PARTNERS FOR ADVANCED TRANSPORTATION TECHNOLOGY
INSTITUTE OF TRANSPORTATION STUDIES
UNIVERSITY OF CALIFORNIA, BERKELEY

I-210 Pilot System Requirements:

Job Descriptions and Duties/Tasks

December 23, 2016

Partners for Advanced Transportation Technology works with researchers, practitioners, and industry to implement transportation research and innovation, including products and services that improve the efficiency, safety, and security of the transportation system.

This page left blank intentionally

TABLE OF CONTENTS

1. REQUIREMENTS: JOB DESCRIPTIONS AND DUTIES/TASKS

This document lists the responsibilities of each job role identified in the System Requirements for the I-210 Pilot. The job roles are:

- Corridor Champions
- Corridor Manager
- Corridor Technical Manager
- Corridor Data Analyst
- Traffic Engineers
- Data Analysts
- Software Engineers
- Electrical Engineers
- Database Administrators
- Stakeholders
- Maintenance Staff
- IT Support
- IT Security
- Traffic Management Center (TMC) Operators
- Traffic Control System (TCS) Operators
- Transit Field Supervisors
- Public Information Officers
- First Responders
- Outreach and Communications Manager

For each role, the responsibilities are grouped by requirement type (Institutional Support, Strategic Response Planning, Data Management, etc.). The intent is to provide a way to understand the Knowledge, Skills, and Abilities (KSAs) needed for each job and to trace the job functions directly to the System Requirements.

Stakeholders decide how these roles will be filled at their particular agencies. Not every agency will have every role, and specific job titles may vary from agency to agency.

2. CORRIDOR CHAMPION(S)

The Corridor Champion is the individual in an organization who leads and advocates for the program, secures the support and participation of the stakeholders and other agencies throughout the process, and acquires resources within the major organizations participating in the Integrated Corridor Management (ICM) process.

2.1. INSTITUTIONAL SUPPORT

Institutional Support focuses on strategic planning and on how organizations and people are structured, funded, motivated, and informed in order to execute strategic plans.

Responsibility
1. Resolve problems in management structure and processes. Assist as needed with ongoing management functions.
2. Resolve communication breakdown issues.
3. Ensure agreements are signed and followed.
4. Resolve outreach and communications issues.

2.2. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed and tested.

Responsibility
1. With stakeholders and the Corridor Manager, determine why quarterly response plan analysis meetings are not being held or attendance is low, and remedy the causes.

3. CORRIDOR MANAGER

The Corridor Manager ensures that the Integrated Corridor Management (ICM) process and project are successful. This is the most important role described in this document and requires organizational, managerial, and technical skills and awareness. The Corridor Manager is the primary point of contact for corridor planning, operations, data, maintenance, and oversight and will make decisions for the good of the corridor that may or may not be part of the job description/tasks. This role touches all areas of the System Requirements, including:

- Institutional Support
- Corridor Monitoring
- Strategic Incident/Event Response Planning
- Real-Time Incident/Event Monitoring
- Real-Time Response Planning
- Response Plan Implementation
- Data Management
- Decision Support
- Core System User Interface
- System Integration
- System Management

3.1. INSTITUTIONAL SUPPORT

Institutional Support focuses on strategic planning and on how organizations and people are structured, funded, motivated, and informed in order to execute strategic plans. The requirements document often states that the following job responsibilities will be carried out "in consultation with stakeholders." We have not included those words in this document.

Responsibility
1. Post-Launch Corridor Strategic Plan
a. Oversee the drafting, review, approval, and maintenance of the Corridor Strategic Plan for data collection, corridor control, and performance metric calculation.
b. Determine if the Corridor Strategic Plan is complete and have it approved by the stakeholders.
c. Review changes to the corridor network, new technologies, and new governmental requirements in order to determine any appropriate changes to the Strategic Plan.
d. Resolve Strategic Plan deficiencies (with appropriate assistance).
e. Ensure the existence of assets and data defined in the Strategic Plan. This may involve purchasing or upgrading of assets and/or data.
2. Corridor Assets
a. Track anticipated changes to the ICM corridor's roadway network, including freeway ramps, arterial lanes, intersections, origin-destination centers.
b. Track anticipated changes to the ICM corridor's transit networks, including rail, express/commuter bus lines, local bus lines.

Responsibility
c. Track anticipated changes to the ICM corridor's traffic control devices (traffic signals, ramp meters, others).
d. Track required maintenance for traffic management devices.
e. Determine when and where traffic management devices would be needed to adequately support ICM system operations.
f. Track anticipated changes to the corridor's traveler information devices (CMS, extinguishable trailblazer signs, etc.).
g. Track required maintenance for traveler information devices.
h. Determine when and where traveler information devices would be needed to adequately support ICM system operations.
i. Track required changes to existing sensors and sensor locations.
j. Track required maintenance for sensors.
k. Determine when and where new sensors are needed to adequately support ICM system operations.
3. Response Plans
a. Track proposed response plan component additions and determine whether new or modified traffic management devices are needed to fulfill these additions.
b. Track proposed response plan component additions and determine whether new traveler information devices are needed to fulfill these additions.
c. Track proposed response plan component additions and determine sensing and data requirements needed to fulfill these additions.
4. Metrics
a. Track anticipated changes to the metrics that must be provided by the ICM system.
b. Track anticipated governmental requirements for collecting performance metrics.
c. Review the acceptability and usefulness of existing metrics and determine changes needed to the metrics produced.
5. Requirements
a. Determine requirements for new metrics, including the need for new or existing data, sensing, and algorithms.
b. Track proposed new or updated user requirements for the ICM system.
6. Organizations and Personnel
a. With the Outreach and Communications Manager, set up and maintain a Connected Corridors Steering Committee, Technical and Operational Advisory Committee, and other committees as needed.
b. Create and maintain a management-level organization chart of all project stakeholders.
c. Review current staff versus needed staff and work with stakeholders to resolve discrepancies.
d. Keep an up-to-date inventory of job descriptions related to the ICM operations.
e. Determine whether personnel in other corridor agencies shall be added to the list of ICM support personnel.
f. With the Outreach and Communications Manager, develop an organizational chart identifying communication contacts.
g. In coordination with the Outreach and Communications Manager, survey personnel and their managers to determine if personnel understand ICM and the cultural changes it requires.

Responsibility
h. In coordination with involved agencies, determine whether ICM support personnel at other agencies shall receive training on ICM operations.
7. Maintain a Risk Register, manage the risks defined in it, ensure it is discussed in the monthly meetings and/or conference calls, keep it up to date.
8. Establish quarterly meetings to keep all stakeholders updated on system and corridor activities.
9. Lead (or delegate a representative to lead) update meetings or teleconferences.
10. With the Outreach and Communications Manager, follow up on information requests about the ICM system. Forward requests to other stakeholders for comment or response when needed.
11. With the Outreach and Communications Manager, oversee the development of applications for funding, track the progress of submitted funding applications, and develop a tracking system to manage approved funding sources.
12. Determine which participating agencies need to review project documents and provide comments on them. Determine if other agencies need to review and comment.
13. Third-Party Relationships
a. In coordination with stakeholders, manage third-party relationships.
b. In coordination with stakeholders, develop a strategy for acquiring real-time and/or historical data from third-party probe data providers (INRIX, HERE, or others).
c. In coordination with stakeholders, develop a strategy to share data with Waze and other travel information providers.
d. In coordination with stakeholders, purchase or develop contracts related to third-party data.
e. In coordination with stakeholders, determine which functions shall be outsourced to contractors.
f. In coordination with stakeholders, develop and maintain contracts with contractors.
g. In coordination with stakeholders, draft contracts for providing data generated by the ICM Environment to third-party entities.
h. In coordination with stakeholders, maintain positive relationships with vendors and contractors.
i. Periodically review third-party purchasing choices and contracts.

3.2. CORRIDOR MONITORING

This function is tasked with determining the state of the corridor and using this state to accurately calculate and report corridor performance measures.

Responsibility
1. Work with Traffic Engineers to ensure that the definition of the transportation network is accurate and up to date in all locations within the ICM Core System, including the estimation and prediction functions, all rules referencing network configuration, user interface maps, network anomaly functions, metrics that may have constants based on network configuration.
2. Ensure any changes to designated reroutes around incidents or events are communicated to all system stakeholders.

3.3. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed and tested.

Responsibility
1. Lead incident/event response planning.
2. Determine the percentage of time that appropriate Traffic Engineers are present for response planning sessions; work with stakeholders to resolve attendance issues.
3. Determine and ensure rules exist.
a. Determine and ensure rules exist for incident detection.
b. Determine and ensure rules exist for incident severity.
c. Determine and ensure rules exist for zone of influence.
d. Determine and ensure rules exist for special situations.
e. Determine and ensure rules exist for building response plans from components.
f. Determine and ensure rules exist for selecting a response plan for implementation.
g. Determine and ensure rules exist for sending response plan instructions to corridor assets.
4. Ensure that stakeholders have identified and defined all response plan components needed to manage incidents and events; determine, with Traffic Engineers, the percentage of required response plan components that are defined and listed.
5. In consultation with all relevant stakeholders, determine the information to be sent to 511 services, HAR stations, and third-party providers as part of response plans.
6. Post-Incident/Event Review
a. Ensure that reports summarizing the results of the incident response plan and its effects on corridor performance are generated after each incident or event in the corridor for which a response plan was generated.
b. Conduct a post-incident analysis review with all affected agencies within one week of each significant event.
c. After each incident, unscheduled event, or planned event, in coordination with Traffic Engineers and other stakeholders, review the selected response plan components, including timing plans, and determine if any are missing, inappropriate, or need to be changed; update the component list as necessary.
d. As the transportation network changes, work with Traffic Engineers to update the list of response plan components.
7. Mock Incidents
a. With Traffic Engineers, determine the proper amount of testing needed for mock incidents and response plans, and ensure the testing takes place.
b. Ensure that Traffic Engineers create and run the mock incidents.
8. Quarterly Review
a. Conduct a quarterly review of the operational effectiveness of the ICM Environment.
b. As part of the quarterly effectiveness evaluation, assign a score to the observed effectiveness of response planning activities. Score corridor performance based on the ability of implemented response plans to reduce delay incurred by travelers within the corridor on a quarter-to-quarter and a year-to-year basis. Score the performance of the Decision Support module based on its ability to select plans that improve corridor response

Responsibility
to incidents and events. Support each published score evaluation with adequate field data.
c. Ensure quarterly stakeholder meetings occur to review/analyze response plan results in the corridor. Keep an updated list of who will attend. If meetings are not held or attendance is low, work with stakeholders and Corridor Champion(s) to determine and remedy the cause.
d. Use the results of the quarterly response plan analyses to influence corridor planning decisions.

3.4. REAL-TIME INCIDENT/EVENT MONITORING

Real-time Monitoring involves ensuring that incidents/events can be accurately detected, identified, and characterized, and that all proper personnel are notified.

Responsibility
1. Incident/Event Information
a. Determine the percentage of time stakeholders provide sufficient incident/event information (location, start time, type, severity, etc.) for the ICM Core System to fully characterize the incident/event.
b. Review all incidents and events and determine when data was not provided. Stakeholders, First Responders, and Public Information Officers must work together to resolve the issues.
2. With Traffic Engineers, review incident/event detection and determine if the system is working correctly.
3. Incident/Event Validation
a. Report the percentage of incidents and events that are validated (verified as actually existing) by stakeholders.
b. Ensure the validation process is working properly. If an incident or event is characterized but not validated, determine why and work with stakeholders to determine a remedy.
4. Incident/Event Characterization
a. Track the percentage of incidents or events that are not fully characterized but still result in the generation of a response plan.
b. Review such cases and work with Software Engineers to diagnose and fix the problem.
5. Stakeholder Notification
a. Determine the percentage of proper personnel notified that an incident or event has occurred.
b. Work with stakeholders to ensure the “who to contact” rule set is updated or that contact details are correct.
6. Updated Incident/Event Information
a. Determine when stakeholders did not provide updated information (such as end-of-incident network changes) to the ICM Core System during an incident/event.
b. Work with stakeholders to resolve issues; update processes as needed.
7. With Traffic Engineers, review all termination recommendations provided by the ICM system for errors; diagnose and resolve issues as needed.

3.5. REAL-TIME RESPONSE PLANNING

Real-time Response Planning requires ensuring that response plans generated by the ICM system are reasonable, accurate, and properly approved by appropriate personnel.

Responsibility
1. Response Plan Generation
a. With Traffic Engineers, determine the percentage of response plans that are correctly generated.
b. With Traffic Engineers, determine when response plans are not reasonable and why.
c. With Traffic Engineers, determine when prediction results are not correct.
d. Review the response plan the system recommends and see if the choice was accurate and based correctly on predefined rules. If not, review the rules and rules engine with Traffic Engineers.
2. Plan Review and Approval
a. Determine the percentage of appropriate stakeholders who reviewed and modified response plans. Determine when plans are not being reviewed and work with stakeholders to identify and resolve issues with the review process.
b. Along with stakeholders, note when approval rules are not followed and determine whether the problem is with the rules or the software; coordinate with Software Engineers to fix the problem.
c. Note the percentage of stakeholders who fulfill their role as approvers of the response plan. If problems exist with approvals, contact stakeholders to determine if the problem is one of human process, software, or rules. Depending on the problem, stakeholders, Software Engineers, or the Corridor Manager resolves the problems.
3. Plan Implementation
a. Note the percentage of time response plan implementation is correctly initiated.
b. Determine the percentage of times new response plans are generated during an incident or event; note when new response plans are not being generated.
c. As needed, command the ICM Core System to terminate a response planning activity.
4. Off-line Analysis
a. Determine the percentage of incident/event response plans that were able to be reviewed by stakeholders in off-line analysis.
b. Work with the Software Engineers, Data Analysts, and Database Administrator to identify and resolve possible issues.

3.6. RESPONSE PLAN IMPLEMENTATION

Implementing a response plan requires ensuring that instructions are sent correctly to corridor assets, keeping instructions current as assets change, notifying proper personnel, and tracking and resolving issues.

Responsibility
1. Instruction Order and Schedule

Responsibility
a. With Traffic Engineers, determine the percentage of time that the ICM Core System correctly identifies the assets to receive instructions and the proper order and times they should be sent.
b. With the Traffic Engineers, determine in post-incident/event analysis where issues arose with the asset status or instructions and/or response plan instructions; resolve issues.
c. As assets and equipment change over time, work with Traffic Engineers to modify the order and time assets receive instructions.
2. Stakeholder Notification
a. Determine the percentage of time proper personnel are notified of response plan deployment.
b. Work with stakeholders to ensure the "who to contact" rule set is updated.
3. Implementation Override
a. Determine percentage of time that the response plan is correctly canceled (due to changed circumstances in the corridor prior to implementation).
b. With Traffic Engineers, determine in post-incident/event analysis where plans were inappropriately implemented.
4. Sending Response Plan Instructions
a. Determine the percentage of time instructions are sent to assets (both ITS and human elements in the response plan).
b. With Traffic Engineers, determine in post-incident/event analysis where issues arose with sending instructions.
5. Instruction Verification
a. Determine percentage of time that the system verifies that assets have received instructions.
b. With Traffic Engineers, determine in post-incident/event analysis where issues arose.
6. Changes in Asset Status
a. Determine the percentage of time that changes in asset status have occurred while a response plan is in place, and stakeholders have been notified.
b. With Traffic Engineers, determine in post-incident/event analysis where status changes occurred and the proper processes were not followed.
7. Return to Normal Status
a. Determine percentage of time that assets return to normal status when an incident or event ends.
b. With Traffic Engineers, determine in post-incident/event analysis where assets did not return to normal status.
8. Historical Records
a. Determine the percentage of time that proper historical records of incidents/events and response plan implementation are saved and available for review.
b. With Traffic Engineers, note issues in post-incident/event analysis and determine why there was difficulty.

3.7. DATA MANAGEMENT

Data and data quality is at the heart of data-driven performance management. Data must be accurate, complete, timely, reliably available, stored safely, and communicated and presented consistently.

Responsibility	
1.	As part of the continuous improvement process, use data quality statistics and trends to improve system performance.
2.	Ensure adequate funding for the data quality management program and for funding and execution of any corrective actions required from data quality management actions.
3.	With the Corridor Data Analyst, conduct quarterly and annual reviews of the system data.
4.	With the Corridor Data Analyst, ensure that the quarterly and annual data review recommendations are funded and executed.

3.8. DECISION SUPPORT

Decision Support involves ensuring that the appropriate rules are captured by the rules engine.

Responsibility	
1.	With the Corridor Technical Manager, determine the percentage of desired rules that have been captured by the rules engine.
2.	Review rules during post-incident response plan analysis.
3.	During post-incident response plan review, determine if rules were not evaluated correctly by the rules engine.
4.	Periodically review the accuracy of the traffic state estimates and forecasts produced by the Decision Support System. At the start of ICM System operations, conduct a review every 2 weeks. Over time, as accuracy increases, review frequency can be spaced to no fewer than once every 3 months.
5.	Initiate comparisons between forecasted and field data for specific traffic forecasts as needed (for instance, traffic forecasts produced on a given day and time, or forecasts associated with a specific incident or event).

3.9. CORE SYSTEM USER INTERFACE

Stakeholders interact with the ICM Core System through software-based user interfaces. This includes providing stakeholders and, in particular, first responders with methods to easily exchange information during incidents.

Responsibility	
1.	Determine, through interviews, ease of information exchange.
2.	Observe communication during incidents and determine if communication issues exist. If so, work with stakeholders to resolve issues.

3.10. SYSTEM INTEGRATION

System Integration requires monitoring system functionality, data control, and asset ownership.

Responsibility	
1.	With the Corridor Technical Manager, track ownership of all corridor assets—including data definitions, algorithms, and workflows, as well as hardware and software systems—and determine the percentage of items that have owners (an individual or organization).
2.	If ownership of an asset is unclear, determine who will work with stakeholders to identify the owner.
3.	As assets change, ensure, with the Corridor Technical Manager, that each asset has an owner.

3.11. SYSTEM MANAGEMENT

System Management involves ensuring that the system is reliably operated and maintained.

Responsibility	
1.	Track the percentage of maintenance activities (both repair and preventative) that are properly reported by stakeholders.
2.	As part of maintaining system reliability, ensure that all sensing, measurement, and control devices used by the ICM Environment operate correctly at any given time, at the level specified in the service level agreement.
3.	With the Corridor Technical Manager, develop a training program for the ICM Environment and ICM Core System.
4.	With the Corridor Technical Manager, conduct quarterly and annual training program reviews and make any necessary changes in the training program.
5.	With the Corridor Technical Manager, review the initial ICM training plan and submit a new ICM training plan on an annual basis.

4. CORRIDOR TECHNICAL MANAGER

The Corridor Technical Manager ensures the software and hardware components of the ICM system are maintained, upgraded, and functioning. This role is linked primarily to the following areas of the System Requirements:

- Institutional Support
- Corridor Monitoring
- Strategic Incident/Event Response Planning
- Real-Time Incident/Event Monitoring
- Data Management
- Decision Support
- Core System User Interface
- System Integration
- System Management

4.1. INSTITUTIONAL SUPPORT

Institutional Support focuses on strategic planning and on how organizations and people are structured, funded, motivated, and informed in order to execute strategic plans.

Responsibility	
1.	With the Corridor Manager and Corridor Data Analyst, determine if the strategic plan is completed.
2.	With the Corridor Data Analyst, determine the percentage of required sensing assets, data sources, and performance metrics, as defined in the Strategic Plan, that are in place.
3.	With the Corridor Data Analyst, determine the most important missing assets or data and work with stakeholders to provide the missing items.

4.2. CORRIDOR MONITORING

This function is tasked with determining the state of the corridor and using this state to accurately calculate and report corridor performance measures.

Responsibility	
1.	To ensure that the real-time status of corridor assets (their health and availability) is available to all stakeholders, review and determine whether the status is available for all corridor assets (including the transportation network, ITS hardware elements, personnel, vehicles and signage, software and supporting servers, and communications).
2.	Work with Electrical Engineers and Software Engineers to determine the reason asset statuses are not available, and work to bring them back online.
3.	To ensure that the real-time state of corridor assets (the current configuration of information on devices, including signal plans, ramp metering plans, CMS messages) is available to all stakeholders, determine the percentage availability of asset state.

Responsibility
4. Work with Software Engineers and Electrical Engineers to determine the reason asset state is not available and resolve the issues.

4.3. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed, tested, and reported.

Responsibility
1. With the Corridor Manager, determine the percentage of required timing plans developed and deployed.
2. Conduct weekly and quarterly evaluations of the rules and their execution.
3. Determine the percentage of time that the ICM Core System is able to correctly build mock incidents and events.

4.4. REAL-TIME INCIDENT/EVENT MONITORING

Real-time Monitoring involves ensuring that incidents/events can be accurately detected, identified, and characterized, and that all proper personnel are notified.

Responsibility
1. Determine the percentage of time that the real-time response planning function is correctly initiated.

4.5. DATA MANAGEMENT

Data and data quality is at the heart of data-driven performance management. Data must be accurate, complete, timely, reliably available, stored safely, and communicated and presented consistently.

Responsibility
1. Data Quality
a. With the Corridor Data Analyst, develop a data quality management program for the ICM Environment to specify processes, procedures, responsibilities, metrics, and best practices for measuring, monitoring, and correcting data issues.
b. With the Corridor Data Analyst, develop a Data Quality Management Guide for the data quality management program.
2. Data Oversight
a. With the Corridor Data Analyst and representatives from stakeholders and data providers, serve on the Data Governance Board.
b. As part of the quarterly or annual data reviews, conduct a review with the Corridor Data

Responsibility
Analyst of data stored both in electronic and non-electronic formats, and its availability to users of the system.
3. Data Formats
a. With Data Analysts, determine the percentage of data stored in electronic format.
b. To ensure that all data, where possible, will be transmitted using TMDD/NTCIP/GTFS formats, work with Database Administrators and Software Engineers to identify when other data formats are being used and work to replace them.
4. With Database Administrators, determine the percentage of time ETL (Extract, Transform, Load) functionality—required for interfacing with external systems—can be used.
5. Determine the percentage of time requests from stakeholders for data additions, removals, or format changes are responded to promptly.
6. Data Policies
a. Develop and follow standards for data archiving, warehousing, and deletion.
b. With Database Administrators, determine the completeness of data management policies and the percentage of time policies are being followed.
c. Update the data management policies and methods as data changes and volumes grow.

4.6. DECISION SUPPORT

Decision Support involves ensuring that the appropriate rules are captured by the rules engine.

Responsibility
1. With the Corridor Manager, determine the percentage of desired rules that have been captured by the rules engine.
2. With Traffic Engineers, determine the percentage of the time rules are evaluated correctly by the rules engine.
3. Review the daily operational evaluation report generated by Decision Support at the end of each day providing a summary of the rules execution and details of the specific rules operation.

4.7. CORE SYSTEM USER INTERFACE

The ICM Core System includes software-based user interfaces for creating, viewing, updating, deleting, and reporting on data, as well as interfaces for managing the process of incident identification, response plan generation, response plan implementation, and Core System management.

Responsibility
1. Track UI functionality.
2. Note when interfaces are not working, displaying insufficient data, or presenting it incorrectly.
3. Determine when interfaces need to be changed or updated.
4. Work with Software Engineers and Database Administrators to diagnose and resolve issues.

4.8. SYSTEM INTEGRATION

System Integration requires monitoring system functionality, data control, and asset ownership.

Responsibility
1. Monitor the percentage of functions, including visualization and reporting functions, accessible through one integrated system.
2. Track functionality, note issues, and work with Software Engineers and other personnel as needed to diagnose and resolve issues.
3. With the Corridor Manager, track ownership of all corridor assets—including data definitions, algorithms, and workflows, as well as hardware and software systems—and determine the percentage of items that have owners (an individual or organization).
4. As assets change, ensure, with the Corridor Manager, that each asset has an owner.

4.9. SYSTEM MANAGEMENT

System Management involves ensuring that the system is reliably operated and maintained. This includes the areas of security, service level agreements, maintenance, training, system recovery, and upgrades.

Responsibility
1. Security
a. Following industry standards, develop and implement security protocols and processes to ensure secure operations of the ICM Environment.
b. Ensure only authorized personnel can access system assets.
c. Designate an IT Security Officer for the ICM Environment who shall have responsibility for the security of the ICM Environment and its operations.
2. Service Level
a. Develop and maintain a service level agreement, in coordination with stakeholders.
b. To ensure the system is available and functioning an agreed-upon percentage of the time, review system logs and up-time reports to determine problems and help resolve issues.
c. Determine the percentage of system activity logs that are properly maintained. With Software Engineers, ensure that any new functionality is attached to viewable logs.
3. System Maintenance
a. Specify the frequency of system backups.
b. Monitor the percentage of time that requests for maintenance, improvements, and bug fixes are properly entered into the tracking system. With Software Engineers, perform normal maintenance on the tracking system.
c. Develop and maintain a list of critical elements that should receive maintenance priority should they fail.
d. Track assets undergoing maintenance (both repair and preventative) by stakeholders; help resolve issues.
e. Note when maintenance reporting is not occurring and work with stakeholders to resolve

Responsibility
any problems.
f. Validate non-catastrophic software bugs reported by stakeholders; ensure Software Engineers are available to fix bugs.
4. Training
a. With the Corridor Manager, develop a training program for the ICM Environment and ICM Core System.
b. With the Corridor Manager, conduct quarterly and annual training program reviews and make any necessary changes in the training program.
c. With the Corridor Manager, review the initial ICM training plan and submit a new ICM training plan on an annual basis.
d. Note if individuals do not know how to perform their functions, operate software/hardware systems, or are not aware of proper procedures due to lack of or inadequate training or documentation. Work with stakeholders to address issues.
5. System Recovery
a. Ensure the ICM Core System can recover from critical failures or disasters.
b. Develop a System Recovery Plan, in coordination with stakeholders; review it quarterly and test it annually.
c. Work with stakeholders to resolve disaster preparedness issues.
6. Software Updates
a. Designate a software development and update process, based on industry standards, for software updates and bug fixes.
b. Develop a schedule for software development updates and bug fixes, and maintain the schedule, providing updates to the schedule on a monthly basis.
c. Develop an annual budget for software updates and bug fixes, with quarterly updates.
d. Produce an annual report of system software maintenance, providing a year in review of the previous year and a plan for the coming year of software maintenance and bug fix activities, schedule, and budget.
7. System Upgrades
a. In concert with corridor stakeholders, develop and maintain a 5-year system upgrade plan.
b. Ensure the plan is adequate and approved by stakeholders.
c. Create an annual upgrade plan that identifies the system upgrades from the 5-year plan that will be implemented within the next year. Deliver the annual upgrade plan a minimum of six months prior to the fiscal year start.
d. Develop a system of governance to ensure each proposed system upgrade receives the appropriate priority and reflects the needs of all corridor stakeholders.
e. Ensure system upgrades are developed, delivered, and implemented according to the budget and planning identified in the annual upgrade plan.
f. Provide updates to the 5-year and annual upgrade plans when changes are identified and approved according to the governance system of the corridor.
g. Manage and implement system upgrades in accordance with the industry standards appropriate to the specific upgrade elements.

5. CORRIDOR DATA ANALYST

Corridor Data Analyst is an extremely important role. It has responsibility for ensuring data quality within the ICM environment by analyzing corridor data, setting quality standards, ensuring data meets those standards, identifying when it does not, and working with stakeholders to meet their data analysis needs. Overall, Connected Corridors and ICM in general are about using data to manage corridor performance. ICM requires quality data, well-defined performance measures, and correct metric calculations—all areas that the Corridor Data Analyst is responsible for.

Data Management requires both a purely technical component (i.e., does the database work, does the communication from the sensors work, etc.) and a definitional and analysis component. The definitional and analysis component is the responsibility of the Corridor Data Analyst. The technical components are shared with the Corridor Technical Manager, database administrators, and software and hardware engineers. The managerial requirements are shared with the Corridor Manager. A number of the following requirements are shared with those other roles, but the Corridor Data Analyst is primarily responsible for overall data management. Thus, those other roles are not listed in the following responsibilities unless of particular importance.

This role is linked primarily to the following areas of the System Requirements:

- Institutional Support
- Corridor Monitoring
- Data Management
- System Integration

5.1. INSTITUTIONAL SUPPORT

Institutional Support focuses on strategic planning and on how organizations and people are structured, funded, motivated, and informed in order to execute strategic plans.

Responsibility
1. Determine the percentage of required sensing assets, data sources, and performance metrics, as defined in the Corridor Strategic Plan, that are in place.
2. Determine the most important missing assets or data and work with stakeholders to provide the missing items.

5.2. CORRIDOR MONITORING

This function is tasked with determining the state of the corridor and using this state to accurately calculate and report corridor performance measures.

Responsibility
1. Determine the percentage of time the system makes high-quality traffic monitoring data available to all stakeholders (e.g., freeway counts/flows, arterial through/turning counts,

bus/train locations, video data, etc.).
2. Determine when traffic monitoring data quality has degraded and when data is not available.

5.3. DATA MANAGEMENT

Data and data quality is at the heart of data-driven performance management. Data must be accurate, complete, timely, reliably available, stored safely, and communicated and presented consistently.

Responsibility
1. Governance
a. Develop a data quality management program for the ICM Environment.
b. Develop a Data Quality Management Guide for the data quality management program.
c. With the Corridor Technical Manager and representatives from stakeholders and data providers, serve on the Data Governance Board.
2. Definition
a. Ensure that the data dictionary is complete, accurate, and up to date.
b. Define and maintain data quality requirements and the methods for calculating the quality.
3. Application of Standards
a. Determine the percentage of data that has appropriate quality metrics.
b. Ensure that all data has a data quality specification.
c. Determine if data quality is being maintained.
d. Ensure that data is meeting data quality specifications at all times.
e. Ensure that processes (both automated and human) are in place and in use for ensuring and measuring the quality of data and for addressing data quality issues when they arise.
f. Ensure that the following metrics are established, measured, and met for all data: • maximum time to detect errors or problems with data quality • maximum time to correct errors or problems • mean time to detect errors or problems • mean time to correct errors or problems
g. Update specifications and calculation methods as data sources and formats change.
h. As data and personnel change, ensure that data quality measurement procedures are in place and that Data Analysts are available and trained.
4. Reviews
a. Conduct a weekly corridor data review, using data quality metrics specified in the Data Dictionary.
b. Conduct a quarterly data quality assessment for all ICM Environment data elements and sources.

Responsibility
c. Conduct quarterly and annual reviews of system data, including: • Measures of the data quality for the quarter and year • Status of the data dictionary • A change management review of the system data sources, data processes, data hub, and externally available data elements • Data management system performance • Recommended actions to improve data, data processes, and data quality
d. Conduct an annual review of data quality metrics definition and calculation method.
e. With the Corridor Manager, ensure that the quarterly and annual data assessment and review recommendations are funded and executed.
f. As part of the quarterly or annual data reviews, conduct a review of data stored both in electronic and non-electronic formats, and its availability to users of the system.
5. Day to Day
a. Measure and report on mean time between failure for all data quality metrics.
b. Promptly report all identified data quality failures to the Corridor Manager and stakeholders.
c. Report on the status of corrections being executed to address data quality failures. This includes reporting on the time needed to perform the correction.
d. Initiate any actions required to address issues identified, either during system operation or as a result of the weekly review.
e. Identify problems and work with stakeholders and third-party providers to refine and update the data quality requirements and calculation methods.
f. Analyze stakeholder requests for data additions, removals, or format changes and determine whether the request can be accommodated by resources and will enhance the ICM function. If requests are appropriate, ensure the maintenance is performed.

5.4. SYSTEM INTEGRATION

System Integration requires monitoring system functionality, data control, and asset ownership.

Responsibility
1. Determine the percentage of appropriate data that use a common set of data definitions, are processed and managed consistently across all ICM components, and are presented to users consistently across all ICM Core System components.
2. Note when integration/consistency standards are not being followed and resolve the problems.
3. Determine the percentage of data that have one and only one system/access protocol of record. Identify and resolve issues.

6. TRAFFIC ENGINEERS

Traffic Engineers fill an essential role in the ICM process. They provide the knowledge required for creating and maintaining the response plans, rules, networks, and models contained in the Decision Support System. They are also responsible for reviewing the results of the application of response plans to incidents and determining if the response plans worked as expected.

A number of the following requirements are shared with other roles, but if the tasks will be performed primarily by Traffic Engineers, those other roles are not listed unless of particular importance in carrying out the responsibilities.

This role is linked primarily to the following areas of the System Requirements:

- Corridor Monitoring
- Strategic Incident/Event Response Planning
- Real-Time Incident/Event Monitoring
- Real-Time Response Planning
- Response Plan Implementation
- Decision Support

6.1. CORRIDOR MONITORING

This function is tasked with determining the state of the corridor and using this state to accurately calculate and report corridor performance measures.

Responsibility
1. Network Definition
a. Work with the Corridor Manager to ensure that the transportation network is well defined in the ICM system and up to date.
b. Check for issues with the accuracy of response plan predictions. If discrepancies are found, correct the network definitions as needed.
2. Performance Metrics
a. With Data Analysts, determine the percentage of time metrics are calculated correctly.
b. Work with Data Analysts and Software Engineers to uncover any issues with performance metric calculations.
c. As new data sources/sensors become available, work with Data Analysts and Software Engineers to update the metric calculation algorithms.
3. Corridor State Determination
a. Determine the accuracy of the results of the DSS Corridor State Determination function. Use observation, statistical analysis, and periodic external evaluations to identify inaccuracies.
b. As the network and data sources change, work with Software Engineers to adjust the algorithms and rules that perform the corridor state determination.
4. Historical Data

Responsibility
a. With Data Analysts, determine the accuracy of historical traffic patterns, using observation and statistical analysis. Work with Software Engineers to resolve issues.
b. As new data sources/sensors and new algorithms become available, work with Data Analysts and Software Engineers to maintain and upgrade the algorithms used to create historical data.

6.2. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed, tested, and reported.

Responsibility
1. Participate in developing response plans.
2. Response Plan Components
a. Determine desired routes to be used as detours for incidents and events.
b. As needed, define the preferred detours to be considered as first potential solutions in building response plans.
c. As needed, define temporary restrictions on the use of specific roadway segments in response plans.
d. Determine the signalized intersections whose traffic signal timing plans may be changed during an incident or event.
e. Determine which freeway ramps shall have their metering rate changed during an incident or event.
f. Create, maintain, and test traffic signal timing plans, and distribute them to the devices in the response plan component list.
g. As traffic conditions change, update and reverify the signal timing plans.
h. Create, maintain, and test ramp metering plans, and distribute them to the devices in the response plan component list.
i. Determine messaging equipment available for use during an incident or event (HAR, fixed CMSs, portable CMSs, extinguishable trailblazer signs, others).
j. Define a minimal percentage of control devices (traffic signals, ramp meters, changeable message signs) that should be available along a detour routes for the route to be considered viable.
k. Determine what vehicles are available for use to implement a response to an incident or event.
l. Determine personnel available for deployment during an incident or event.
m. Determine typical information to be sent to agency personnel responding to an incident or event.
n. Determine messages to be posted on fixed and/or portable CMS devices when responding to an incident or event.
o. With the Corridor Manager, determine the percentage of required response plan components that have been defined and listed.
3. Response Plan Rule Creation

Responsibility
a. Define the rules (metrics and the value of those metrics) to be used in determining the existence of an incident.
b. Define the rules to be used in determining the severity of an incident or event and its zone of influence.
c. Define the rules for assessing the level of impact of an incident or event on corridor operations.
d. Define the rules for building response plans from a set of possible response actions.
e. Define the rules for handling special situations.
f. Define the rules for selecting a recommended response plan among a set of alternate plans.
g. Define the rules for sending response plan instructions to corridor assets.
h. Define the rules for determining agency personnel who should be notified of a response planning action.
i. Specify the conditions under which the implementation of an approved response plan can be canceled.
4. Rule and Component Evaluation
a. Review the incident detection rules to determine if the application of the rules resulted in the correct identification of an incident and, if not, determine where the error lies. Correct any inaccurate rules.
b. Review the rules to determine if the application of the rules resulted in the correct severity and zone of influence determination and, if not, determine where the error lies. Correct any inaccurate rules.
c. Review the special situation rules applied during incidents or events to determine if their application resulted in the correct response plan component selection. If inaccurate, update the rules.
d. During incidents or events, review the rules for building response plans from components to determine if the application of the rules resulted in the generation of appropriate response plans. Correct any inaccurate rules.
e. Review the response plans selected during incidents or events to determine if the rules for selecting a plan resulted in the correct selections. Correct any inaccurate rules.
f. Review the execution order of instructions sent to corridor assets to determine if the rules for choosing the order/schedule resulted in the correct ordering. Correct any inaccurate rules.
g. As the corridor changes, review and update the rules.
h. After each incident, unscheduled event, or planned event, in coordination with the Corridor Manager and other stakeholders, review the selected response plan components and determine if any are missing or inappropriate; update the component list as necessary.
i. As the transportation network changes, work with the Corridor Manager to update the list of response plan components.
j. After each incident, unscheduled event, or planned event, work with the Corridor Manager to review the timing plans to determine any changes needed. Make the changes.
5. Testing
a. Create mock incidents and events and review the resulting response plans; run the response plans through the prediction system; analyze the results to determine the likely effectiveness of the plans.

Responsibility
b. With the Corridor Manager, determine the proper amount of testing needed for the mock incidents and response plans, and ensure the testing takes place.
c. With Software Engineers, Data Analysts, and Database Administrators, identify problems and resolve issues related to the mock incidents and events.

6.3. REAL-TIME INCIDENT/EVENT MONITORING

Real-time Monitoring involves ensuring that incidents/events can be accurately detected, identified, and characterized, and that all proper personnel are notified.

Responsibility
1. Determine the percentage of time the ICM software properly identifies incidents.
2. With the Corridor Manager, review incident/event detection and determine if the system is working correctly.
3. With Software Engineers, tune incident detection algorithms and rules.
4. With the Corridor Manager, review the system's incident/event termination recommendations for errors; resolve issues.

6.4. REAL-TIME RESPONSE PLANNING

Real-time Response Planning requires ensuring that response plans generated by the ICM system are reasonable, accurate, and properly approved by appropriate personnel.

Responsibility
1. With the Corridor Manager, determine through observation and analysis the percentage of response plans that are correctly generated.
2. With the Corridor Manager, determine when response plans are not reasonable and why.
3. With the Corridor Manager, determine when prediction results are not correct.
4. If the system chooses an inaccurate response plan, work with the Corridor Manager to review the rules and rules engine.

6.5. RESPONSE PLAN IMPLEMENTATION

Implementing a response plan requires ensuring that instructions are sent correctly to corridor assets, keeping instructions current as assets change, notifying proper personnel, and tracking and resolving issues.

Responsibility
1. Determine the percentage of time that instructions for response plan implementation are sent in

Responsibility
the correct order and schedule.
2. Determine in post-incident/event analysis where issues related to order and time arose; resolve issues.
3. As assets and equipment change, work with the Corridor Manager to modify the order and time they receive instructions, as needed.
4. Determine in post-incident/event analysis where response plans were inappropriately implemented; update rules to resolve issues.
5. As corridor assets change, update the rules as needed.
6. Determine in post-incident/event analysis where issues arose with sending instructions to corridor assets (both ITS and human elements in the response plan) and verifying that instructions were received.
7. Determine in post-incident/event analysis where issues arose with the system monitoring, and assets communicating, any changes in status and notifying stakeholders of the changes while a response plan is in place.
8. Determine in post-incident/event analysis where assets did not return to normal status when an incident or event ends.
9. Note in post-incident/event analysis where the ICM system did not save all information relevant to response plan implementation; determine why.

6.6. DECISION SUPPORT

Decision Support involves ensuring that the appropriate rules are captured by the rules engine.

Responsibility
1. With Corridor Technical Manager, determine the percentage of time the rules are evaluated correctly.
2. Using observation, measurement, and statistical analysis, assess whether the corridor state determination results are correct.
3. With Software Engineers, update and maintain the algorithms and data used to determine corridor state based on changes in the corridor.
4. Using observation, measurement, and statistical analysis, assess whether the future corridor state prediction results are correct.
5. With Software Engineers, use modeling skills to update and maintain the algorithms and data used to predict corridor state based on changes in the corridor.
6. Using observation, measurement, and statistical analysis, assess whether the system is correctly determining if traffic is within normal variability for a given date and time.

7. DATA ANALYSTS

Data Analysts are responsible for day-to-day implementation of the data quality standards, ongoing review of ICM environment data quality, and initiation of corrective actions.

This role is linked primarily to the following areas of the System Requirements:

- Corridor Monitoring
- Strategic Incident/Event Response Planning
- Real-Time Response Planning
- Data Management
- System Integration

7.1. CORRIDOR MONITORING

This function is tasked with determining the state of the corridor and using this state to accurately calculate and report corridor performance measures.

Responsibility
1. Performance Metrics
a. With Traffic Engineers, determine the percentage of time performance metrics are calculated correctly.
b. Watch for unusual metrics and work with Traffic Engineers and Software Engineers to uncover any issues.
c. As new data sources and sensor types become available, work with Traffic Engineers and Software Engineers to update the metric calculation algorithms.
2. Historical Data
a. With Traffic Engineers, use observation and statistical analysis to determine the accuracy of historical patterns.
b. As new data sources/sensors and new algorithms become available, work with Traffic Engineers and Software Engineers to maintain and upgrade the algorithms used to create historical data.

7.2. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed, tested, and reported.

Responsibility
1. Diagnose and resolve issues with executing response plan rules for incident detection, severity, zone of influence, special situations, building response plans, choosing a plan to implement, and sending plan instructions to corridor assets.
2. With Traffic Engineers, Software Engineers, and Database Administrators, identify and resolve

Responsibility
issues related to creating and executing mock incidents and events.
3. With Software Engineers and Database Administrators, resolve problems in the generation of after-incident/event reports.

7.3. REAL-TIME RESPONSE PLANNING

Real-time Response Planning requires ensuring that response plans generated by the ICM system are reasonable, accurate, and properly approved by appropriate personnel.

Responsibility
1. Work with Corridor Manager, Software Engineers, and Database Administrators to identify and resolve issues with incident/event response plans being able to be reviewed and analyzed by stakeholders off-line.

7.4. DATA MANAGEMENT

Data and data quality is at the heart of data-driven performance management. Data must be accurate, complete, timely, reliably available, stored safely, and communicated and presented consistently.

Responsibility
1. With Database Administrators, assist the Corridor Data Analyst in maintaining the Data Dictionary, ensuring that it is accurate and up to date.
2. With Database Administrators, note any discrepancies between the Data Dictionary and the actual data and resolve them.
3. Review the quality of data and determine the reasons for any deviations from data quality requirements.
4. Assist the Corridor Technical Manager with determining the percentage of data stored in electronic format.
5. Note when data is not being stored in electronic format and work with stakeholders, Software Engineers, and Database Administrators to store the data.
6. As data types and formats change over time, work with stakeholders, Software Engineers, and Database Administrators to ensure that storage methods are up to date.
7. With Database Administrators, ensure ETL (Extract, Transform, and Load) operations continue to work when external data formats change.
8. Review requests from stakeholders for data additions, removals, or format changes; determine the appropriateness of the changes.

7.5. SYSTEM INTEGRATION

System Integration requires monitoring system functionality, data control, and asset ownership.

Responsibility
1. Continually watch for copies of data that are being erroneously used as systems of record. Work with the Corridor Data Analyst, Software Engineers, and Database Administrators to identify and resolve issues.

8. SOFTWARE ENGINEERS

Software Engineers investigate and remedy software-related problems ("bugs") and provide upgrades as required. A significant and essential percentage of the requirements for the ICM Core System are implemented using software. It is impossible to maintain a nimble system capable of responding to changes in the corridor, new data, new requirements, and the general needs of the core system without utilizing software engineering expertise. In addition, all software has bugs, and these bugs must be fixed in a timely way.

This role is linked primarily to the following areas of the System Requirements:

- Corridor Monitoring
- Strategic Incident/Event Response Planning
- Real-Time Incident/Event Monitoring
- Real-Time Response Planning
- Response Plan Implementation
- Data Management
- Decision Support
- Core System User Interface
- System Integration
- System Management

8.1. CORRIDOR MONITORING

This function is tasked with determining the state of the corridor and using this state to accurately calculate and report corridor performance measures.

Responsibility	
1.	With the Corridor Technical Manager and Electrical Engineers, determine the reason asset statuses are not available and work to bring them back online.
2.	Where asset status is provided through automation, work with Electrical Engineers to ensure status is available.
3.	With Electrical Engineers, determine the reason asset state (the current configuration of information on devices, including signal plans, ramp metering plans, CMS messages) is not available and resolve the issue.
4.	With Electrical Engineers, maintain software and hardware.
5.	Work with Data Analysts and Traffic Engineers to uncover any issues with performance metric calculations.
6.	As new data sources/sensors become available, work with Data Analysts and Traffic Engineers to update the metric calculation algorithms.
7.	As the network and data sources change, work with Traffic Engineers to adjust the algorithms and rules that perform the corridor state determination.
8.	Work with Traffic Engineers to resolve issues with the accuracy of historical patterns.
9.	As new data sources/sensors and new algorithms become available, work with Data Analysts and Traffic Engineers to maintain and upgrade the algorithms used to create historical data.

8.2. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed, tested, and reported.

Responsibility
1. Diagnose and resolve issues with executing response plan rules for incident detection, severity, zone of influence, special situations, building response plans, choosing a plan to implement, and sending plan instructions to corridor assets.
2. Diagnose and fix the problems with the building of mock incidents or events used in testing response plans.
3. With Traffic Engineers, Data Analysts, and Database Administrators, identify and resolve issues related to creating and executing mock incidents and events.
4. With Data Analysts and Database Administrators, resolve problems in the generation of after-incident or after-event reports.
5. Upgrade and maintain after-incident/event reports.

8.3. REAL-TIME INCIDENT/EVENT MONITORING

Real-time Monitoring involves ensuring that incidents/events can be accurately detected, identified, and characterized, and that all proper personnel are notified.

Responsibility
1. With Traffic Engineers, tune the algorithms and rules used to identify potential incidents.
2. Work with the Corridor Manager to diagnose and resolve problems where the ICM system generated a response plan without a fully characterized incident or event.
3. Determine why the response planning function was not initiated once an incident/event was characterized; resolve the problem.

8.4. REAL-TIME RESPONSE PLANNING

Real-time Response Planning requires ensuring that response plans generated by the ICM system are reasonable, accurate, and properly approved by appropriate personnel.

Responsibility
1. Ensure changes in rules and data are properly handled by the response plan building function.
2. Resolve software issues with the generation, evaluation, and recommendation of response plans.
3. Resolve problems where the response plan approval process is not followed by the ICM system or stakeholders because of software issues.
4. Determine why response plan implementation was not properly initiated and resolve the issues.
5. Track down and resolve issues with the system not periodically generating new response plans while traffic conditions warrant.

Responsibility
6. Work with the Corridor Manager, Data Analysts, and Database Administrators to identify and resolve issues where incident/event response plans are unable to be reviewed and analyzed by stakeholders off-line.

8.5. RESPONSE PLAN IMPLEMENTATION

Implementing a response plan requires ensuring that instructions are sent correctly to corridor assets, keeping instructions current as assets change, notifying proper personnel, and tracking and resolving issues.

Responsibility
1. As assets and equipment change, modify the way instructions are sent to hardware and software assets, as needed.
2. As assets and equipment change, update the software to ensure and verify that assets have received instructions.
3. As corridor assets and policies change, update software as needed to ensure assets return to normal status when an incident or event ends.
4. With Database Administrators, resolve issues where the ICM system did not save information relevant to response plan implementation.
5. As new data is used, work with Database Administrators to update the ICM Core System software as needed.

8.6. DATA MANAGEMENT

Data and data quality is at the heart of data-driven performance management. Data must be accurate, complete, timely, reliably available, stored safely, and communicated and presented consistently.

Responsibility
1. Work with stakeholders, Data Analysts, and Database Administrators to store data in electronic format.
2. As data types and data formats change over time, work with stakeholders, Data Analysts, and Database Administrators to ensure that the data is stored correctly.
3. With Database Administrators, determine the percentage of time that data is transmitted using TMDD/NTIP/GTFS (data) format, the preferred standard for the ICM system. With Database Administrators and the Corridor Technical Manager, identify when other data formats are being used and work to replace them with the preferred format.
4. As the TMDD/NTCIP/GTFS (data) specification is updated, work with Database Administrators to modify the system to stay in compliance.
5. With Database Administrators, fulfill stakeholder requests for data additions, removals, or format changes.

8.7. DECISION SUPPORT

Decision Support involves ensuring that the appropriate rules are captured by the rules engine.

Responsibility
1. With Database Administrators, perform normal maintenance of the rules system, taking note of and discussing the existence of rules that have not been used for a long period of time.
2. Fix problems with the rules engine not evaluating rules correctly.
3. As new data and new rules are required, update the rules engine as needed.
4. As the corridor changes, work with Traffic Engineers as needed to update and maintain the algorithms and data used to determine and predict corridor state.
5. With Database Administrators, perform ongoing maintenance to ensure the system accurately determines if traffic is within normal variability for a given date and time.

8.8. CORE SYSTEM USER INTERFACE

The ICM Core System includes software-based user interfaces for creating, viewing, updating, deleting, and reporting on data, as well as interfaces for managing the process of incident identification, response plan generation, response plan implementation, and Core System management.

Responsibility
1. Asset Information
a. With Database Administrators, resolve issues with user interfaces for managing asset information, including: • Asset inventory • Asset health • Asset availability • Asset state
b. Maintain the interfaces.
2. Incident/Event Information
a. With Database Administrators, resolve issues with user interfaces for managing incident/event information, including: • Type of incident/event • Time of occurrence • Expected duration • Roadway/transit segment where occurred • Location along roadway/transit segment • Lane(s) affected • Agency responsible for managing incident/event • Verification status of incident/event • User confirmation interface
b. Maintain the interfaces.
3. Mock Incidents

Responsibility
a. As needed, modify the user interfaces for creating mock incidents, including: • Creating, viewing, updating, and deleting mock incidents • Map-based interface for choosing incident location • Setting the start/end times, duration, lanes/routes/tracks affected
b. As needed, modify the user interfaces for testing mock incidents, including: • Submission of mock incidents to the Decision Support module for testing • Map display of the response plan elements recommended for a mock incident • Generation of a post-incident report for a mock incident
4. Response Plans
a. As needed, modify the user interfaces for managing response plans, including: • Viewing response plans (triggering event, agencies involved, reroutes, control assets, messaging, personnel, constraints) • Managing Decision Support rules (creating, testing, visualizing) • Setting preferences • Selecting/approving a plan • Implementing a plan • Confirming incident/event termination • Notifying stakeholders
b. Update the interfaces as new features are added.
5. ICM Core System
a. As needed, modify the user interfaces for managing the ICM Core System, including: • Viewing all log activity • Customizing ICM Environment operations (system configuration, user adminstration, user preferences) • Starting and shutting down Core System components
b. Update the interfaces as new features are added.
6. Geospatial visualization
a. With Database Administrators, resolve problems with map-based visualization of data, including: • Viewing (corridor characteristics, roadway geometry, sensing/control assets, operational status, incidents/events, response plan elements) • Accessing information from map displays (roadway details, device configuration, video feeds, traffic state, incident/event details) • Layering of display elements • Customizing (user selection/customization of display and content, saved user preferences) • Managing (user interaction with ICM system from map displays to modify of asset usage and state, verify incidents, select/approve response plans)
b. Update the user interfaces as data and data presentation needs change and bugs are found.
7. Reporting, Charting, and Graphing
a. With Database Administrators, resolve problems with reporting, charting, and graphing functions, including: • Standard and customized reporting (creating/saving, scheduled/on-demand, printed/on-screen)

Responsibility
• Summary reports (roadway elements, sensing/control devices, response planning, system performance) • Plot-based visualizations (2d, 3d, heat map) • Graphing displays (org charts, decision trees, flow charts, pie/line/bar/histogram charts) • Tables • User queries
b. Update the user interfaces as data and data presentation needs change and bugs are found.
8. Post- incident/event reports
a. With the Corridor Technical Manager, diagnose and resolve issues when post-incident/event analysis reports are not generated.
b. Update the reports as new features are added.
9. Software System
a. As the system undergoes planned modifications, work with Database Administrators to maintain the central interface for managing software system parameters.

8.9. SYSTEM INTEGRATION

System Integration requires monitoring system functionality, data control, and asset ownership.

Responsibility
1. Ensure the system provides a single user interface for visualization and reporting and for Core System control functions. Keep the system in compliance with these standards as new features are added, bugs are fixed, etc.
2. With the Corridor Data Analyst and Database Administrators, resolve problems when standards are not followed for integrated data definition, capture, processing, and presentation.
3. As data needs change and bugs are found, work with Database Administrators to update the user and programming interfaces.
4. Work with the Corridor Data Analyst, Data Analysts, and Database Administrators to identify and resolve issues where copies of data are being erroneously used as systems of record.

8.10. SYSTEM MANAGEMENT

System Management involves ensuring that the system is reliably operated and maintained. This includes the areas of security, service level agreements, maintenance, training, system recovery, and upgrades.

Responsibility
1. Resolve issues with inaccurate or missing logging activity. Ensure new functionality is attached to viewable logs.
2. Resolve issues with the tracking system used for maintenance requests, improvement requests,

Responsibility
and bug fix requests. With the Corridor Technical Manager, perform normal system maintenance.
3. Fix software bugs as needed.

9. ELECTRICAL ENGINEERS

Electrical Engineers are responsible for investigating and remedying hardware- and communication-related problems and for installing upgrades as required.

9.1. CORRIDOR MONITORING

This function is tasked with determining the state of the corridor and using this state to accurately calculate and report corridor performance measures.

Responsibility	
1.	With the Corridor Technical Manager and Software Engineers, determine the reason asset statuses are not available and work to bring them back online.
2.	Where asset status is provided through automation, work with Software Engineers to ensure status is available.
3.	With Software Engineers, determine the reason asset state (the current configuration of information on devices, including signal plans, ramp metering plans, CMS messages) is not available and resolve the issue.
4.	With Software Engineers, maintain software and hardware.

10. DATABASE ADMINISTRATORS

Database Administrators ensure access to and proper storage of all corridor data.

This role is linked primarily to the following areas of the System Requirements:

- Strategic Incident/Event Response Planning
- Real-Time Response Planning
- Response Plan Implementation
- Data Management
- Decision Support
- Core System User Interface
- System Integration

10.1. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed, tested, and reported.

Responsibility
1. With Traffic Engineers, Software Engineers, and Data Analysts, identify and resolve issues related to creating and executing mock incidents and events.
2. With Software Engineers and Data Analysts, resolve problems in the generation of after-incident/event reports.
3. With Software Engineers, upgrade and maintain after-incident or after-event reports as their format and content change over time.

10.2. REAL-TIME RESPONSE PLANNING

Real-time Response Planning requires ensuring that response plans generated by the ICM system are reasonable, accurate, and properly approved by appropriate personnel.

Responsibility
1. Work with Corridor Manager, Software Engineers, and Data Analysts to identify and resolve possible issues with incident/event response plans being able to be reviewed and analyzed by stakeholders off-line.

10.3. RESPONSE PLAN IMPLEMENTATION

Implementing a response plan requires ensuring that instructions are sent correctly to corridor assets, keeping instructions current as assets change, notifying proper personnel, and tracking and resolving issues.

Responsibility
1. With Software Engineers, resolve issues where the ICM system did not save information relevant to response plan implementation.
2. As new data is used, work with Software Engineers to update the ICM Core System as needed to ensure all relevant data is saved for post-incident analysis.

10.4. DATA MANAGEMENT

Data and data quality is at the heart of data-driven performance management. Data must be accurate, complete, timely, reliably available, stored safely, and communicated and presented consistently.

Responsibility
1. Data Dictionary
a. With Data Analysts, assist the Corridor Data Analyst in maintaining the Data Dictionary, ensuring that it is accurate and up to date.
b. With Data Analysts, note any discrepancies between the Data Dictionary and the actual data and resolve them.
2. Data Storage
a. Work with stakeholders, Software Engineers, and Data Analysts to store data in electronic format.
b. As data types and formats change over time, work with stakeholders, Software Engineers, and Data Analysts to ensure that storage methods are up to date.
3. Data Formats
a. With Software Engineers, determine the percentage of time that data is transmitted using TMDD/NTIP/GTFS (data) format.
b. With Software Engineers and the Corridor Technical Manager, identify when other data formats are being used and work to replace them.
c. With Software Engineers, as the TMDD/NTCIP/GTFS (data) specification is updated, modify the system to stay in compliance.
4. ETL (Extract, Transform, and Load)
a. Assist with using ETL (Extract, Transform, and Load) for interfacing with external systems.
b. With the Corridor Technical Manager, determine the percentage of time ETL-provided functions can be used.
c. With Data Analysts, ensure ETL operations continue to work when external data formats change. Perform continual maintenance, as external and internal formats may change at any time.
5. With Software Engineers, fulfill stakeholder requests for data additions, removals, or format

Responsibility
changes.
6. Review and determine the percentage of time that state-of-the-art technologies are used to store, access, and select data, and queries executed with appropriate response times.
7. Review query logs to determine when performance is not meeting requirements; resolve issues.
8. With the Corridor Technical Manager, determine the completeness of data management policies and the percentage of time policies are being followed.

10.5. DECISION SUPPORT

Decision Support involves ensuring that the appropriate rules are captured by the rules engine.

Responsibility
1. With Software Engineers, perform normal maintenance of the rules system, taking note of and discussing the existence of rules that have not been used for a long period of time.
2. With Software Engineers, perform ongoing maintenance to ensure the system accurately determines if traffic is within normal variability for a given date and time.

10.6. CORE SYSTEM USER INTERFACE

The ICM Core System includes software-based user interfaces for creating, viewing, updating, deleting, and reporting on data, as well as interfaces for managing the process of incident identification, response plan generation, response plan implementation, and Core System management.

Responsibility
1. With Software Engineers, resolve issues with user interfaces for managing asset and incident/event information; maintain the interfaces.
2. With Software Engineers, resolve problems with geospatial visualization of data and reporting, charting, and graphing functions; update the user interface as data and data presentation needs change and bugs are found.

10.7. SYSTEM INTEGRATION

System Integration requires monitoring system functionality, data control, and asset ownership.

Responsibility
1. With the Corridor Data Analyst and Software Engineers, resolve problems when standards are not followed for integrated data definition, capture, processing, and presentation. With Software Engineers, update the user and programming interfaces as data needs change and bugs are found.
2. Work with the Corridor Data Analyst, Data Analysts, and Software Engineers to identify and resolve issues where copies of data are being erroneously used as systems of record.

11. STAKEHOLDERS

Stakeholders are the key representatives from the corridor agencies who participate in the ICM project. Many stakeholder responsibilities are carried out by specific personnel within an agency, such as Traffic Engineers, Data Analysts, and so on, and, where possible, those responsibilities are listed under those particular job titles in this document. Tasks not associated with a specific job title, or that are the responsibility of the stakeholder agency generally, are listed in this "Stakeholders" section.

Stakeholders are involved in all areas of the System Requirements, including:

- Institutional Support
- Corridor Monitoring
- Strategic Incident/Event Response Planning
- Real-Time Incident/Event Monitoring
- Real-Time Response Planning
- Response Plan Implementation
- Data Management
- Decision Support
- Core System User Interface
- System Integration
- System Management

11.1. INSTITUTIONAL SUPPORT

Institutional Support focuses on strategic planning and on how organizations and people are structured, funded, motivated, and informed in order to execute strategic plans.

Responsibility
1. Strategic Planning
a. In consultation with the Corridor Manager, oversee the drafting, review, approval, and maintenance of the Corridor Strategic Plan for data collection, control, and performance metric calculation processes.
b. With consultants who are not direct stakeholders, review the Corridor Strategic Plan.
c. Approve the Corridor Strategic Plan.
d. Ensure that the assets and data defined in the Strategic Plan are available and properly maintained. Work with the Corridor Technical Manager and Corridor Data Analyst to provide any missing items. This may involve purchasing or upgrading assets and/or data.
2. Personnel and Management
a. Name and identify Corridor Champions. Replace Champions no longer with the project or agency.
b. In coordination with the Corridor Manager, write job descriptions for ICM roles within each organization and identify the individuals who will fill the roles.
c. Ensure that ICM support personnel are in place and trained.
d. Work with Corridor Manager to resolve discrepancies between current staff versus needed staff.

Responsibility
e. Develop new procedures and practices supporting ICM corridor management objectives.
f. Continuously engage in ICM corridor activities.
g. Provide feedback, when surveyed, on the management team, structure, and processes of the ICM effort.
3. Interagency Cooperation
a. Participate in developing a culture of cooperation and communication with agencies, organizations, other stakeholders, and all other personnel in the ICM environment (elected officials, travelers, the press, etc.).
b. Provide feedback on whether agency personnel understand ICM and the cultural changes required.
c. Provide feedback, through surveys and after-incident/event reviews, on communication effectiveness and/or breakdowns.
d. Analyze why communication is not working or where the breakdown occurred and involve senior management and Champions in resolving the issues.
e. Attend regular corridor update meetings or teleconferences.
f. Assist as needed with the drafting, review, approval, and maintenance of interagency agreements, such as the Project Charter, Memorandum of Understanding, and Operations and Maintenance Plan.
g. Sign agreements submitted for approval in a timely manner.
h. Analyze why and how interagency agreements are not signed and followed; work with proper Champions to resolve issues and ensure all conditions within the documents are adhered to.
i. Determine needs for ongoing communication training, including items such as conflict resolution, customer service, facilitation, speaking skills, etc.
4. Funding
a. Continually review budgets and identify existing funding gaps and needs for new funds.
b. Work with Caltrans to identify federal, state, regional, and local funding sources.
c. Identify agency personnel to help with the development, submission, and tracking of funding applications.
d. When needed, write Letters of Support for funding applications.
5. Outreach and Communications
a. Provide an organizational chart, names of Board members and office directors, key contact persons, and other relevant institutional information to the Outreach and Communications Manager.
b. Designate an individual in the agency who shall be responsible for outreach and communications.
c. Provide feedback on outreach and communication efforts and the effective handling of inquiries. With Corridor Champion(s), help resolve issues.
d. Review project documents and provide comments by agreed-upon deadlines.
e. Keep the Corridor Manager informed of scheduled events and associated street closures and recommended detours along corridor arterials.
f. In coordination with the Corridor Manager, develop contracts and positive relationships with third parties. Periodically review and renew purchasing choices and contracts.

11.2. CORRIDOR MONITORING

This function is tasked with determining the state of the corridor and using this state to accurately calculate and report corridor performance measures.

Responsibility	
1.	Ensure that the status of corridor assets is communicated to the ICM system, when status information is not provided through automation but through human processes.
2.	Create and edit device problem reports, where reports are not generated automatically by the ICM Core System.
3.	In coordination with external consultants, review performance metrics once per year.

11.3. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed, tested, and reported.

Responsibility	
1.	Work with the Corridor Manager to resolve attendance issues for response planning meetings.
2.	Specify whether active response plans involving agency assets can be automatically terminated by the ICM Core System.
3.	Define periods during which manual approval is required and periods during which automated approval is possible.
4.	After each incident, unscheduled event, or planned event, in coordination with the Corridor Manager and Traffic Engineers, review the selected response plan components and determine if any are missing or inappropriate.
5.	Note any problems building mock incidents.
6.	Each quarter, as well as following each major incident, meet to discuss and review the results of the application of response plans to the corridor. If meetings are not being held or attendance is low, work with the Corridor Manager and Corridor Champion(s) to determine and remedy the causes.

11.4. REAL-TIME INCIDENT/EVENT MONITORING

Real-time Monitoring involves ensuring that incidents/events can be accurately detected, identified, and characterized, and that all proper personnel are notified.

Responsibility	
1.	Incident/Event Information
	a. Provide information characterizing an incident/event to the ICM Core System (e.g., location, start time, type, severity, etc.). If the Corridor Manager determines that information was not provided, work with First Responders and Public Information Officers

Responsibility
to resolve the issues.
b. Review all incident/event information communication processes periodically and ensure that personnel are aware of and follow these processes.
c. Manually enter information about planned lane/roadway closures or scheduled events into the ICM Core System if not automatically retrieved by the system.
2. Incident/Event Validation
a. Validate that an incident or event exists before a response plan is applied.
b. If an incident or event is characterized but not validated, work with the Corridor Manager to determine and remedy the cause.
3. Incident/Event Notification
a. Inform the Corridor Manager if notification is not received from the ICM system when an incident or event occurs.
b. Work with the Corridor Manager to ensure the "who to contact" rule set is updated.
c. Maintain the "who to contact" list.
4. Updated Incident/Event Information
a. Provide updated event information (for example, end-of-incident network changes) to the ICM Core System.
b. Work with Corridor Manager to determine when incident information was not properly updated and resolve issues.

11.5. REAL-TIME RESPONSE PLANNING

Real-time Response Planning requires ensuring that response plans generated by the ICM system are reasonable, accurate, and properly approved by appropriate personnel.

Responsibility
1. Review response plans the system recommends for implementation. When reviews are not taking place, work with the Corridor Manager to identify and resolve issues with the review process.
2. If part of the plan approval process, approve, or disapprove, the response plan. If approval is not occurring, work with the Corridor Manager to determine the cause and resolve the problems.
3. With the Corridor Manager, note when approval rules are not followed and determine whether the problem is with the rules or the software.
4. As needed, review and analyze off-line each step in the response planning workflow, to understand how predictions were performed, recommendations made, and plans chosen.

11.6. RESPONSE PLAN IMPLEMENTATION

Implementing a response plan requires ensuring that instructions are sent correctly to corridor assets, keeping instructions current as assets change, notifying proper personnel, and tracking and resolving issues.

Responsibility	
1.	Assist where needed in resolving issues related to the order and schedule of asset instructions.
2.	Inform the Corridor Manager if not appropriately notified that a response plan is being deployed. Work with the Corridor Manager to ensure the "who to contact" rule set is updated and maintained.
3.	Permit the ICM Core System to contact designated agency personnel with requests for performing preapproved actions.
4.	Assist where needed in resolving issues related to sending asset instructions to both ITS and human elements in the response plan.
5.	As personnel change, modify as needed the manner in which instructions are sent.
6.	As assets and equipment change, modify as needed the system components and policies for verifying that asset instructions have been received.
7.	Assist as needed in resolving issues where status changes during a response were not communicated to stakeholders.
8.	Assist as needed in resolving issues where assets did not return to normal status when an incident or event ended.

11.7. DATA MANAGEMENT

Data and data quality is at the heart of data-driven performance management. Data must be accurate, complete, timely, reliably available, stored safely, and communicated and presented consistently.

Responsibility	
1.	Designate a representative to serve on the data governance board.
2.	With consultants, annually review data quality requirements and calculation methods. As needed, work with the Corridor Data Analyst and third-party providers to refine and update the data quality specifications.
3.	Work with the Software Engineers, Data Analysts, and Database Administrators to store data in electronic format.
4.	As data types and formats change, work with the Software Engineers, Data Analysts, and Database Administrators to ensure that storage methods are up to date.
5.	As needed, submit requests for data additions, removals, or format changes to Data Analysts.
6.	Notify the Corridor Data Analyst of any changes to data sources from systems owned by the agency.
7.	Determine why policies for data archiving, warehousing, and deletion are not being followed and ensure proper data management occurs.

11.8. DECISION SUPPORT

Decision Support involves ensuring that the appropriate rules are captured by the rules engine.

Responsibility
1. Create simple rules for the rules engine to use in developing response plans. (More complex rules require programming skills.)
2. Update rules as data changes. (More complex rules must be created/updated by Software Engineers.)

11.9. CORE SYSTEM USER INTERFACE

The ICM Core System includes software-based user interfaces for creating, viewing, updating, deleting, and reporting on data, as well as interfaces for managing the process of incident identification, response plan generation, response plan implementation, and Core System management.

Responsibility
1. Inform Corridor Technical Manager when user interfaces are not functioning.
2. Work with the Corridor Manager to resolve any interagency communication issues observed during incidents.

11.10. SYSTEM INTEGRATION

System Integration requires monitoring system functionality, data control, and asset ownership.

Responsibility
1. Work with the Corridor Manager as needed to clarify who owns a given corridor asset.

11.11. SYSTEM MANAGEMENT

System Management involves ensuring that the system is reliably operated and maintained. This includes the areas of security, service level agreements, maintenance, training, system recovery, and upgrades.

Responsibility
1. Security
a. Resolve issues related to unauthorized access to system assets.
2. Service Level Agreement
a. Review and approve the service level agreement.
b. Each year, in coordination with the Corridor Technical Manager, determine the desired

Responsibility
service level agreement metrics and provide resources to ensure they can be met.
3. Logging and Tracking
a. Report inaccurate or missing logging activity in system health, status, and other logs.
b. Use a system for tracking maintenance requests, improvement requests, and bug fix requests. Report any problems with using the system.
c. Report software bugs.
4. Maintenance
a. Be responsible for maintenance (both repair and preventative) of all system components (ITS components, vehicles, people, software, hardware, use approvals, etc.). Work with the Corridor Technical Manager to resolve issues.
b. Report maintenance activities (both repair and preventative). Work with the Corridor Technical Manager to resolve any reporting problems.
5. Training
a. Ensure that appropriate training and training materials are provided for all aspects of the ICM system.
b. Ensure that appropriate documentation, both user manuals and workflow descriptions, is available for all functions. Work with the Corridor Technical Manager to improve documentation as needed.
6. System Recovery
a. Work with consultants to periodically review disaster preparedness; work with the Corridor Technical Manager to resolve issues.
7. System Upgrades
a. Approve the 5-year system upgrade plan. Work with the Corridor Manager to resolve issues related to the plan and to maintain it.

12. MAINTENANCE STAFF

Maintenance Staff ensure all ICM hardware and communication components are maintained and in working order.

12.1. CORRIDOR MONITORING

This function is tasked with determining the state of the corridor and using this state to accurately calculate and report corridor performance measures.

Responsibility
1. Ensure that hardware and communication systems are working.

12.2. SYSTEM MANAGEMENT

System Management involves ensuring that the system is reliably operated and maintained. This includes the areas of security, service level agreements, maintenance, training, system recovery, and upgrades.

Responsibility
1. Perform maintenance (both repair and preventative) for system components (ITS components, vehicles, hardware, etc.).
2. Open/close/edit maintenance ticket items as needed.
3. Report maintenance activities (both repair and preventative).

13. IT SUPPORT

IT Support ensures the day-to-day operation and maintenance of workstations, security patch management, internet access, and proper software installation and configuration.

Responsibility
1. Troubleshoot and resolve technical issues associated with network connectivity, identity access, computer desktops, and peripheral devices.
2. Participate in disaster preparedness exercises and assist stakeholders in resolving technical issues.
3. Provide consultation as needed.

14. IT SECURITY

IT Security ensures that all ICM components (software, hardware and personnel) are safe and secure.

14.1. SYSTEM MANAGEMENT

System Management involves ensuring that the system is reliably operated and maintained. This includes the areas of security, service level agreements, maintenance, training, system recovery, and upgrades.

Responsibility	
1.	Be responsible for the security of the ICM Environment and its operations.
2.	Develop and implement security protocols and processes for the ICM Environment and ensure they are maintained.
3.	Maintain and review a log of access for evidence of unauthorized use of the system.
4.	Conduct formal reviews of the ICM Environment security processes at a regular frequency in accordance with the security protocols and processes, with a minimum frequency of quarterly.
5.	Direct a formal review of ICM Environment security, led by external security experts, at a regular frequency in accordance with the security protocols and processes, with a minimum frequency of annually.

15. TRANSPORTATION MANAGEMENT CENTER (TMC) AND LOCAL TRAFFIC CONTROL SYSTEM (TCS) OPERATORS

TMC/TCS Operators are responsible for day-to-day interaction with the ICM system, documenting incident information, and approving response plans. TMC Operators may be at Caltrans or local agencies such as a city or county. Local TCS Operators are at the local level, such as a city or county.

15.1. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed, tested, and reported.

Responsibility
1. Specify whether active response plans involving agency assets can be automatically terminated by the ICM Core System.
2. Define periods during which manual approval is required and periods during which automated approval is possible.

15.2. REAL-TIME INCIDENT/EVENT MONITORING

Real-time Monitoring involves ensuring that incidents/events can be accurately detected, identified, and characterized, and that all proper personnel are notified.

Responsibility
1. Confirm that an incident or event has been effectively terminated before the ICM Core System identifies it as such.

15.3. REAL-TIME RESPONSE PLANNING

Real-time Response Planning requires ensuring that response plans generated by the ICM system are reasonable, accurate, and properly approved by appropriate personnel.

Responsibility
1. As needed, manually select a response plan from a list of recommended response plans.
2. As needed, propose minor modifications to a recommended response plan.
3. Review and approve application of response plans.
4. As needed, propose changes to an implemented response plan.
5. Review and approve termination of response plans.
6. As needed, manually inform the ICM Core System that an incident or event has terminated

16. TRANSIT FIELD SUPERVISORS (RAIL, BUS)

Transit Field Supervisors are responsible for day-to-day interaction with the ICM system, providing incident information to the system and relaying response plan recommendations to operators.

16.1. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed, tested, and reported.

Responsibility
1. Participate in response planning activities.
2. Determine, if needed, detour routes that may be used during incidents and events impacting transit operations.
3. Determine, if needed, information to be sent to transit personnel during an incident or event.
4. Participate in defining or validating rules for building response plans.
5. Participate in defining or validating rules for handling special situations.

16.2. REAL-TIME INCIDENT/EVENT MONITORING

Real-time Monitoring involves ensuring that incidents/events can be accurately detected, identified, and characterized, and that all proper personnel are notified.

Responsibility
1. Enter into the ICM Core System information about transit incidents or service disruptions.

16.3. REAL-TIME RESPONSE PLANNING

Real-time Response Planning requires ensuring that response plans generated by the ICM system are reasonable, accurate, and properly approved by appropriate personnel.

Responsibility
1. Use information from the ICM Core System's response actions under consideration to make potential transit service adjustments.

17. PUBLIC INFORMATION OFFICERS (PIO)

PIOs at stakeholder agencies are responsible for public and media relations during major incidents or major changes to the ICM system.

17.1. INSTITUTIONAL SUPPORT

Institutional Support focuses on strategic planning and on how organizations and people are structured, funded, motivated, and informed in order to execute strategic plans.

Responsibility
1. Actively participate in ICM outreach and communications activities, such as press events, announcements, briefings on incidents/events, etc.
2. Assist the Outreach and Communications Manager with surveys to determine stakeholders' satisfaction with interagency communication.
3. Maintain ongoing communication with PIOs at other stakeholder agencies.

17.2. REAL-TIME INCIDENT/EVENT MONITORING

Real-time Monitoring involves ensuring that incidents/events can be accurately detected, identified, and characterized, and that all proper personnel are notified.

Responsibility
1. Work with stakeholders and First Responders to resolve issues when information characterizing an incident/event was not provided to the ICM Core System by stakeholders.

18. FIRST RESPONDERS

First Responders are emergency response personnel who are at the scene of an incident or event, take the lead in securing the scene, and direct others.

18.1. INSTITUTIONAL SUPPORT

Institutional Support focuses on strategic planning and on how organizations and people are structured, funded, motivated, and informed in order to execute strategic plans.

Responsibility
1. Ensure that ICM support personnel are in place and trained.
2. Attend quarterly ICM corridor update meetings where first response procedures are on the agenda.
3. Provide organizational charts, names of key contact persons, and other relevant institutional information to the Outreach and Communications Manager.

18.2. STRATEGIC INCIDENT/EVENT RESPONSE PLANNING

Strategic Response Planning means ensuring that response plans for incidents/events can be designed, developed, reviewed, tested, and reported.

Responsibility
1. Participate in incident/event response planning.
2. Determine desired routes to be used as detours for incidents and events.
3. Determine personnel to be available for deployment during an incident or event.
4. Determine typical information to be sent to agency personnel when responding to an incident or event.
5. Participate in defining rules for handling special situations.

18.3. REAL-TIME INCIDENT/EVENT MONITORING

Real-time Monitoring involves ensuring that incidents/events can be accurately detected, identified, and characterized, and that all proper personnel are notified.

Responsibility
1. Work with stakeholders and PIOs to resolve issues when information characterizing an incident/event was not provided to the ICM Core System by stakeholders.

19. OUTREACH AND COMMUNICATIONS MANAGER

The Outreach and Communications Manager is responsible for ensuring an ongoing flow of information between all ICM stakeholders both during incidents and as part of planning, implementation, and general PR efforts.

19.1. INSTITUTIONAL SUPPORT

Institutional Support focuses on strategic planning and on how organizations and people are structured, funded, motivated, and informed in order to execute strategic plans.

Responsibility
1. Organization Composition
a. Maintain information on stakeholder agencies (org chart, board members and officers, contacts, etc.).
b. Develop and maintain a list of current Corridor Champions from each stakeholder agency.
c. With the Corridor Manager, set up and maintain a Connected Corridors Steering Committee, Technical and Operational Advisory Committee, and other committees as needed.
2. Communications Strategy
a. Develop a communications strategy.
b. Cultivate and maintain ongoing positive relationships with stakeholders, partners, and other agencies.
c. Responsible for organizing regular meetings with stakeholders, PIOs, and first responders.
d. Create and maintain outreach materials in multiple formats, including newsletters, fact sheets, website, social media, etc.
e. Follow up on information requests; forward requests to other stakeholders for comment as needed.
f. Monitor elections, funding opportunities, and the political environment which may affect the ICM effort.
g. Conduct outreach and communications efforts to ensure that ICM is understood and accepted by all stakeholders (particularly when there is staff or elected official turnover).
h. In coordination with the Corridor Manager, survey personnel and their managers to determine if personnel understand ICM and the cultural changes required.
i. Responsible for stakeholder surveys and after-incident/event reviews focusing on communication and/or communication breakdowns.
3. Funding
a. Along with the Corridor Manager, research and track funding opportunities; prepare and submit funding applications.
4. Interagency Agreements
a. Draft a Project Charter and manage the process leading to its adoption by stakeholders.
b. Ensure interagency agreements are drafted, approved, and current.
c. Track when current stakeholder agreements are set to expire and whether they need

Responsibility
updating or amending. Inform stakeholders of agreement status and lead discussions on the renewal, updating, or amending of existing agreements.