**MAT v 1.0**

Task 5 MAT MOD Operational Readiness Framework

# Multimodal and Accessible Travel Mobility On-Demand Operational Readiness Framework

## Multimodal and Accessible Travel Standards and Vulnerable Road User Cyber security Support Project

July 2023

This document is produced by the MAT and Cyber security Subject Matter Experts (SMEs).

Published by:

ite
A Community of Transportation Professionals

Supported/Sponsored By: The United States Department of Transportation (USDOT)

U.S. Department of Transportation

# Table of Contents

## Contents

# 1 Introduction

## 1.1 Scope

This document describes a framework for assessing the operational readiness of a Mobility on Demand (MOD) project. The MOD Operational Readiness Framework provides a checklist for assessing the maturity of the technical, integration, security, and institutional (governance / policy) elements related to planning, designing, deploying, and operating MOD projects.

## 1.2 Objective

The objective of this assessment is to guide system deployers about the readiness to design, build and operate MOD based on technologies and integration elements. In addition, MOD services are typically based on coordination among multiple organizations, systems and physical environments. To that end, the this document's objectives include the following:

- Develop a framework that state and local agencies can utilize to determine if they are ready to start deploying mobility MOD systems and services.
- Develop a multi-dimensional framework that identifies maturity levels for multiple aspects of deploying and operating a MOD service.
- Provide a checklist for each dimension to achieve the next readiness level
- Provide guidance on how to use the framework to assess the maturity of a MOD project.

The recommendations identified in the document support program developers in identifying risks early in the concept and development phases so that they can reduce risks and problems later in the development. The framework was derived from existing readiness rubrics that are used for technology, integration, institutional and security readiness issues. In particular, this framework focuses on MOD projects that involve new institutional and business models, emerging technologies, new partners and stakeholders, and evolving cyber security threats to these systems.

## 1.3 Audience

The audience for this document includes researchers, planners, deployers, and operators who plan to or do operate and maintain MOD systems.

## 1.4 Background

The United States Department of Transportation (USDOT), ITE, and their standards development partners have worked on ITS standards since the inception of the ITS Standards Program more than 20 years ago. In recent years, traditional ITS technologies have started to integrate with multimodal travel and support vulnerable road users (VRUs). Working with the multimodal community to survey existing standards and how they can support/augment ITS implementations is a necessary step. Additionally, ensuring that the security needs of VRUs are addressed in both standards and ITS deployments is critical to the safety and security of those VRUs. USDOT previously had a MAT (MAT) Standards project that produced a Multimodal and Accessible Travel Standards Assessment (MATSA) and Roadmap that this project is expected to build upon. This project is to defining critical activities to better address the convergence of ITS technologies, with multimodal and accessible travel, and VRUs.

The objective of this project is to continue the work started under the Multimodal and Accessible Travel Standards project to address gaps in standards for MAT and VRU technologies when integrating with ITS environments and technologies, including connected vehicle (CV) technologies. Identifying the unique security and privacy risks associated with VRUs participating in ITS environments is a key activity that will be used to inform future cyber security guidance and standards development efforts. A key consideration in addressing the gaps is that MAT interfaces are addressed by numerous specification efforts that occur outside of the traditional Standard Development Organization (SDO) arena.

The MOD Operational Readiness Assessment helps MAT and MOD project planners understand the gaps and research needs related to their deployment. In many cases, the absence or limited number of standards impact integration readiness. Additionally, readiness for deployment does not account for all the impacts and risks associated with deployment. Institutional, policy, and regulatory drivers also contribute to the success of a project. The MOD Operational Readiness Framework provides a method to assess the holist maturity and sustainability of the project, not just one aspect of the project deployment.

## 1.5 Document Organization

This document is organized into the following nine sections:

**Section 1 Introduction** provides a high-level overview of the document scope and background.

**Section 2 Operational Readiness Overview** presents an overview of the readiness assessment approach that encompass readiness factors associated technical, integration, institutional and cyber security provisions of a MOD deployment.

**Section 3 Technical Readiness** describes the goals, issues/gaps, standards, and stakeholders that are associated with Vulnerable Road Users using Vehicle-to-Everything (V2X) standards.

**Section 4 Integration Readiness** describes the goals, issues/gaps, standards, and stakeholders that are associated with public right of way user needs.

**Section 5 Institutional Readiness** describes the goals, issues/gaps, standards, and stakeholders related to cross-cutting issues associated with how cyber security and Personally identifiable information (PII) standards are applied to MAT projects.

**Section 6 Cyber Security and Privacy Readiness** describes the goals, issues/gaps, standards, and stakeholders that are working on RSD standards and implementations.

**Section 7 Using this Framework for Assessing Your MOD Project** provides insight into how to assess your project's readiness for deployment.

.

# 2 Operational Readiness Overview

MOD projects may be characterized by several factors that diverge from typical technology deployments in several respects. They not only deploy mature and emerging technologies, but they may also integrate multiple systems and transportation modes operated by various public and private organizations for the public. The public must trust the fidelity, reliability, and protection of services and information managed by these systems.

In general, an operational readiness assessment may take the form of a checklist to plan the processes to achieve a state of readiness. There are several published checklists, lessons learned, and frameworks that describe the level of readiness associated with the technology [1, 2, 10], integration [10], cyber security / privacy [11] and institutional concerns [4, 5, 6, 7, 8, 9, 10] for MOD projects or general technology deployments.

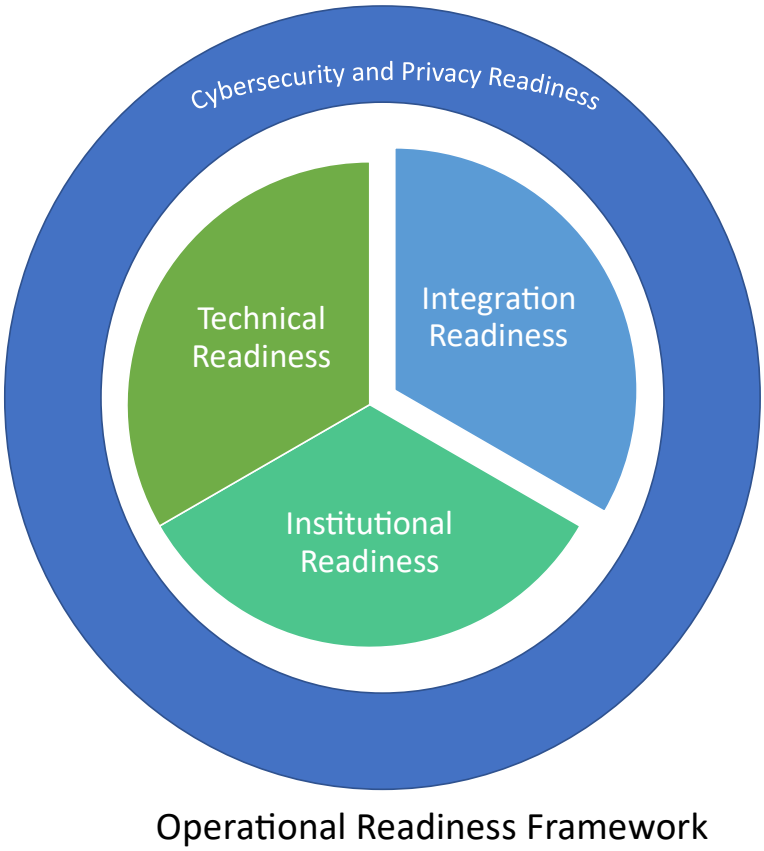


**Figure 1. MOD Operational Readiness Framework**. *Source: ITE.*

To that end, the MOD Operational Readiness Framework is composed of all four areas of assessment. The four areas are adopted from existing frameworks such as technical and cyber security/privacy or influenced by system engineering processes and lessons learned from multiple MOD project evaluations. The four areas are described as follows:

The **Technical Readiness Framework** covers the technologies and tools used to deploy MOD systems. They include the technology built into the hardware, software and communications components of a device or system. The guide used to assess technical readiness is based on the *Technical Readiness Level Guidebook* [1].

The **Integration Readiness Framework** covers assessing whether ITS systems and services are ready to integrate with MOD systems. An example of a system that might be under consideration would be a Self-Driving Shuttle (SDS) Automated Driving System. An example of the services that might be under consideration would be Transit Next Stop Request. The integration readiness assessment identifies and analyzes the maturity of the individual components (subsystems), interfaces, communications, and processes to integrate with other MOD services, systems, and subsystems.

The **Institutional Readiness Framework** covers the institutional, regulatory, and policy considerations during the planning, design, operation, maintenance, and evaluation of MOD services. The readiness assessment addresses the maturity of the institutional environment in terms of the stakeholders and the elements that enable MOD services and support the MOD ecosystem: business models, institutional partnerships and cooperation, infrastructure, and policies and regulations.

The **Cyber security and Privacy Readiness Framework** determines an organization's ability to detect and respond to security breaches, malware attacks, phishing attacks, and theft of data from both outside and inside the network. The cyber security and privacy readiness framework is based on the NIST Cyber security and Privacy Framework.

Technical and cyber security and privacy readiness have been addressed previously in the transportation technology sector but the readiness of technology integration, institutional coordination, and policy and regulatory impact has not. The purpose of including these aspects of MOD operational readiness is to ensure that the entire MOD ecosystem is considered when an agency is planning, designing, deploying, and evaluating MOD services. Further, because of the potential number of MOD stakeholders and relationships among these stakeholders, institutional conditions must be understood, and coordination, roles, and responsibilities must be well-defined before a MOD service can be successfully operated and maintained. Finally, MOD services often require system and data integration, so the readiness to develop required interfaces among MOD systems and databases must be understood before deploying MOD services.

# 3 Technical Readiness

Technical readiness covers the technologies and tools used to deploy MOD systems. The guide for assessing technical readiness is based on the *Technical Readiness Level Guidebook* (USDOT, FHWA-HRT-17-047. September 2017). The readiness levels were developed to "rank the maturity level of a technology" to function within a defined operational environment or deployment. As stated in the guidebook, the Technology Readiness Level (TRL) Assessment is a tool for understanding the functions and gaps in the technological solutions. In understanding these, deployers can better understand the potential risks and impacts during the deployment and operations of the technology.

The *TRL Guidebook* defines nine levels with questions by which deployers could assess the technology level. The nine levels and associated criteria are listed in **Table *1***.

**Table 1. Descriptions and Requirements of Technical Readiness Levels**

| TRL | Description | Requirements |
|---|---|---|
| **Basic Research** | | |
| **1** | Basic principles and research | • Do basic scientific principles support the concept?<br>• Has the technology development methodology or approach been developed? |
| **2** | Application formulated | • Are potential system applications identified?<br>• Are system components and the user interface at least partly described?<br>• Do preliminary analyses or experiments confirm that the application might meet the user need? |
| **3** | Proof of concept | • Are system performance metrics established?<br>• Is system feasibility fully established?<br>• Do experiments or modeling and simulation validate performance predictions of system capability?<br>• Does the technology address a need or introduce an innovation in the field of transportation? |
| **Applied Research** | | |
| **4** | Components validated in laboratory environment | • Are end-user requirements documented?<br>• Does a plausible draft integration plan exist, and is component compatibility demonstrated?<br>• Were individual components successfully tested in a laboratory environment (a fully-controlled test environment where a limited number of critical functions are tested)? |
| **5** | Integrated components demonstrated in a laboratory environment | • Are external and internal system interfaces documented?<br>• Are target and minimum operational requirements developed?<br>• Is component integration demonstrated in a laboratory environment (i.e., fully-controlled setting)? |
| **Development** | | |

| | | |
|---|---|---|
| **6** | Prototype demonstrated in relevant environment | • Is the operational environment (i.e., user community, physical environment, and input data characteristics, as appropriate) fully known?<br>• Was the prototype tested in a realistic and relevant environment outside the laboratory?<br>• Does the prototype satisfy all operational requirements when confronted with realistic problems? |
| **7** | Prototype demonstrated in operational environment | • Are available components representative of production components?<br>• Is the fully-integrated prototype demonstrated in an operational environment (i.e., real-world conditions, including the user community)?<br>• Are all interfaces tested individually under stressed and anomalous conditions? |
| **8** | Technology proven in operational environment | • Are all system components form-, fit-, and function-compatible with each other and with the operational environment?<br>• Is the technology proven in an operational environment (i.e., meets target performance measures)?<br>• Was a rigorous test and evaluation process completed successfully?<br>• Does the technology meet its stated purpose and functionality as designed? |
| **Implementation** | | |
| **9** | Technology refined and adopted | • Is the technology deployed in its intended operational environment?<br>• Is information about the technology disseminated to the user community?<br>• Is the technology adopted by the user community? |

The *TRL Guidebook* describes the assessment process as follows:

1. **Identify the technical components of the system or services being assessed**. For example, technology components may include the following:
    - Communications such as
        - Bluetooth low-energy beacons used for indoor / outdoor navigation
        - Near field communication used to identify locations or information from back office sources
        - CV2x communications for use by vulnerable road users
    - Automated shuttle customer services such as automated wheelchair tiedowns, automated ramps, and other accessibility features
    - Condition and status information collected from conveyances such as elevators and escalators
    - Data collection of public right of way information to support wayfinding by vulnerable road users especially through work zones that obstruct sidewalks and divert paths to a detour

- Use of microservices to process sidewalk data

2. **Assess each technology component's readiness level** based on the criteria associated with **Table *1***. The TRL categories and levels are based on maturity levels from multiple industries, including highway, defense, and space technologies. The levels help identify the technical maturity and hence the degree of risk related to the deployment element. The assessment is typically based on research reviews, test results, and number of deployments in various environments.

The USDOT ITS4US program used this assessment to describe the maturity of technology in the five projects awarded Phase 1 grants. An example of a technology assessment developed for the University of Washington for use of "microservices architecture for data collection, aggregation, transformations, and other lifecycle activities." [https://rosap.ntl.bts.gov/view/dot/62479, p., 12-29, 51-56].

Other examples include enabling technologies from the Buffalo ITS4US project [https://rosap.ntl.bts.gov/view/dot/62478] including the following:

- Community Shuttle Trip Booking Transaction Technology Interfaces
- Navigation Technology Integration with Smart Signs
- Mobile Pedestrian Crossing Technology Interface
- Mobile App Positioning and Orientation Technology
- SDS [self-driving shuttle] Accessibility Support Technologies

# 4 Integration Readiness

The Integration Readiness Assessment identifies and assesses the maturity of the individual components (subsystems), interfaces and processes to implement and deploy the overall system. In addition, the assessment considers whether other aspects of ITS environments (including connected and automated vehicle environments) and mobility systems are ready to integrate with MOD systems.

## 4.1 Integration Discussion

Before addressing the Integration Readiness of a project, this section identifies key considerations regarding defining and carrying out system integration. The following three general areas are defined:

- Identification of Integration Needs
- Evaluation of System Maturity
- Integration Activities in the Project Life Cycle

**Identification of Integration Needs**

The first step in performing integration readiness assessment is to clearly define the integration aspects of the system. To do this the following activities should be considered:

1. Identify the components (subsystems) that are to be integrated into the overall system. Each of these components would be subject to a Technical Readiness Assessment as described in Section 3.
2. Identify the interfaces between the components as part of the overall system. For each interface, are there existing standards or specifications that will define the different aspects of the interface (information, protocols, management, and security). Another consideration regarding interfaces is whether their definition is from open source or proprietary.
3. Identify the organizations involved in the operations, maintenance and users of the overall system, and the roles and responsibilities of each organization.

Note that information on each of these considerations will be a part of any project ITS architecture developed for the effort. In the absence of a project ITS architecture, much of this information can also be found in the applicable regional ITS architecture.

**Evaluation of System Maturity**

The Integration Assessment evaluates the maturity of the **overall system**. Some of the activities that should be considered in evaluating the system maturity are the following:

a. Evaluate the maturity of the **interfaces** between the different components. Is each interface open or proprietary? Is each interface fully defined by existing standards or specifications? Or is some development needed? For example, if the system has an interface between user devices and roadside devices, is an open standard being used to define the interface, or is a proprietary interface defined by the manufacturer of the devices. If the interface is being defined by an open standard, what is it and are there any known issues with deploying that standard.

   Some of the aspects of each interface that should be considered are:
   a. Information or data definition

b. Transmission protocols definition
c. Level of Security required

If the interface does not have a standardized definition for any of these aspects, what is the basis for the interface definition to be used on the project? Has the interface definition been successfully deployed before with similar requirements (or capabilities)?

b. Consider the maturity of the operational environment of the system. Are the performance requirements of the system defined? For example, each subsystem may have a processing performance requirement, but what's the performance requirement for the overall system, from the time the data is first "sensed," processed, exchanged, and shared with the end user? Has the system been deployed in an operational environment elsewhere? Are there any operational differences between the planned system and other deployments? Have any unique operational constraints been identified? For example, the system must operate within the current staffing levels.
c. Consider the other issues that may affect integration activities:
    a. How will users interface with the system. Are there any accessibility needs relating to joining or using the system that requires universal design considerations?
    b. Do interfaces cross organizational boundaries and will this impact the integration needs?
    c. Have the operating and data sharing needs been considered?

**Integration Activities in the Project Life Cycle**

When developing a project, one of the key considerations is what Integration Activities will be needed on the project. When will they be performed, by whom, and how? How will they "check out" each component and each interface. Integration is an aspect of the systems engineering, one representation of such is the VEE diagram as shown below. Integration occurs following SW/HW implementation, but the planning for it occurs earlier during the Concept of Operations, Requirements, and Design phases of the process.

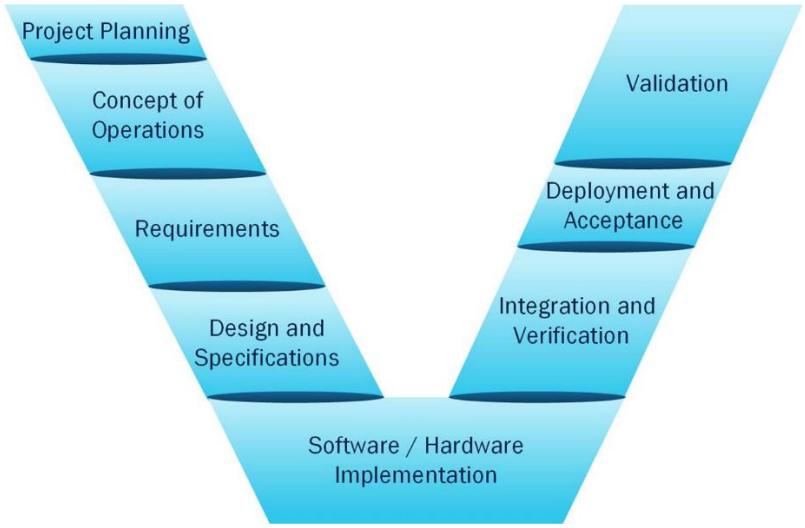


**Figure 2. Systems Engineering Project Life Cycle.**

Integrating the system is a key systems engineering activity that includes basic planning, preparation, and execution activities as described below:

1. A key output of the integration planning is an integration strategy document that defines the order in which the project components are integrated with each other and with other systems that the project must interface to. Each integration step includes integration tests that verify the functionality of the integrated components with particular focus on the interfaces. For less complex projects, the integration strategy can be an informal plan. For complex projects, there will have to be careful planning so that the system is integrated in efficient, useful increments consistent with the master schedule. The Integration Strategy should also address the who, how, and when of the integration.
2. Establish integration environment – The tools that will be used to support integration are defined, procured, and/or developed. For complex systems, this could include simulators that are used to simulate operational interfaces, test equipment that is used to inject failures and monitor system responses, etc.
3. Perform Integration – The system is progressively integrated based on the integration strategy. The system components are integrated with each other and with other interfacing systems. Integration tests are used to verify that the components and higher-level assemblies work together properly and do not interfere with one another. Integration tests are used to exercise the interfaces and verify the interface documentation in detail. The process confirms that all interfaces are implemented per the documentation.

## 4.2 Integration Readiness Levels

In order to perform the Integration Readiness Assessment, the three integration consideration areas defined above are evaluated against the levels below, which are based on the levels contained in the *TRL Guidebook*.

**Level 1: Integration needs not yet defined**

Many less complex projects do not use a systems engineering process, so they may have a less formalized definition of its needs, requirements, and design. In this case, outputs of the applicable regional ITS architecture may be used to help define the integration needs. A project that does use the systems engineering process typically begins to define interfaces during the Concept of Operations (ConOps) and Systems Requirements development, with the first full description of the system interfaces and the standards/specifications that apply to the interfaces being described during High Level Design. So early in the development process, there may be an initial idea of what integration will be needed, but until the project gets to the design phase, the integration needs will remain largely not yet defined.

The following set of requirements can relate to both this level and the next. A negative answer to some or all of these questions would indicate that the project's level of integration readiness is that the "integration needs are not yet defined".

- Have user needs been defined (which may contain some indication of integration needs)? Note this would typically be done in a Concept of Operations if the project has one.

- Have the system requirements been developed and do they include interface requirements?
- Has a system diagram been created that identifies all key interfaces?

**Level 2: Integration needs partially understood**

Definition of integration needs will be facilitated if the project uses at least some aspects of the systems engineering process. The Concept of Operations may contain system overview information that provides an initial idea of the subsystems and interfaces that will need to be integrated. In addition, the concept of operations will likely include a discussion of the stakeholders involved in the project as it provides an initial understanding of the subsystems and interfaces. This information can help identify early where interfaces cross stakeholder boundaries, and hence may be subject to additional integration issues.

An area that is related to integration is the institutional issues associated with the project. The institutional setup (e.g., the organizations involved in the operations, maintenance and users of the overall system, and the roles and responsibilities of each organization) has an impact on integration readiness, but is central to the Institutional readiness discussed in Section 6 in this report.

So, in some cases, even if a project has not reached the design phase (or possibly is early in the design phase) then its integration readiness assessment would most likely be that the integration needs are partially understood. For the following requirements, a positive answer to each of these questions would indicate that the project's integration readiness is that the integration needs are partially understood:

- Is Concept of Operations completed and does it contain a discussion of integration needs?
- Have the system requirements developed and do they include interface requirements?
- Has a system diagram been created that identifies all key interfaces? Is there a project ITS architecture that can be used to define the standards defined for the interfaces?

**Level 3: Integration Needs Defined**

To progress to this level of Integration Readiness all of the activities of the **Identification of Integration Needs** should be completed, and the activities of the **Evaluation of System Maturity** section at least preliminarily addressed. The interface evaluation usually occurs during the detailed design phase of a project where questions of the maturity of each interface planned for the project must be addressed.

In order to assess that integration needs are defined, for every interface that is not well defined by a standard or specification, an approach must be developed to both define the interfaces and to plan for how it will be integrated into the system.

One key output in the definition of integration needs is an Integration Strategy, described above in the Integration Activities section. For larger, or more complex projects this will likely be a separate document, while for less complex projects it may be a section of some other systems engineering documentation. This document is the logical place to consider the Operational environment, and the Institutional environment described in Section 6 and briefly above.

For the following requirements, a positive answer to each of these questions would indicate that the project's integration readiness is that the integration needs are defined.

- Has a project ITS architecture been created?
- Has the system design been completed?
- Have the standards or specifications that will define each interface been defined and documented (possibly in Interface Control Documents)?
- Has the maturity of the interface standards or specifications been identified?
- If the project is complex, has an integration strategy been developed?
- Have institutional issues relating to interfaces that span different stakeholder groups been defined and documented?

**Level 4: Integrated components demonstrated in a laboratory environment**

For projects developing systems with new or untested capabilities, some level of integration and testing in a laboratory environment may be called for. This integration and testing might involve simulations or a sandbox testing environment that approximates but does not duplicate an operational environment. To perform this sandbox testing, the system must be defined (per level 3) and in addition, the laboratory environment must be defined, procured, integrated, and tested. This may involve a limited set of integration and testing steps to assemble just a subset of the overall system, as many systems contain elements that are well-defined along with those that need prototyping. If such a sandbox is deemed necessary, then its definition, along with the definition of the laboratory environment, would logically be described in the Integration Strategy document.

For the following requirements, a positive answer to each of these questions would indicate that the project's integration readiness is at the integrated components demonstrated in a laboratory environment level:

- Are the integration needs defined (per level 3)?
- Is the laboratory environment defined and documented, for example in an Integration Strategy document?
- Are target and minimum operational requirements developed?
- Is component integration demonstrated in a laboratory environment (i.e., fully controlled setting)?

**Level 5: Prototype demonstrated in operational environment**

Some projects develop a prototype in an operational environment before doing the full deployment. One reason for doing this is that production components may not be readily available. When doing this, a key consideration is whether the prototype components are representative of production components. In addition, the testing of individual interfaces should be done to test not just basic functionality, but also stressed or anomalous conditions. Finally, another consideration should be whether the fully integrated prototype is demonstrated in an operational environment (i.e., real-world conditions, including the user community)?

For the following requirements, a positive answer to each of these questions would indicate that the project's integration readiness is at the Prototype demonstrated in operational environment readiness level:

- Is the operational environment (i.e., user community, physical environment, and input data characteristics, as appropriate) fully known?
- Was the prototype tested in a realistic and relevant environment outside the laboratory?
- Does the prototype satisfy all operational requirements when confronted with realistic problems?
- Have MOUs and agreements for all the stakeholders/organizations involved been identified and are in the process of being approved?
- Are available components representative of production components?
- Is the fully-integrated prototype demonstrated in an operational environment (i.e., real-world conditions, including the user community)?
- Are all interfaces tested individually under stressed and anomalous conditions?

**Level 6: Ready for System Integration with Some Risk**

The highest levels of readiness for System Integration are when the production system is ready for system integration. In this case, the integration strategy has been documented, and the system interfaces have been designed and evaluated for their maturity. In addition, the integration environment has been developed, with needed tools that will be used to support integration procured, and/or developed.

For the following requirements, a positive answer to each of these questions would indicate that the project's integration readiness is at the Ready for System Integration with some risk readiness level:

- Are all system components form-, fit-, and function-compatible with each other and with the operational environment?
- Are some of the interfaces defined by mature standards or specifications?
- Is the technology proven in an operational environment (i.e., meets target performance measures)?
- Are the MOUs and agreements for all the stakeholders/organizations involved formally signed?

**Level 7: Ready for System Integration with Reduced Risk**

The highest level of readiness for System Integration is when the production system is ready for system integration. In this case, the integration strategy has been documented, the system interfaces have been designed and evaluated for their maturity. In addition, the integration environment has been developed, with needed tools that will be used to support integration procured, and/or developed.

For the following requirements, a positive answer to the following question would indicate that the project's integration readiness is at the Ready for System Integration with reduced risk readiness level:

- In addition to meeting the requirements of Level 6, do most (or all) of the system interfaces use mature standards/specifications?

# 5 Institutional Readiness

This section describes an Institutional Readiness Level (IRL) assessment for Mobility on Demand (MOD) services. For the purpose of this report, institutions are defined as MOD organizational stakeholders, including public transit and paratransit agencies, MOD service providers, transportation and traffic management agencies, metropolitan planning organizations, and local, state, and federal governments. A more detailed description of MOD organizational stakeholders is in the following subsection.

IRL Assessments can be a tool for determining the maturity of the institutional environment. This environment is complex. Further, because of this complexity, the readiness of this environment to fully support MOD services has not been defined previously even though institutional issues have been addressed as part of the USDOT MOD and Accessible Transportation Technologies Research Initiative[1] programs, and several related European programs and projects, including Institutional Frameworks for Integrated Mobility Services in Future Cities[2],[3] and Sustainable Urban Mobility Plans.[4]

This section presents an IRL scale which is composed of identifying specific levels of institutional readiness that support the design, operations and maintenance of MOD service. Because MOD services have a wide variety of stakeholders, as identified in the MOD Operational Concept Report[5] and MOD Planning and Implementation: Current Practices, Innovations, and Emerging Mobility Futures, the IRL scale is presented at a relatively high level.

## 5.1 MOD Stakeholders and Enablers

According to the MOD Planning and Implementation Report, “A variety of stakeholders both influence and are impacted by MOD, including federal agencies, state agencies, regional agencies, local governments, policymakers, the private sector, and other institutions.”[6] Further, these stakeholders are directly involved in the following elements that enable MOD services and support the MOD environment:

- Business models
- Institutional partnerships
- Infrastructure
- Policies and regulations

MOD standards play a role in each of these support elements but is considered primarily in the last element: policies and regulations.

While not specifically documented, the aforementioned stakeholders may be involved in other activities related to institutional readiness such as MOD planning, MOD project development (including resource identification), and the development of MOD operations and maintenance procedures.

The primary MOD business models are shown in Table 1:[7],[8]

| **Business Model** | **Description** |
|---|---|
| Business to Consumer (B2C) | Providing individual consumers with access to a business-owned and operated transportation service (e.g., shared mobility). |

| | |
|---|---|
| Business to Government (B2G) | Providing transportation services to a public agency for public-sector related purposes. |
| Business to Business (B2B) | Providing business customers with access to transportation services for work-related trips. |
| Government to Consumer (G2C) | Providing public transportation services to consumers. |
| Consumer to Consumer (C2C) | Providing peer-to-peer transportation services. |

Another business model, which is not addressed in this report is mobility as a service (MaaS).

The most prevalent MOD partnerships are public-private partnership, which can assist in the following:

- Data sharing
- First- and last-mile connections
- Integration with third-party applications
- Low density and off-peak services
- Paratransit service
- Risk sharing

MOD infrastructure can include that for public transit (e.g., bus stops, passenger loading zones, technology to enable MOD services) and supporting services such as sidewalks, bike lanes, and paths, and traffic signals.

MOD policies and regulations "include enablers, such as equity, safety, mobility, sustainability, accessibility, and standardization. Policy and regulatory enablers are the best tools to address challenges with the applicability of existing laws and regulations, accessibility for people with disabilities, economic accessibility, digital poverty, and the urban and rural divide. Likewise, standardization (both technological and infrastructure) is crucial to ensure interoperability among different components of the MOD ecosystem and to enable a more efficient and usable system. The public sector has a major role as a stakeholder and an enabler affecting different transportation modes by defining legislative frameworks, ensuring fair market performance, establishing incentives, and initiating pilot programs (Cohen and Shaheen, 2016; Shaheen et al., 2016)."[9]

## 5.2 The IRL Assessment Framework

The IRL Assessment Framework, which takes the aforementioned MOD stakeholders and enablers into account, has six levels. The Framework, shown in Table 1, is loosely based on the analytical framework of the aforementioned IRIMS project (which draws upon institutional theory) and institutional involvement in the development of Sustainable Urban Mobility Plans.[10] The levels of institutional readiness coincide generally with the process of deploying a MOD service.

**Table 1. Descriptions and Requirements of IRLs**

| IRL | Description | Requirements |
|---|---|---|
| 1 | Pre-planning for MOD services | • Have relevant local, regional and statewide stakeholders/institutional actors been identified along with their interests/agendas?<br>• Have the skills, knowledge, capacities, and resources of the institutional actors been assessed?<br>• Has funding/financing been identified for operating and maintaining the service?<br>• Will the MOD service present new opportunities for revenue income?<br>• Will the MOD service be completely accessible (from a physical perspective and equitable from a cost perspective) to all potential riders?<br>• Will legislation or regulations (e.g., Americans with Disabilities Act) create a barrier for operating the service?<br>• Have institutional cooperation structures (e.g., partnerships) been created or established?<br>• Have legal cooperation frameworks been investigated (e.g., memoranda of understanding)?<br>• Has a strategy for citizen and stakeholder engagement been developed? |
| 2 | Identify MOD service goals and objectives | • Have the operational preconditions for implementing the MOD service been identified?<br>• Have the levels and methods of involvement by the institutional stakeholders been determined?<br>• Has an appropriate business model been identified?<br>• Have the existing public transit/shared mobility conditions, performance measures, goals, issues and trends been analyzed?<br>• Have the indicators/performance measures for service monitoring and evaluation been selected/defined?<br>• Have the operating and data sharing needs been considered?<br>• Have new data sources been sought or identified? |
| 3 | Identify MOD concept of operations, including defining service characteristics | • Have data standards related to the data needed for MOD service operation, maintenance, monitoring and evaluation been identified along with the standards' maturity?<br>• Has "before" data associated with service monitorin and evaluation been collected or is being collected?<br>• Have anticipated institutional roles and responsibilities been defined?<br>• Has a method to manage institutional partnerships been developed? |

| | | |
|---|---|---|
| | | • Do interfaces cross organizational boundaries and will this impact the integration needs? (see Integration Readiness Framework in Section 4 above)<br>• Has a service monitoring and evaluation plan been developed?<br>• Have arrangements been made, including technical, policy, regulatory, or institutional provisions, that affect data and their cycle (creation, collection, storage, use, protection, access, sharing, and deletion) across policy domains and organizations?<br>• Is there potential labor union involvement in MOD service operation?<br>• Has the external environment been described, including the required interfaces to existing technology systems?<br>• Has the support environment been described, including maintenance of the MOD service?<br>• Has the operational environment been described?<br>• Have normal operational, maintenance and failure scenarios been described?<br>• Do the scenarios include the viewpoints of all involved stakeholders?<br>• Are institutional constraints on the MOD service development identified?<br>• Are there differences in policy (e.g., payment/fares, discounts) that may confuse customers?<br>• How will institutional roles/responsibilities impact customers?<br>• How much of the integration described earlier will impact the customer experience? |
| 4 | Develop implementation plan | • Have suitable types of policy measures across the stakeholders been identified and analyzed?<br>• Have the details of policy measures and packages been specified and appraised?<br>• Have the contractual terms and conditions that must be met by the MOD vendor been defined?<br>• Has the level of service (service level agreement [SLA]) expected from a MOD vendor been identified, as well as remedies or penalties should service levels not be achieved?<br>• Have MOD service standard operating procedures been developed?<br>• Has the data analysis, reporting, and maintenance been defined along with reporting frequency?<br>• Has sustainable funding been identified for ongoing operations and maintenance? |
| 5 | Implement MOD service | • Are institutional partnerships and coordination being evaluated? |

| | | |
|---|---|---|
| | | • Is the stakeholders' participation process being evaluated?<br>• Is the MOD service development process being evaluated?<br>• Is data analysis and reporting being performed regularly based on the performance metrics identified earlier?<br>• Is data maintenance being conducted?<br>• Are the SOPs being reviewed for updates? |
| 6 | Conduct MOD service evaluation | • Are continual process improvement and lessons learned being conducted and documented, respectively?<br>• Are periodic reviews of policies (e.g., institutional coordination, regulations, etc.) being conducted?<br>• Are periodic reviews of data standards, collection, management, and maintenance being conducted?<br>• Are performance metrics being reviewed for modifications to the MOD service?<br>• Are performance metrics being reviewed for modifications to the metrics? |

# 6 Cyber Security and Privacy Readiness

The cyber security and privacy readiness framework is based on the NIST Cyber Security and Privacy Framework.

## 6.1 NIST Cyber Security and Privacy Framework

A cyber security readiness framework determines an organization's ability to be able to detect and respond to security breaches, malware attacks, phishing attacks, theft of data from both outside and inside the network.

Before a MOD service is ready to be deployed into the transportation infrastructure, an assessment can determine whether basic cyber security protections are in place to protect against these attacks. The National Institutes of Standards and Technology's (NIST) Cyber Security Framework (CSF) and their Privacy Framework (PF) have included procedures to guide users through this process.

The CSF begins with five Core Functions which consist of the following:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

The "Core" is a set of cyber security activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. It presents industry standards, guidelines, and practices in a manner that allows for communication of cyber security activities and outcomes across the organization from the executive level to the implementation/operations level.[11]

Implementation "Tiers" help an organization do an assessment to determine if they are 1 or 4 range (see graphic, below) by determining how well integrated cyber security risk decisions are into broader risk decisions, and the degree to which the organization shares and receives cyber security info from external parties such as threat intelligence information from ISACS.

The "Tiers" describe the degree to which an organization's cyber security risk management practices exhibit characteristics such as risk and threat aware (Tier 1), repeatable (Tier 3), and adaptive (Tier 4). The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, supply chain cyber security requirements, and organizational constraints. While these Tiers do not represent cyber security maturity models, they assist management in assessing risk in helping prioritize where to utilize the organization's cyber security resources. Specific questions to consider in assessing an organization's Tier level are included in the CSF document. [12]

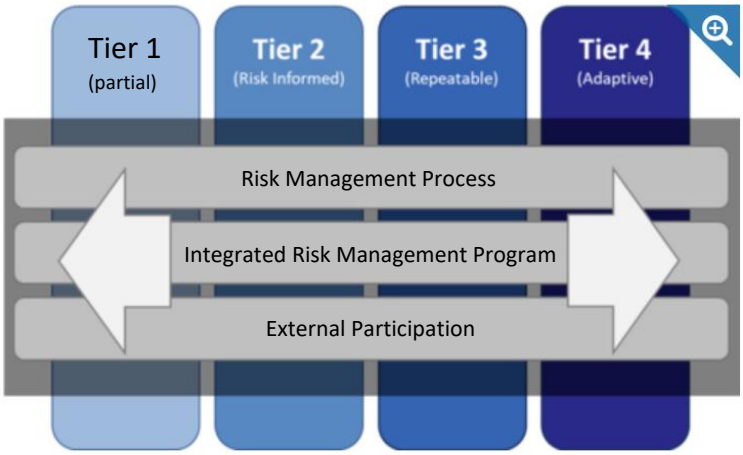


*Figure 3: Figure 3. Implementation Tiers 1 through 4. Source: NIST*

After a Tier Assessment has been conducted, an organization can create their own Framework "Profile" which will help determine how a solution will enable the organization to implement components of the CSF to move towards Tier 4. [13] This will give a better picture of the organization's Current State and Target State. Gaps between these two states reveal where cyber security risk management objectives should be focused.

> "The alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cyber security risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities."

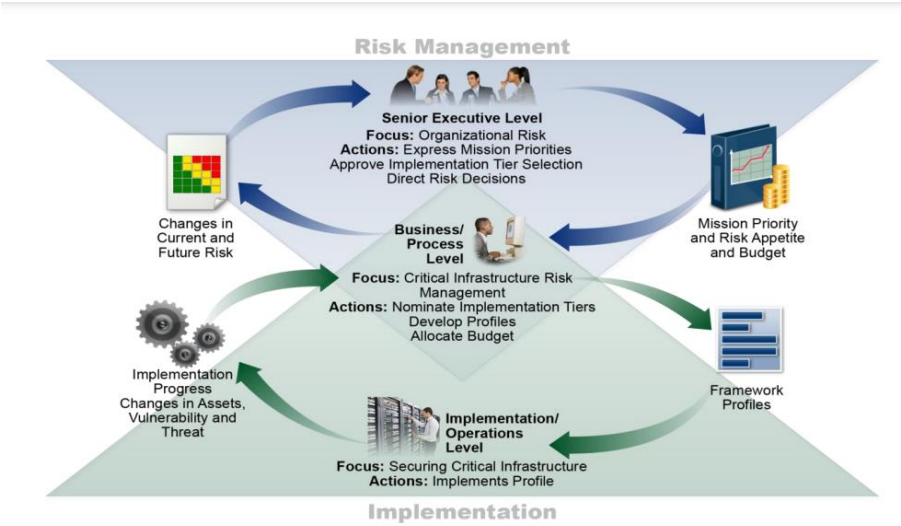


*Figure 4: This graphic represents how a Framework Profile and Tiers fit into a Risk Management process.[14]*

## 6.2 NIST Cyber security Framework's Application to a Privacy Readiness Assessment

If an organization collects or stores Personal Identifying Information (PII) or Sensitive Personal Identifying Information (SPII), NIST's Privacy Framework structure and risk assessment structure is similar with a few different components that are particular to privacy. [15]

The Functions are as follows:

1. Identify
2. Govern
3. Control
4. Communicate
5. Protect
6. etect (same as CSF)
7. espond (same as CSF)
8. ecover (same as CSF)

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| **ID-P** | Identify-P | ID.IM-P | Inventory and Mapping |
| | | ID.BE-P | Business Environment |
| | | ID.RA-P | Risk Assessment |
| | | ID.DE-P | Data Processing Ecosystem Risk Management |
| **GV-P** | Govern-P | GV.PO-P | Governance Policies, Processes, and Procedures |
| | | GV.RM-P | Risk Management Strategy |
| | | GV.AT-P | Awareness and Training |
| | | GV.MT-P | Monitoring and Review |
| **CT-P** | Control-P | CT.PO-P | Data Processing Policies, Processes, and Procedures |
| | | CT.DM-P | Data Processing Management |
| | | CT.DP-P | Disassociated Processing |
| **CM-P** | Communicate-P | CM.PO-P | Communication Policies, Processes, and Procedures |
| | | CM.AW-P | Data Processing Awareness |
| **PR-P** | Protect-P | PR.PO-P | Data Protection Policies, Processes, and Procedures |
| | | PR.AC-P | Identity Management, Authentication, and Access Control |
| | | PR.DS-P | Data Security |
| | | PR.MA-P | Maintenance |
| | | PR.PT-P | Protective Technology |
| **DE** | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| **RS** | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| **RC** | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

*Figure 5: Functions Supported by NIST CSF*

## 6.3 Application of the NIST Cyber security Framework to the Transportation Infrastructure

The NIST CSF was created to help organizations assess and manage their cyber security risk. It was written towards a broad application for organizations operating in the critical infrastructure sector which includes the transportation infrastructure. After an organization applies the Framework steps and creates a Profile, a question might remain as to, "What do we do next?"

As applied to MOD organizations and services, recommendations for cyber security best practices, standards, and frameworks are in Task 2 and reiterated in Task 4. A summary of important topics from those reports is below:

- Inventory and control of assets
- ata destruction plans
- Security for payment processing/mobility payment integration
    - PCI-DSS
    - Blockchain technology for pseudonymity to authorize payments
        - Pivot App
- isaster response plans and event recovery
    - NIST Special Publication 800-184 "Guide for Cyber security Event Recovery"
- Encryption standards defined for data at rest and data in transit
- Signals (DSRC, cellular, Bluetooth, etc.) security and privacy policies and standards
- etail and standardized protection of metadata
    - ASTM 2468-05
- Log management
- Access Management
- Security and privacy awareness and trainin
- Testing of security systems, such as vulnerability scanning and penetration testin
    - ITRE ATT&CK or Microsoft STRIDE
- Security design frameworks
    - ITRE ATT&CK or Microsoft STRIDE
- Engineering of secure and cyber resilient systems
    - NIST SP800-160 vol 1 & 2
- Security for communications between the user's app and traffic field systems
    - NEMA Standards Publication TS 8-2018
- Security for how management station interfaces with a field device to control and monitor traffic signal controllers and are relevant to Personal Safety Messages (PSM)
    - NTCIP 1202 v03
- Privacy protection of PII
    - NIST Cyber security Privacy Framework
    - NIST SP800-122 and SP800-53 controls for Sensitive PII
    - NIST SP800- 122, Section 4.2.4 for Anonymization Methods
- Security and Privacy for health care information
    - HIPAA

When deciding which of the best practices, standards, and frameworks to apply to a organization or service, below are some questions to start the assessment:

Some cyber security questions to ask:

1. **IDENTIFY** - What are your assets and where are they? Have you conducted a risk assessment and determined risk appetite?
2. **PROTECT** - Do you have awareness and training? Do you have monitoring of your assets?
3. **DETECT** - Do you have anomaly detection capabilities?
4. **RESPOND** - Do you have response planning and a communications plan?
5. **RECOVER** - Do you have a back-up management and restoration plan?

Some privacy protection questions to ask:

1. **IDENTIFY** - Where are your assets and data stored? Have you conducted a risk assessment and determined risk appetite?
    a. Do you have cameras collecting images, apps collecting location and account subscriber usernames and passwords, geo-location of clients, information about mode of transportation for clients with mobility concerns (wheelchairs vs e-scooters), travel patterns attributable to identifiable clients, home addresses and phone number for subscribers, etc.?
2. **GOVERN** - Do you have awareness and training? Do you have monitoring of your assets and data?
3. **CONTROL** - Do you have policies regarding collection, processing, and storing data?
4. **COMMUNICATE** - Do you have a process to implement activities to engage in dialog about how data are protected, processed, and associated privacy risks?
5. **PROTECT** - Do you have safeguards to ensure delivery of critical infrastructure services?
6. **RESPOND** - Do you have a breach notification requirement and/or process? Do you have mitigation processes?
7. **RECOVER** - Do you have a back-up management and restoration plan?

## 6.4 Summary of Cyber Security and Data Privacy Readiness Assessment

The NIST Cyber Security Framework was designed to assess where an organization is related to their cyber security and privacy protection status. The first step in creating a readiness assessment is to identify the organization's assets, critical systems, and data and need to be protected. Once that has been done, asses the organization's cyber security status by using the Tiers. This will identify the organization's current security controls and practices, as well as any gaps or vulnerabilities. Next, a risk management plan is created by creating a Profile. This should identify the organization's cyber security risks, assess the likelihood and impact of those risks, and develop controls to mitigate those risks. Depending on where the organization is ranked in the 1-4 "Tiers," implementation of a risk management plan includes implementing controls and monitoring the effectiveness of those controls. Lastly, review and improvement is a continual process. This is an ongoing process and should be revised and improved as the organization progresses towards Tier 4.

# 7 Using this Framework for Assessing Your MOD Project

The MOD Operational Readiness Framework provides a checklist for project leaders to assess the maturity or readiness of a deployment to be successful. Composed of technical, integration, institutional, and cyber security/privacy levels, the ORF highlights risks in deploying projects. Applying technologies that are not ready, integrations that do not meet needs, unresolved institutional issues, and inability to detect and respond to security breaches are areas addressed by this framework.

As mentioned in several of the assessment categories, the first step to using this assessment is to identify the technology components (technical), subsystems and their interactions (integration), and the stakeholders / business model your project is deploying (institutional). Once these readiness levels are identified and described, the cyber security and privacy risks may be assessed.

The *TRL Guidebook* recommends that a team of subject matter experts be assembled to review the results of the assessment. As shown in **Figure 6.**, the assessment should include four steps prior to conducting the review.

**Goals** – a clear, concise description of assessment review goals. The goals should frame the purpose and expected outcome of the review.

**Select SMEs** – Experts should represent the range of stakeholders associated with the deployment – technology, security, integration, data, policy, and operations.

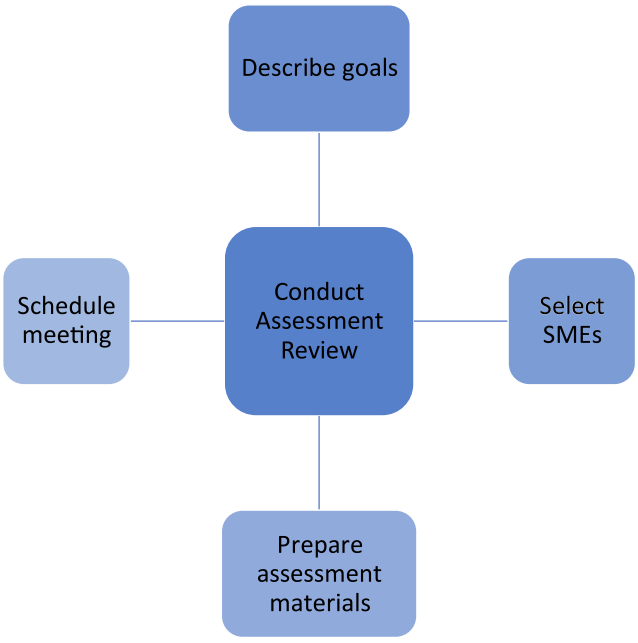


**Figure 6. MOD ORF Assessment.**

**Materials** – conduct the assessments by applying the project components to the readiness level checklists. Has each component sufficiently met the criteria identified in the readiness level for technical, integration, institutional and cyber security/privacy described in Sections 3 through 6?

**Schedule** – schedule the meeting at a time and location that is convenient for the participants.

The outcome of the meeting is to identify the readiness of the project to move forward, including recognizing gaps and areas of risk to the project's success and sustainability.

# 8 Acronyms

| Acronym | Description |
|---|---|
| **ConOps** | Concept of Operations |
| **CV** | Connected Vehicles |
| **CSF** | Cyber security Framework |
| **IRL** | Institutional Readiness Level |
| **ITS** | Intelligent Transportation Systems |
| **MaaS** | Mobility as a Service |
| **MAT** | Multimodal and Accessible Travel |
| **MOD** | Mobility On-Demand |
| **NIST** | National Institute of Standards and Technologies |
| **ORF** | Operational Readiness Framework |
| **PF** | Privacy Framework |
| **SDO** | Standard Development Organization |
| **TRL** | Technical Readiness Assessment |
| **USDOT** | United States Department of Transportation |
| **V2X** | Vehicle-to-Everything |
| **VRU** | Vulnerable Road User |

# 9 References

## 9.1 Publications

[1] USDOT, *Technical Readiness Level Guidebook*, FHWA-HRT-17-047. September 2017

[2] Framework for Integrating Emerging Trends and Technologies to Advance TSMO Programs (in development, USDOT)

[3] TCRP B-47 Impact of Transformational Technologies on Underserved Populations (Playbook, in development)

[4] Susan Shaheen, Adam Cohen, Jacquelyn Broader, Richard Davis, Les Brown, Radha Neelakantan and Deepak Gopalakrishna, Mobility on Demand Planning and Implementation: Current Practices, Innovations, and Emerging Mobility Futures, prepared for U.S. Department of Transportation Office of the Assistant Secretary for Research and Technology, Intelligent Transportation Systems Joint Program Office, March 2020, Report No. FHWA-JPO-20-792

[5] Susan Shaheen, Adam Cohen, Balaji Yelchuru, and Sara Sarkhili, Mobility on Demand Operational Concept Report, prepared for U.S. Department of Transportation, Intelligent Transportation Systems Joint Program Office, September 2017, Report No. FHWA-JPO-18-611

[6] Ivo Cré, Thomas Mourey, Alistair Ryder, Steve Heckley, and Mojca Balant, Institutional cooperation: Working jointly with institutional partners in the context of Sustainable Urban Mobility Plans, prepared for CH4LLENGE – Addressing Key Challenges of Sustainable Urban Mobility Planning, Grant Agreement No IEE/12/696/SI2.644740, March 2016

[7] Scott Baker, Viktor Zhong, Jerry Hsu, Patricia Macchi, Shawn Kimmel, Lindsay Gladysz, Mohammed Yousuf, Candace Groudine and Kenneth Wood, ATTRI Institutional and Policy Issues Assessment Summary Report, prepared for U.S. Department of Transportation Intelligent Transportation Systems Joint Program Office, February 16, 2017, Report No. FHWA-JPO-17-506

[8] Jana Sochor, "Fitting the Puzzle Together – Challenges and Opportunities for MaaS," International Transport Forum Discussion Papers, No. 2021/08, OECD Publishing, Paris. https://www.itf-oecd.org/integrating-public-transport-mobility-service-maas-roundtable

[9] Dalia Mukhtar, MariAnne Karlsson, Till Koglin, Annica Kronsell, Emma Lund, Steven Sarasini, Göran Smith, Jana Sochor and Björn Wendle, "Institutional conditions for integrated mobility services (IMS): Towards a framework for analysis," Institutional fRameworks for Integrated Mobility Services (IRIMS) project, 2016-10-28

[10] Taehyung Kim, Ho Lee, Hyunju An, Jaehyun So, Felipe Targa, Seunghyun Kim and Jeongjin Oh, "Readiness Assessment Methodology for Smart Mobility," International Joint Research Series on Future Mobility (III), Copyright © 2020 by The Korea Transport Institute

[11] National Institutes of Standards and Technology's (NIST) Cyber Security Framework (CSF) and Privacy Framework (PF)

## 9.2 References / Endnotes


[1] Baker, S., Zhong, V., Hsu, J., Macchi, P., Kimmel, S., Gladysz, L., Yousuf, M., Groudine, C. and Wood, K., "ATTRI Institutional and Policy Issues Assessment Summary Report," prepared for U.S. Department of Transportation Intelligent Transportation Systems Joint Program Office, February 16, 2017, Report No. FHWA-JPO-17-506

[2] Dalia Mukhtar, MariAnne Karlsson, Till Koglin, Annica Kronsell, Emma Lund, Steven Sarasini, Göran Smith, Jana Sochor and Björn Wendle, "Institutional conditions for integrated mobility services (IMS): Towards a framework for analysis," Institutional Frameworks for Integrated Mobility Services (IRIMS) project, K2 Working Papers 2016:16, 2016-10-28

[3] Emma Lund, Johan Kerttu and Till Koglin, "Drivers and Barriers for Integrated Mobility Services: A review of research," Institutional Frameworks for Integrated Mobility Services (IRIMS) project, K2 Working Papers 2017:3, 2017-04-25

[4] Ivo Cré, Thomas Mourey, Alistair Ryder, Steve Heckley, and Mojca Balant, "Institutional cooperation: Working jointly with institutional partners in the context of Sustainable Urban Mobility Plans," prepared for CH4LLENGE – Addressing Key Challenges of Sustainable Urban Mobility Planning, Grant Agreement No IEE/12/696/SI2.644740, March 2016

[5] Shaheen, S., Cohen, A., Yelchuru, B. and Sarkhili, S., "Mobility on Demand Operational Concept Report," prepared for U.S. Department of Transportation, Office of the Assistant Secretary for Research and Technology, Intelligent Transportation Systems Joint Program Office, September 2017, Report No. FHWA-JPO-18-611

[6] Shaheen, S., Cohen, A., Broader, J., Davis, R., Brown, L., Neelakantan, R., and Gopalakrishna, D., "Mobility on Demand Planning and Implementation: Current Practices, Innovations, and Emerging Mobility Futures," prepared for U.S. Department of Transportation, Office of the Assistant Secretary for Research and Technology, Intelligent Transportation Systems Joint Program Office, March 2020, Report No. FHWA-JPO-20-792, page 2

[7] Ibid, page 15

[8] Martin Sparks, "4 basic business models in e-commerce," Firmbee, July 21, 2022, https://firmbee.com/4-basic-business-models-in-e-commerce

[9] Shaheen, S., Cohen, A., Broader, J., Davis, R., Brown, L., Neelakantan, R., and Gopalakrishna, D., Ibid, page 16

[10] Ivo Cré, Thomas Mourey, Alistair Ryder, Steve Heckley, and Mojca Balant, Ibid

[11] National Institute of Standards and Technology, 2018. *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology (NIST) available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] Ibid.