spreadsheet that performs calculations on the answers, the MDOT/IT group found there is a tendency for requestors to want to answer positively to these questions, partly because from their points of view their projects are high priority. MDOT reviews the priorities each year, with an intent to identify projects that are needed to maintain funding level(s). MDOT notes that the priorities are frequently interpreted to mean that a project needs to follow some procedure in order to justify the expenditure of funds, which is not the same thing as their intent.

The results of this process is a prioritized list of IT projects that is forwarded to the Steering Committee (several bureau chiefs) for approval. The committee reviews the projects, and the prioritization method is explained. Also discussed is staging and timing of the projects. Most of the issues/questions have already been addressed during prioritization.

MDOT has been following this process for several years, and it seems to work well. It has allowed them to be flexible and adapt to changing MDOT conditions, statewide IT efforts, varying funding levels and sources, etc. Additionally, it closely follows the process MDOT uses to identify and select highway projects.

Bottoms Up Process (Montana DOT)

Within the Montana DOT, there is an Information Services Division led by a Division Administrator. This individual oversees procurement, initiation, and implementation of IT objectives within the agency. The division acts as a clearinghouse for IT investment and supports requests coming from other divisions in the agency (e.g., engineering, planning,

aviation, etc.). Investment decisions come through a bottoms-up process. Each division prioritizes their needed investments, which are then presented to the IT Division. The IT Division, with DOT leadership oversight, then helps to prioritize requests coming from all of the DOT divisions.

For IT investment decisions, projects are grouped into three different levels of investment, with increasing stringent procedures for larger projects:

- For projects that are estimated to require less than 100 hours of internal work, the request is coded as a simple work ticket that is entered into a prioritization queue for internal delivery.

- Projects requiring between 100 and 500 hours will involve a higher level of project oversight and more documentation. Such projects will receive a dedicated project manager and IT resources, and the department may decide to contract externally for some of this work.

- Projects requiring more than 500 hours of work—for example, a request to replace a bridge management system—must go through the most stringent oversight and approvals process. Such projects must be presented before the IT investment selection board, which includes all of the division administrators along with department director and deputy director. The investment selection committee makes decisions about competing large investments and discusses where to find funding.

Per recent legislation, State CIO approval is required for any IT investment that is projected to exceed $50,000 over the life of the project (5 years). The CIO may decline to approve a project if it does not match well with broader State IT strategy.

For projects exceeding $200,000, the investment needs to be included in the MDT investment plan, which will in turn be filed with State legislative plan. This enables MDT to request the required funding from the legislature.

Decision Lens Software Methodology (Pennsylvania DOT)

Pennsylvania DOT Office of the CIO uses Decision Lens software to prioritize IT projects and allocate resources to the highest value projects in an effort to reduce advocacy-based decision-making. The CIO meets with a committee of representatives from each of the departments to develop a prioritization model for the entire organization, including departmental goals, objectives of IT projects, technical evaluations, and department priorities. From there, project

prioritization is facilitated within each department, using parts of the department model. To create a final prioritization list, each department's ranking of project priorities is combined with an overall evaluation of both strategic and technical criteria. The office then initiates on ongoing process for the addition of new projects and removal of completed ones.

The Decision Lens software includes the following steps in an IT project prioritization process:

- Criterion Development. Development of a decision model or criteria hierarchy identifies what the organization is trying to achieve so that IT can select projects that best align with those objectives.

- Criterion Weighting. The selected criterion are then ranked in order of importance by members of the selection team. Decision Lens uses pairwise comparison, in which users select priorities among pairs of criteria, and the software produces a weighted priority list. A percentage weighting is assigned to each of the criteria based on their importance or ranked preference. For example: Financial Returns – 0.33; Strategic Alignment – 0.18; Platform Alignment – 0.16; Geographic Alignment – 0.15; Internal Process Improvement – 0.10; and Ability to Execute – 0.08.

- Prioritizing Projects. Each project is then rated against each criterion using a scale ranging from zero to one, where zero = project does not meet criterion and one = project exceeds criterion. The rating is multiplied by the criterion weighting, resulting in a value score between zero and 1 for each project based on its rating on the criterion and the criterion's relative weight. The projects are then ranked in order of priority based on the value score results.

- Allocate Resources. The priority results are used to select projects for funding. Resources are allocated in a way that optimizes the value returned across the entire portfolio. Projects may be fully funded, partially funded, or deferred.

Project Portfolio Management Methodology (New Mexico DOT)

New Mexico DOT has adopted the Project Portfolio Management (PPM) methodology, which is a strategic prioritization methodology employed to analyze and manage current or proposed projects within an organization. The aim of PPM is to determine the best grouping and sequencing of projects to achieve organizations' business goals, in order to see them through from concept to completion. The Department employs Project Management Professionals

(PMP) within the Compliance and Project Management Program and the Administrative Services Division that are Project Management Institute (PMI) certified.

NMDOT is at a maturity Level 3 "Value Management." This level requires metrics, models, and tools for quantifying the value to be derived from projects. The Department is in the process of assessing project interdependencies and portfolio risks. This analysis will allow projects to be ranked based on "bang-for-the-buck," producing a good approximation of the value – maximizing project portfolio.

In the PPM method, projects must be evaluated against common, weighted criteria to determine where they fit into the portfolio mix. Often, organizations will implement PPM software tools to aid in the decision-making process. PPM tools are used to enable visibility, standardization, measurement and process improvement. A strong IT governance structure is considered a crucial component of a project and portfolio management strategy as well. This structure typically includes a Project Management Office that supports the project development process, manages the IT project pipeline, evaluates project performance, and prioritizes IT projects. In addition, a Governance Council (executive steering team) reviews prioritized project list, interprets strategic plans and initiatives, provides budget and resource parameters, and makes final project selections.

IT PROJECT SELECTION CRITERIA

Prioritization Based on IT Priorities (Michigan DOT)

The priorities for prioritizing projects in a particular year are contained in Section Three of Michigan DOT's Call for Projects Questionnaire. These criteria include the following:

- Maintains critical or essential MDOT services through IT systems
- Migrates existing software applications from unsupported technologies
- Maintains funding
- Supports the required delivery of the Five-Year Transportation Program
- Supports IT related aspects of Federal or State legislation
- Promotes efficiencies & effectiveness of operations and/or ensures value for MDOT/DTMB investments
- Supports safety & security and/or health & welfare of Michigan citizens
- Promotes technologies that enhance integration & connectivity of the transportation system across & between modes

- Promotes collaborative business relationships between MDOT, technology stakeholders, other transportation entities, or local government agencies
- Promotes technologies that aid the public in accessibility to goods and services & opportunities that enhance quality of life

IT project selection criteria may change from year to year and are established based on the Department's strategic objectives, IT priorities, and executive management input.

Decision Lens Software Criteria Hierarchy (Pennsylvania DOT)

The Decision Lens Software used by Pennsylvania DOT allows development of a decision model or criteria hierarchy based on what the organization is trying to achieve. This allows an agency to select IT projects that best align with those objectives. Example criteria provided by Decision Lens include:

- Strategic Alignment – How does the project support the organization's strategy or objectives?
- Financial Returns – What value will the project deliver in terms of sales or margin contribution, future cost savings or some other measurable return on investment?
- Ability to Execute – Can it be done? Are there technical, resource based, cultural, or other potential hurdles that could affect the organization's ability to execute the project?
- Platform Alignment – How does a proposed project or asset fit in the organization's current or targeted IT environment?
- Internal Process Improvement – How, or to what extent, does the project make work easier, more effective or more efficient?
- Geographic Alignment – Whom does the project reach? Where are the targets located? Is the focus on internal users or external customers?

Project Portfolio Management (PPM) Criteria (New Mexico DOT)

In the Project Portfolio Management (PPM) process used by New Mexico DOT, selection criteria typically includes:

- Ranking potential projects by value & benefits
- Appraisal of risk

- Inventory of resource availability and allocation
- Determination of an optimal or acceptable size of the project pipeline
- Alignment of projects with strategic plans
- Balancing different types of projects by purpose and benefit
- Balancing opportunity, benefits, and risk

KEY COMPONENTS OF GOOD PRACTICES

Based on the best practices review, the following are characteristics/key components of good practices:

1. Establish formal process for submitting IT project requests
    a. Annual call for IT projects
    b. Project questionnaire to obtain information on the nature of the project, expected benefits and costs, & support of IT priorities
    c. Require sponsors to obtain signatures from office/division level directors to establish executive support for the proposed effort
2. Establish a formal project prioritization & selection process
    a. Pre-review of IT project requests to discuss how proposals fit into priorities and identify alternate ways requests might be handled
    b. Utilize IT or Project Management Office staff to support development of project proposals, prioritize and select projects
3. Establish criteria for IT project prioritization
    a. Ranking potential projects by value & benefits
    b. Appraisal of risk
    c. Inventory of resource availability and allocation
    d. Determination of an optimal or acceptable size of the project pipeline

e. Alignment of projects with department's strategic objectives, IT plan, & executive management input

f. Balancing different types of projects by purpose and benefit

g. Balancing opportunity, benefits, and risk

4. Use tools to support project prioritization process & enable visibility, standardization, measurement, & process improvement

    a. Spreadsheet tools

    b. Decision Lens Software

    c. Severity and Risk Assessment matrix

    d. Project Portfolio Management tools

5. Manage the IT pipeline

    a. Maintain a database of current and potential projects

    b. Periodic measurement of project status & performance using Earned Value Analysis techniques

    c. Evaluate project status & performance against critical parameters

    d. Report items outside of targets/limits/thresholds

    e. Apply Stage-Gate model for continuation/termination decisions at major project stages

6. Engage executives in the IT project development & maintenance process

    a. Establish a governance council (executive steering team) to determine strategic plans & initiatives, review recommendations, finalize project selections, & determine budget and resource parameters

    B. Meet with IT Director on a regular basis to review prioritization and align new investment opportunities with business priorities

APPENDIX I. GLOSSARY OF DATA BUSINESS PLANNING TERMS

This guide introduces several terms related to data management. Below is a glossary of data business planning terms:

Community of Interest – Association of people comprised of internal and external stakeholders who share a common interest as users of a data system.

Data – A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or computers.

Data Owner – An individual responsible for definitions, policy, and practice decisions about data within their area of responsibility. For business data, the individual may be called a business owner of the data.

Data Business Plan (DBP) – Documents business rules and data quality standards for the information systems that support data programs, which will result in improved data management and data governance practices.

Data Governance – The execution and enforcement of authority over the management of data assets and the performance of data functions. This includes the people, policies, and procedures that govern data management and information systems. Data governance promotes the understanding of data as a valuable asset to the organization and encourages the understanding and management of data from both a technical and business perspective.

Data Management – The development, execution, and oversight of architectures, policies, practices, and procedures to manage the information lifecycle needs of an enterprise in an effective manner as it pertains to data collection, storage, security, data inventory, analysis, quality control, reporting, and visualization.

Data Program – A data program refers to specific data systems that support a business area of the organization. The "program" usually includes the functions of data collection, analysis, and reporting. It also includes policies, procedures, and resources for supporting these functions. In the case of a DOT, some examples of these programs include traffic, roadway inventory, safety, and pavement data.

Data Set – Any organized collection of data.

Extract, Transform, and Load – The process by which safety data are moved from their native systems, transformed into the format required by a specific analytic software, and loaded into the analytic software tool.

Information – Data and documents given value through analysis, interpretation, or compilation in a meaningful form.

Knowledge – Information combined with experience, context, and interpretation that make it possible to understand and draw implications from both data and information. Knowledge consists of data and information organized and processed to convey understanding, experience, accumulated learning, and expertise as they apply to a current problem or activity.

Safety Data – Safety data means crash, roadway, and traffic data on a public road, and, includes, in the case of a railway-highway grade crossing, the characteristics of highway and train traffic, licensing, and vehicle data.

Service Oriented Architecture – Software or database design that is independent of vendors, products, and technologies.

Silo Data System – A repository of data under the control of one department and is incompatible or not integrated with other data systems.

State Safety Data System – A SSDS must perform analyses supporting the goals in the SHSP and HSIP. The system must include 1) all public roadways, 2) crash, roadway, traffic, and railway-highway grade crossing data, 3) geolocation of safety data to a common basemap, 4) analysis and evaluation capabilities, and 5) the MIRE FDEs.

System Owner – IT professional(s) supporting the technical and functional aspects of data management and information delivery for specifically assigned business areas, subject areas, or databases.

For More Information:

Visit https://safety.fhwa.dot.gov/rsdp/manage.aspx

FHWA, Office of Safety

Stuart Thompson, P.E.

Stuart.Thompson@dot.gov

202-366-8090

FHWA-SA-17-047