

Emergency Management Systems Interoperability Framework

Overview

M. Abramson, ASMG Ltd.

Version 0.51

[Type the abstract of the document here. The abstract is typically a short summary of the contents of the document. Type the abstract of the document here. The abstract is typically a short summary of the contents of the document.]

Change History

Version	Description	Date /Author



Executive Summary

Public safety and emergency managers and government decision makers require timely access to relevant and accurate information in order to exercise their mandates and responsibilities. Improving the quality of information, and making that information “discoverable”, “accessible”, and “understandable” has long been the target of the public safety and emergency management communities, decision makers and stakeholders. The ability to share and access information across a number of heterogeneous organizations, systems and services is commonly referred to as “interoperability”. But, as desirable and interoperability is to stakeholders, the ability to achieve interoperability within an agency, let alone a diverse community of agencies has been difficult to achieve.

With the objective of delivering voice and information interoperability, Public Safety Canada (PSC), with the support of Defence Research and Development Canada (DRDC) has initiated the development of the Emergency Management Systems Interoperability (EMSI) Framework (EMSIF). The EMSIF will provide a foundation of architectural and engineering concepts and practices that will enable participating agencies to develop (/acquire) capabilities, systems and services that can

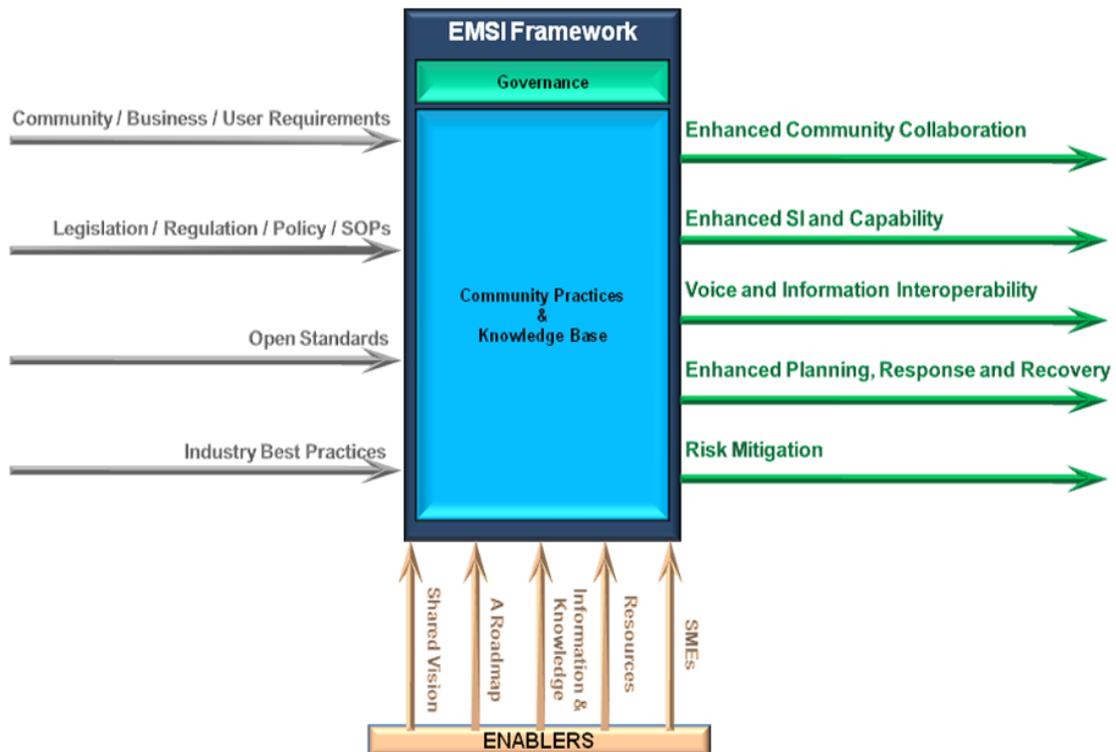


Figure 0-1: EMSI Framework Context Diagram

better interoperate with the broader Emergency and Public Security communities. Additionally, these well established practices could assist agencies with their own internal needs for enhanced information sharing and interoperability.

PSC plans to achieve its objectives the adoption of community practices and standards that are vetted through established governance structures and supported by community resources. Individual agencies will have the option to align with the EMSIF elements in accordance with their legislative mandates and priorities. As an incentive for agencies to align, PSC will provide access to EMSIF knowledge based resources through a Web Portal, and where possible, provide accesses to community tested applications and services that deliver capabilities, systems, services and application that will allow rapid agencies to interoperate.

The EMSI Framework (EMSIF) has been divided into the following element:

1. Governance;
2. Knowledge base:
 - a. Practices, Processes and Tools,
 - b. Standards,
 - c. Profiles and Guidance,
 - d. Architecture Models, and
 - e. Training and Exercise Data;
3. Supporting Services:
 - a. Interoperability Continuum;
 - b. Support Infrastructure;
 - c. Capability/Performance Metrics; and
 - d. Architecture Framework.

Each of these elements is outlined in section 3 of this document.

Table of Contents

Change History	2
Executive Summary.....	3
Table of Contents.....	5
1 Introduction	5
1.1 Scope.....	6
1.2 Objectives for the EMSIF.....	7
1.3 EMSI Challenge	7
1.4 Emergency Management System Interoperability.....	8
1.5 System Interoperability.....	9
1.6 Guiding Principles for EMSI.....	10
1.7 <i>Related Documents</i>	10
1.8 Document Overview	11
2 EMSIF Elements.....	12
2.1 Governance.....	14
2.2 Knowledge Base	17
2.2.1 Practices, Processes and Tools.....	17
2.2.2 Standards.....	17
2.2.3 Profiles and Guidance.....	18
2.2.4 Architecture Models	18
2.3 Interoperability Continuum	18
2.4 Support Services	20
2.5 Capability/Performance Metrics.....	22
2.5.1 Self Assessment.....	22
2.5.2 Community Assessment.....	22
2.5.3 Continuum Dashboard.....	22

2.6	Architecture Framework.....	23
3	Implementation support.....	28
3.1	<i>Working Groups</i>	28
3.1.1	<i>Central Activities</i>	28
3.1.2	Communications and Networks.....	28
3.1.3	Middleware	28
3.1.4	Information Services	28
3.1.5	Interoperability Domain Models.....	28
3.1.6	Schema and RDF specifications.....	29
3.1.7	Web Services and Browser Plug-ins.....	30
3.1.8	Risk Mitigation Prototypes.....	Error! Bookmark not defined.
3.1.9	Test Reference System(s).....	Error! Bookmark not defined.
3.2	<i>EMSI Metadata Standards</i>	30
3.3	EMSIF Development Timeframe.....	30
4	Roles and Responsibilities.....	31
4.1	<i>PS Interoperability Directorate</i>	31
4.2	DRDC CSS.....	31
4.3	<i>Public sector organisations</i>	31
4.4	<i>Senior IM/IT Committees</i>	32
4.5	Working Groups (Terms of Reference for Each WG need to be developed)	32
4.5.1	<i>EMSIF Working Group</i>	32
4.5.2	<i>System Architecture Working Group (SAWG)</i>	32
4.5.3	<i>XML Schema Working Group (XSWG)</i>	32
4.5.4	<i>Information and Metadata Management Working Group (IMMWG)</i>	33
4.5.5	Testing and Demonstration Working Group (TDWG).....	33
4.5.6	<i>Other working groups</i>	34
5	Change management	35

5.1	Change Cycle	35
5.2	Management of Change	36
5.3	Compatibility with Legacy	36
5.4	Open Standards and Architecture	36
5.5	Agency Specific and Peer-to-Peer Adaptations	36
5.6	XML Message Schemas	36
5.7	<i>EMS resource owner</i>	37
5.8	<i>Consultation and innovation</i>	37
	<i>Request for Comments</i>	37
	<i>Request for Proposals</i>	37
6	Aligning to EMSIF	39
6.1	<i>What does Alignment Mean?</i>	39
6.2	<i>Alignment Timetable</i>	39
6.3	<i>Stakeholders</i>	39
6.4	<i>Alignment responsibilities</i>	40
6.5	<i>Aligning to new versions of the EMSI Framework</i>	40
6.6	<i>Additional guidance</i>	41
7	Glossary	42
8	Attachment 2: Definitions.....	44
8.1.2	Application Interoperability	50
8.1.3	Security Interoperability	50
8.1.4	SOP Interoperability.....	50
8.1.5	Governance Interoperability.....	51

1 Introduction

Modern emergency management demands ready access to quality information that enables decision makers to effectively respond to dynamic real world events; where quality information is categorised as:

- **Accurate:** semantics to accurately convey the perceived situation.
- **Relevant:** information tailored to specific requirements of the mission, role, task or situation at hand.
- **Timely:** information flow required to support key processes, including decision making.
- **Usable:** information presented in a common, easily understood format.
- **Complete:** information that provides all necessary (or available) information needed to make the decision.
- **Brief:** information tailored to the level-of-detail required to make decisions and reduces data overload.
- **Trustworthy:** information quality and content can be trusted by stakeholders, decision makers and users.
- **Secure:** Information is protected from inadvertent or Malicious Release.

Delivering quality information to stakeholders and decision makers will require deployment of information, network and communication systems that have the capacity, when needed, to interact in a seamless and coherent manner across the three levels of Government, the Private Sector and the General Public. As illustrated in Figure 1-1, the EMSI initiatives will seek to realign policies, practices, systems and services in areas between jurisdictions and mandates. It will provide agencies with mechanisms to de-compartmentalize capabilities and provide the ability to rapidly align agency capability with other community systems; while preserving the ability of agencies to exercise legislated mandates and priorities.

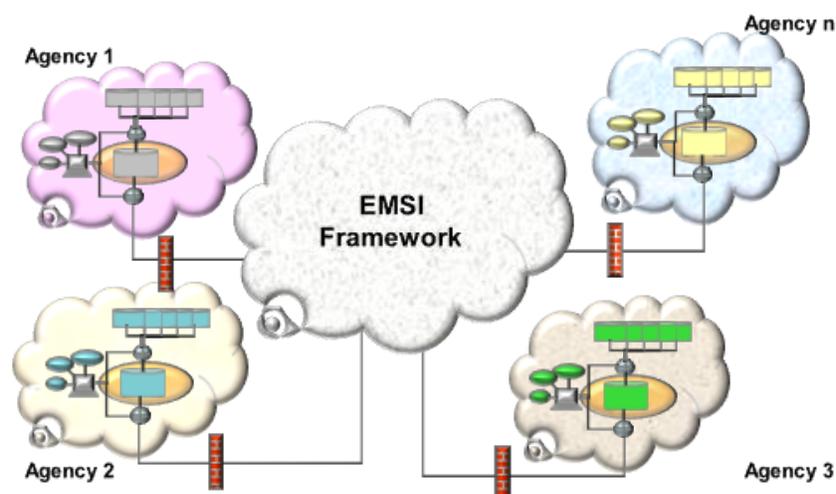


Figure 1-1 – EMSIF Operating Between the Defined Agency Domains

The Emergency Management System Interoperability (EMSI) Framework (EMSIF – Figure 1.2) represents GC capability to catalogue and characterise applicable policies, standards, best practices and technologies that will allow organizations, systems and services to interoperate.

“System Interoperability” is the ability of heterogeneous systems to work together (inter-operate).

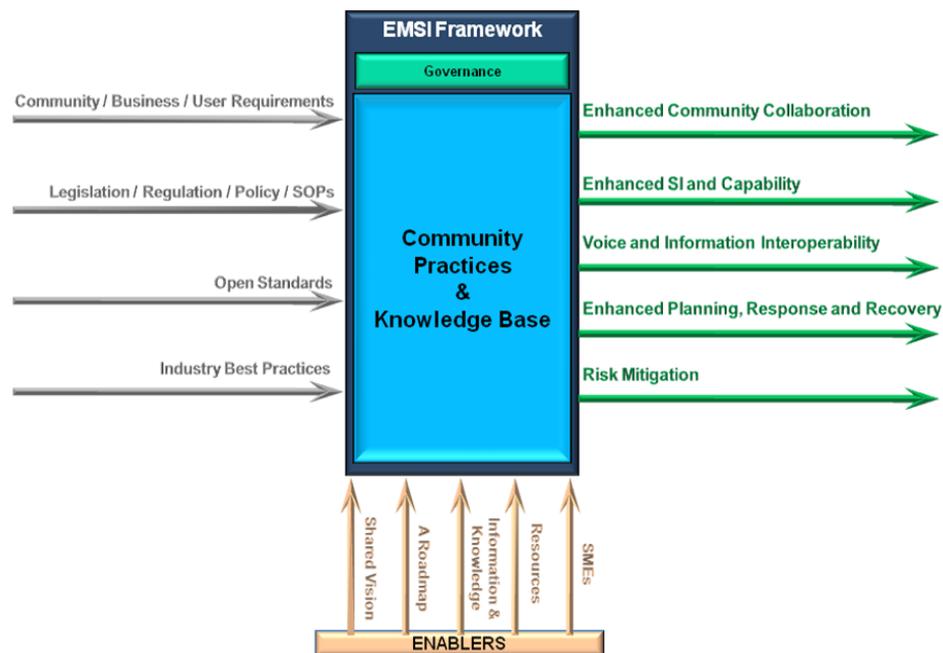


Figure 1-2– EMSI Framework

1.1 Scope

This document describes the elements of the Emergency Management System Integration (EMSI) Framework; as illustrated in Figure 1-2. As illustrate the Framework provides a governance structure for the identification and ratification of Governments of Canada (GC) Emergency Management (EM) community practices for the development of interagency system interoperability. In addition this governance structure will assess and ratify the information and knowledge base supporting the development of these capabilities.

1.2 Objectives for the EMSIF

The objectives for the EMSIF were gathered during a 2009 workshop conducted by public Safety Canada in Ottawa, and attended by some fifty members of the Emergency Management and Public Security Communities. The defined objectives included::

- Improve information quality during the planning, response and recovery from an emergency or public security incident; and enhance decision making;
- Enhance the Government(s) of Canada’s ability to effectively plan, execute and monitor the operational situation and coordinate support for the accomplishment of operational objectives while adapting to changing situations.
- Leverage community developed capabilities:
 - Capabilities, resources and systems.
 - Common of the shelf capability (e.g., Google Earth, Bing Maps),
 - SAFECOM
 - Open-standards and publically accepted specifications,
 - National Information Exchange Model,
 - Common Alerting Protocol (Canadian Profile),
 - Shared Operational Picture Exchange Services.
 - Off-the-shelf and open-source solutions (e.g., Multi-Agency Situational Awareness System (MASAS)).
- Allow agencies to evolve capability based on mandates and priorities; aligned to a shared vision of interoperability.
- Integrate lessons-learned into the EMSI development portfolios of the participating agencies.

1.3 EMSI Challenge

During the planning, response and recovery phases of emergency and public security events, the effective sharing of *quality information* is critical. Situational (/domain) awareness, operational planning and coordination, and decision making are all dependent on the availability of timely and accurate information. This information comes from a host of different sources; and increasingly these sources are crossing organizational, agency and international boundaries. Traditional organization centred approaches to capability development and portfolio management can no longer support the Emergency and Public Security communities and there growing cross domain requirements.

It has been broadly reported (e.g., 9-11, Katrina, tsunami, SARS, and the 1998 Ice Storm) that information sharing within and between agencies has not been effective. The EMSIF Vision

Document outlines the challenges face by the communities. Current legislation, policy, capability, systems and services are severely limited in their ability discover, exchange and use information, critically limiting the planning, response and recovery capabilities of community. In many instances, emergency and public security organizations do not even have the capacity to identify, evaluate and exploit advancing capabilities (practices, standards and technologies).

In response, some have called for a single integrated EM capability for Canada. This goal, though laudable, is likely not achievable in a foreseeable timeline. The goal of an integrated EMS crossing all three levels of government and international partners (e.g., United States) runs the hurdles of multiple international agreements, legislative mandates, policies, cultures and procurement regimes. Each would require a major overhaul to achieve a fully integrated environment.

Based on this assessment, a concurrence of many in the community, Public Safety Canada is targeting “**INTEROPERABILITY**” of information sharing (both Voice and Data) using current and evolving international standards. It is through adoption of these standards that PSC sees convergence on the core EM capabilities, systems and services, and acceptance by a large cross-section of stakeholders, agencies and vendors. The adoption of these standards will allow multiple vendors to develop off-the-shelf systems and services that can inherently interoperate across the voice and data domains.

1.4 **Emergency Management System Interoperability**

Emergency Management System Interoperability requires a collaborative effort between large number of agencies, crossing all three levels of government, the private sector, academia and international partners. Government agencies, in particular, are seeking commercial-off-the-shelf (COTS) products that plug and play with each other, legacy applications and partner deployed capability systems and services. These same agencies are also seeking continual innovation and adaptation of capability to changing operational needs (/threats), legislated mandates, and demands of citizens. They are seeking flexible, agile systems, services and networks that can dynamically adapt to real world changes (e.g., new threats, multiple events, additional/new operational partners and/or escalation in scale, complexity and/or severity of the event), while maintaining information security, confidentiality and privacy. New capability must be deployed in an evolutionary manner, without imposing a detrimental impact on existing capability.

Traditional IM/IT development provides static, predefined solutions to fixed requirements; typically taking months or years to deploy; and rarely delivering full capability, on-time and on budget. The modern environment cannot operate under these traditional constraints. PSC is seeking new and innovative strategies, practices, standards and technologies to address these real-work challenges. The EMSI provides the foundation for these efforts.

1.5 System Interoperability

There are quite a number of definitions for the term “system Interoperability”:

1. (military¹) the ability of different forces to exchange services so as to operate effectively together.
2. (computing²) the ability of software systems that may be running under different operating systems and hardware to exchange information through compliance with technical [interoperability] specifications, which typically define how different file formats and messaging protocols can work together.
3. (Wikipedia³) is a property referring to the ability of diverse systems and organizations to work together (inter-operate). The term is often used in a technical systems engineering sense, or alternatively in a broad sense, taking into account social, political, and organizational factors that impact system to system performance.
4. (OSD⁴) The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces, and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. (DoDD 5000.1).
5. (SAFECOM⁵) Interoperability refers to the ability of emergency responders to work seamlessly with other systems or products without any special effort. Wireless communications interoperability specifically refers to the ability of emergency response officials to share information via voice and data signals on demand, in real time, when needed, and as authorized.

In more general terms, “System Interoperability” refers to the ability of heterogeneous systems (mechanical, electronic, communications and information) to work together (inter-operate). More broadly, Interoperability can take into account social, political, and organizational factors that impact system(s) ability to interoperate with other systems.

In a loosely coupled environment of a service-oriented architecture, individual systems do not need to know the details of how other systems work, but enough common ground (interface specification or contract) that enables a reliably exchange messages without error or misunderstanding. Standardized specifications go a long way towards creating this common ground, but differences in implementation may still lead to breakdowns in communication or interoperability.

The ultimate test for interoperability is the *coherent exchange of information and/or services between agencies and systems*. It must also be possible to *replace any component or product with another that adheres to the common interface specification (/contract)*.

¹ <http://en.wiktionary.org/wiki/inter-operability>

² <http://en.wiktionary.org/wiki/inter-operability>

³ <http://en.wikipedia.org/wiki/Interoperability>

⁴ <http://www.acq.osd.mil/osjtf/termsdef.html>

1.6 Guiding Principles for EMSI

The following statements represent the key decisions that have shaped the EMSIF:

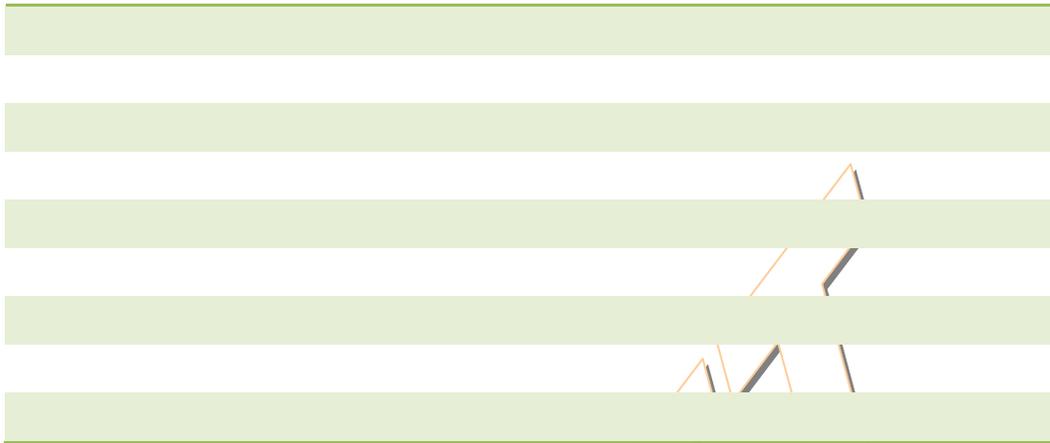
Policy	The EMSIF will align government legislation and policy with information sharing needs of the emergency management, and public safety and security of the communities.
Information Protection and Security	All framework elements will align to best practices and standards for Information security and protection for sensitive information (classified, private and confidentiality).
Open Standards	The EMSIF elements will align to open-standards and publically accepted specifications (PAS). Where require the EMSIF Working group will would with standards bodies to develop and issues open community standards. The adoption of Open Standards will yield more commercial off the shelf and open-source options for the community; better controlling development and life-cycle cost and increased innovation in the environment.
Architecture	The EMSIF will incorporate best industry best practices in the development of segment architecture for community capabilities. The EMSIF is seeking to adopt The Open Group Architecture Framework (TOGAF), DOD Architecture Framework (DODAF) and Unified Profile for DODAF and MODAF (UPDM). This approach appears consistent with the efforts of TBS and the community partners in DHS.
Flexibility and Agility	Specifications that demonstrate the ability to adapt to rapid changes in operations conditions without impact to other aspects of the environment.
Scalability	Specifications that have the capacity to be scaled to satisfy changed demands made on the system, such as changes in data volumes, number of operational nodes.

1.7 Related Documents

The following document support the discussions presented in this document:

Reference	Title	Version / Date
EMSI-1	EMSIF Vision Document	Version 0.52

⁵ <http://www.safecomprogram.gov/SAFECOM/interoperability/default.htm>



1.8 Document Overview

This document is intended to identify and briefly describe the core elements of the Emergency Management System Interoperability Framework (EMSIF). As work progresses, thinking evolves and business requirements become more descriptive, these elements will be expanded and detailed in supporting documents.

This document contains are seven sections:

Sections 1 Introduction	Introduces the elements of the EMSIF and identifies supporting efforts and materials incorporated into the framework.
Section 2 EMSIF Elements	Briefly describes each of the framework elements.
Section 3 Implementation Support	Briefly outlines the implementation support PSC and DRDC CSS are planning to provide the EM community in order promote EM system interoperability.
Section 4 Roles and Responsibilities	Briefly outlines the roles and responsibilities of organizations under this framework.
Section 5 Change Management	Briefly describes the change and configuration management practices to be applied under this framework.
Section 6 How EM agencies Align to the EMSI	Briefly outlines the community expectations for agencies seeking to align to the EMSIF.

2 EMSIF Elements

As illustrated in Figure 2-1, the EMSIF comprises xx elements, including:

- Governance
- Knowledge base:
 - Practices, Processes and Tools
 - Standards
 - Profiles and Guidance
 - Architecture Models
 - Training and Exercise Data
- Supporting Services
 - Interoperability Continuum
 - Support Infrastructure
 - Capability/Performance Metrics
 - Architecture Framework

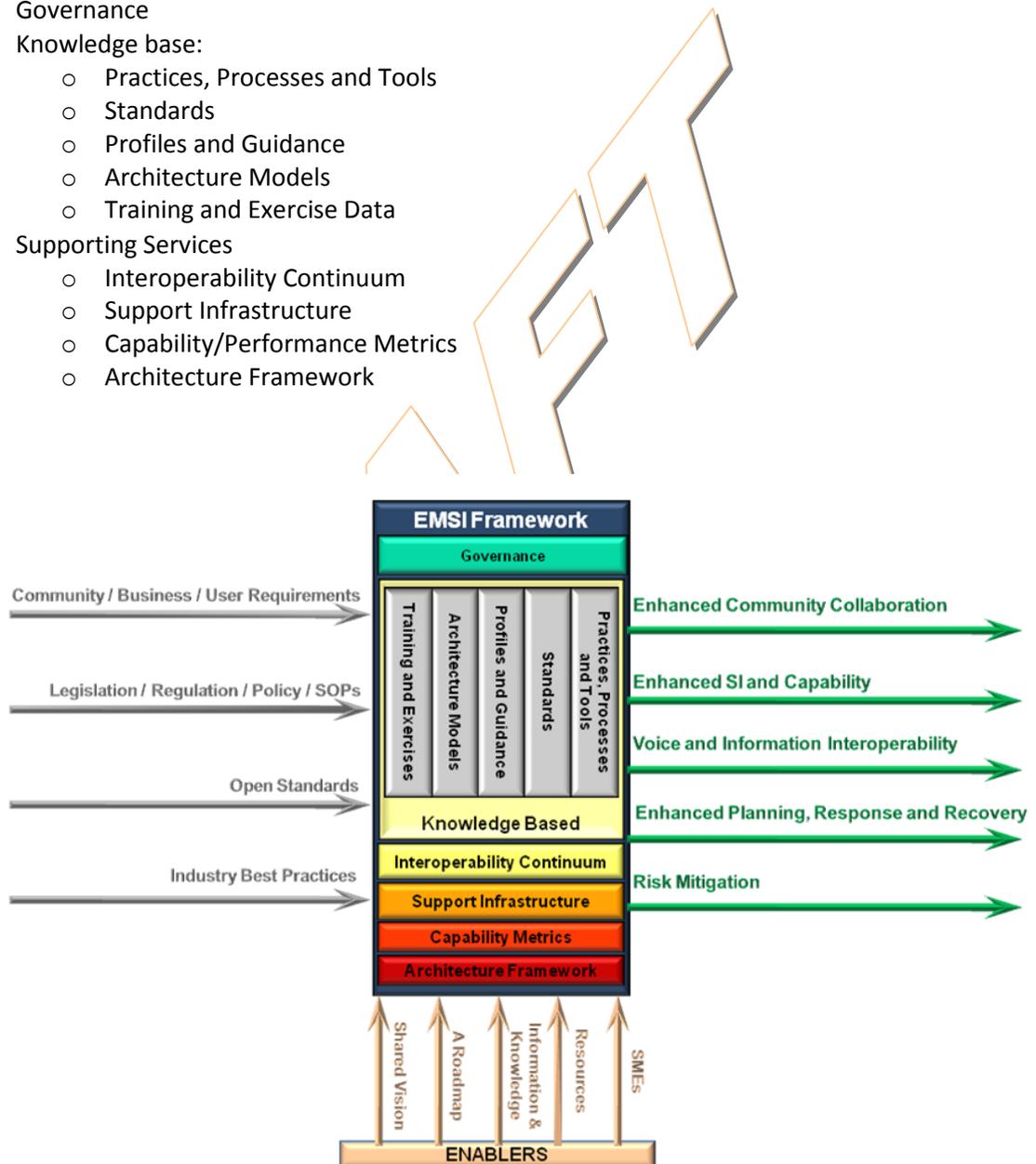


Figure 2-1 EMSI Framework Context

The following table identifies and briefly describes the core elements of the EMSI framework.

	Core Element	Description
	Governance	Community defined practices, procedures, technologies and organizational authorities to assess and certify the resources comprising the EMSI framework.
Knowledge Base	Practices, Processes and Tools	Community adopted practices, processes and tools that support the specification, development/acquisition, deployment and operation of interoperable EM and PS capabilities, systems and services.
	Standards	Community adopted process, architecture and technical standards and publically accepted specifications. The EMSIF will collate the standards and specifications adopted under the EMSIF governance regime.
	Profiles and Guidance	The EMSIF will publish a catalogue of standards, specifications, best practices, et... that have been adopted by the community.
	Architecture Models	Community and stakeholder developed and published architecture models and supporting information describing their contributions to overall PS and EM Capability. These model would be made availability for analysis and use by targeted groups to guide the development of interoperability capability.
	Training and Exercise Materials	Community adopted practices, processes, guidance and datasets that enable the community to evolve its capacity to train and exercise at the local, regional and national levels.
Support Services	Interoperability Continuum	Community dashboard that illustrates progress along a continuum of capability. The continuum seeks to present capability in a manner that: <ul style="list-style-type: none"> • Simply illustrate the state of interoperability to stakeholder, decision makers and planners. • Foster understanding and collaboration across disciplines. • Foster commitment to resource allocations from policy makers, stakeholders, planners. • Promotes the regular use interoperability solutions and capabilities.

	Core Element	Description
		<ul style="list-style-type: none"> • Enable planning and budgeting for ongoing enhancements to systems, procedures, and documentation. • Align elements across Interoperability Continuum elements.
	Support Infrastructure	<p>Community supported capabilities that bridge the processes, systems and services delivered by each of the participating members.</p> <p>Where needed and appropriate the GC will develop and community enabling technology and infrastructure. The EMSIF will document the technical information needed by stakeholders to align their internal capabilities to these technologies and infrastructure.</p>
	Capability Metrics	A set of self performance and assessment metrics (against architectural elements) that enables an assessment of progress along the elements of the interoperability continuum.
	Architecture	Practices, procedures and technologies that enable the capture, maintenance and dissemination of segment architectures that describe the business/operations needs, capabilities, systems and services being developed and deployed by the participating agencies..

2.1 Governance

Within the context of the EMSIF, “Governance” comprises the organizational structures, business processes, information and services that inform, direct, manage, and monitor the development of the elements that comprise the EMSIF.

As illustrated in Figure 2-2, Oversight and Governance processes draw on the data deliveries of processes such as Life-cycle management, enterprise architecture, systems delivery and project

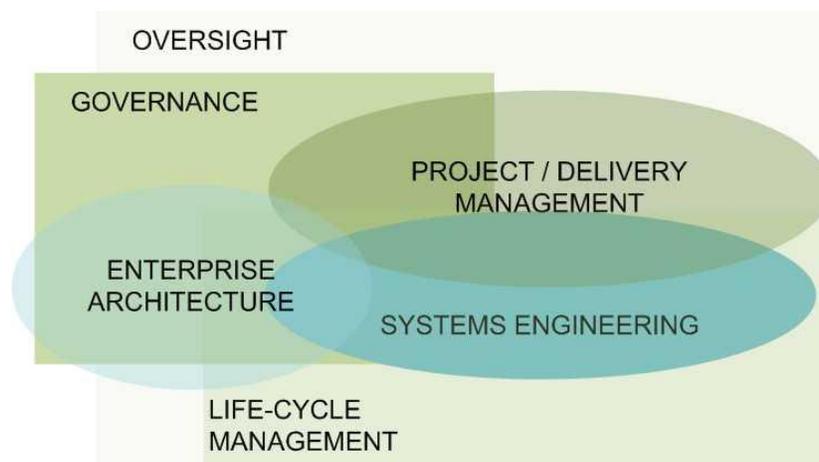


Figure 2-2 Interdependent Information Environment

management. Standards are needed for the delivery of this information to ensure that governance structures have insight into the evolution of the EM capability direct and manage activities and resources. Figure 2.1 illustrates the overlap on information domains applicable to the governance of EMSIF delivery.

DRAFT

Governance elements of the EMSIF will comprise:

Governance Structure⁶

The organizational structure for the EMSIF will comprise stakeholder supported committees and the EMSI working group. The EMSI WG will align with existing GC IM/IT committees including:

- CIO Council
- Business IM/IT Council
- IM/IT Investment Committee
- IM/IT Architecture and Standards Committee
- Management of Government Information
- TBSCIOB
- Department CIO
- CSEC (C&A, Common Criteria)

The EMSI Working group provides first level oversight and coordination of the other EMSI working parties, which has the responsibilities for identifying, assessing and recommending (for adoption) the artefacts comprising the knowledge base and support services. and Working Parties (WP), including:

- Domain Models Working Party (DMWP)
- Architecture Working Party (AWP)
- Metadata Working Party (MDWP)
- XML Working Party (XMLWP)
- Performance Measures and Interoperability Continuum Working Party (PMICWP)

Governance Domain Model⁷

The EMSIF Working Group will develop and maintain a governance domain model describing the information requirements of the governance processes for the EMSIF. This domain model defines key aspects of the EMSIF Knowledge Base.

Governance Tool Specifications

The EMSIF Working Group will develop specifications and demonstrations for knowledge management tools and decision aids that assist community members in the assessment of their capability against the stated objectives of the communities of interest and practice comprising supported by the Government(s) of Canada. Off interest are tools that support:

1. PSC Interoperability Continuums; and
 2. System Certification.
-

⁶ As of the issuance of Version 1 of this document this element was not completed. The initial three month definition phase did not have the time nor resources to define the EMSIF governance structure. Completion of this work is included in the EMSIF Road Map.

⁷ As of the issuance of Version 1 of this document this element was not completed. . The initial three month definition phase did not have the time nor resources to define the EMSIF governance Domain Model. Completion of this work is included in the EMSIF Road Map.

2.2 Knowledge Base

2.2.1 Practices, Processes and Tools

The EMSIF will collate government and industry best practices, processes and tools that support capability planning, specification, implementation, deployment and maintenance of EMSI Capabilities, systems and services. The policies practices and tools will be used during the development of community capabilities and offered to participating agencies for their consideration and adoption.

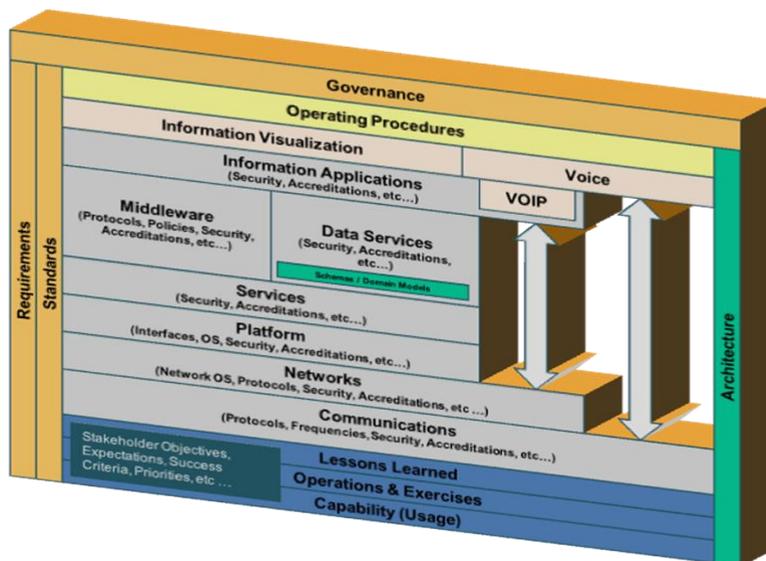
Where needed the EMSI Working Group (see section 5) will provide guidance on the use of the practices, processes and tools that better align the efforts of the community. The goal for these elements of the knowledge Base is the development of reusable architecture and engineering artefacts (e.g., Government open applications, Operational models, and interface specifications and designs).

2.2.2 Standards

The EMSIF will collate government and open industry standards that enable the planning, specification, implementation, deployment and maintenance of EMSI Capabilities, systems and services. Standards will be selected and recommended for each of the system domain illustrated in Figure 2-x.

The EMSIF Working Group will maintain a registry of adopted standards on an EMSIF portal.

Standards bodies being focused on include: TBS, NIEM, OASIS, ISO, The Open Group, and OMG; ach



is working on standards and open specification with direct applicability to the development of interoperable capabilities, systems and services for EMS and Public Security.

2.2.3 **Profiles and Guidance**

The EMSIF working group will develop or adopt implementation profiles and guidance describing how the community will adopt and adapt best practices, tools and standards to the operational needs of the EMS and public security community.

As good example of a profile is the Canadian Profile for the Common Alerting Protocol (CAP). The original CAP was developed by Organization for the Advancement of Structured Information Standards (OASIS).

2.2.4 **Architecture Models**

Architecture is a conceptual blueprint that defines the structure and operation of an architectural element (e.g., organization, capability, system or service). The intent of architecture is to determine and document how architectural elements can most effectively achieve its current and future business (/operational) objectives. Architecture contains several view-points addressing business/operational, system/application, information, security and the technology perspectives. Sharing architectural view-points, specifications and components will improve decision making, reduce resource requirements, and improve organizational adaptability to changing demands or operational conditions; eliminating of inefficiencies and redundant processes; and optimizing the use of organizational resources.

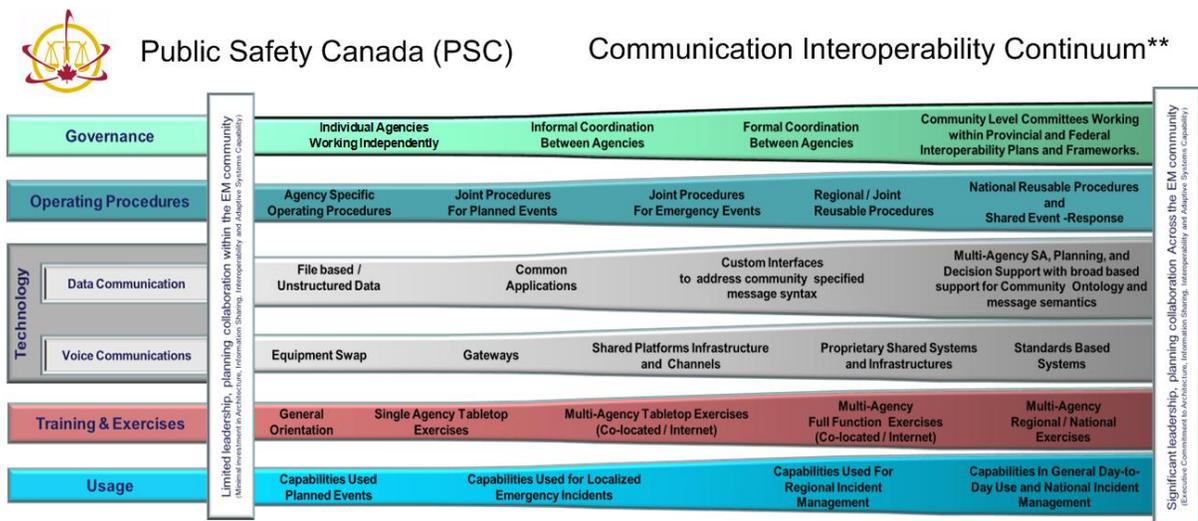
The EMSIF knowledge based will collate architectural artifacts, developed by the GC, industry and academia on behalf of the EM and PS communities. The artifacts will describe capabilities currently deployed and/or in development by community members.

The Metadata Working Group will develop and publish an architecture domain meta-model defining the architecture information requirements of EMSI. This domain model will be used to outline the architecture information that needs to be shared amongst EM community members to enable EMSI. This model will identify the element of the platform independent, platform specific and physical (code) models the will be hosted on the EMSIF portal.

2.3 **Interoperability Continuum**

The Emergency Management System Interoperability (EMSI) Continuum (Figure 2-4) initiative seeks to provide Public Safety (PS) Canada with the ability to define continuum for system interoperability that enables an incremental enhancement of community interoperability across the communication, network, information and process domains.

By providing the community consistent and comprehensive set of practices, strategies and guidance, the EMSI Framework will promote a whole of government approach to the management and execution of information sharing during the planning, execution and recovery phases of EM and PS operations. Participating agencies and stakeholders will have a consistent way of tackling common issues which cross multiple agency mandates and track progress in the resolution of these issues. Most of the practices and standards being adopted by the EMSIF team are based on Treasury Board guidance and well established industry practices, capability and tools. Because of this approach, many of the recommended practices can be readily adopted by community members as the EMSIF evolves a real capability. Training and subject matter expertise is readily available



** Information in this diagram is based on the Department of Homeland Security Interoperability Continuum)

Figure 2-4 EMSI Communication Interoperability Continuum

from multiple government and commercial agencies.

Using the guidelines and metrics being developed by Public Safety participating agencies will have the capacity to self assess their capability against the established targets for Communications Interoperability. The goal is to provide stakeholders with the ability to identify, prioritize and acquire (/develop) interoperability within well defined capability portfolio; one that reflects their legislative mandates and priorities.

Public Safety is also investigating extensions to the continuum (Figure 2-5) that will enable assessment versus the information interoperability goals and objects currently being developed.

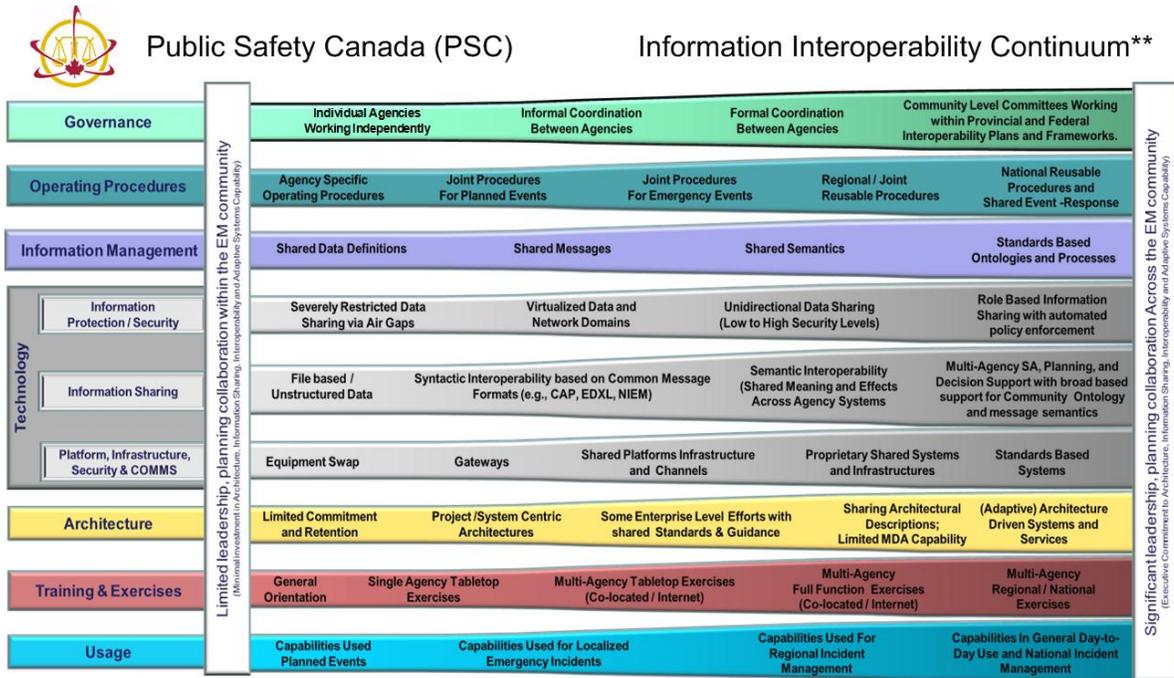


Figure 2-5 - EMSI Communication Interoperability Continuum

2.4 Support Services

It is anticipated that Public Safety will develop a set of support services to aid in the development and management of EMSI capability portfolios. The following table briefly describes several of the projected services. Detailed specifications for the development (acquisition and integration) will be identified in the EMSIF Capability road map.

Item	Description
Web Portal	All materials maintained as part of the EMSI “Knowledge Based” w
Decision Support Services and Aids	The EMSIF will specify a set of decision aids to support the governance process. These services will enable the use of architecture data to determine the alignment of an agencies policies, procedures, systems, services and information to the EMSIF. <ul style="list-style-type: none"> Audit Services: The EMSIF will specify and deliver a set

Item	Description
	<p>of audit services to gather metrics on the effectiveness of the EMSI effort. Embedded metrics gathering into the Audit and Accounting Services, to collect metrics designed to measure levels of interoperability and agency alignment to the EMSIF.</p> <ul style="list-style-type: none"> Certification and Accreditation Services The EMSIF will specify and deliver a set of C&A services to aid agencies and projects collect the data requisite to the successful completion of the C&A and Delta-C&A requirements. This will include decision aids that report on agency alignment to EMSIF standards, specifications and guidance. Statement of Sensitivity Service The EMSIF will specify and deliver a set of C&A services to aid agencies and projects in the development of statements of sensitivity prior to the release of sensitive information holdings. Threat Risk Assessment Services The EMSIF will specify and deliver a set of C&A services to aid agencies and projects perform a Threat Risk Assessment prior to the release of sensitive information holdings, deployment of new capability, or the modification of existing capability.
<p>Community Supported Applications</p>	<p>The EMSIF WG will collate and publish community sponsored (government open) standards based applications that deliver elements of communication and information interoperability, Situational Awareness and collaboration.</p> <p>This part of the knowledge base and support services will seek open-source and shareware applications that are vetted by the community as providing basic or core capability for those agencies that do not have the resources to develop specific capabilities (often low priority for day-to-day operations) or acquire Commercial off the shelf (COTS) applications which tend to be fairly expensive to integrated and customize.</p> <p>The EMSIF WG will be seeking Web enabled applications for at least basic SA and collaboration services.</p>

2.5 Capability/Performance Metrics

2.5.1 Self Assessment

The EMSIF working group will be seeking to develop a set of capability/performance metric that participating members can use to assess their ability to interoperate with members of a specific community of interest or practice. The goal is for participating agencies to self-assess in support of their capability road map. The measures will be structure in a manner that facilitates both a measure of capability related to internal agency interoperability and another measure for an agency’s ability to interoperate with other community measures.

This will provide stakeholders with a consistent way to track and reports the progress of their capability development portfolios.

2.5.2 Community Assessment

An additional set of metrics will be developed to assist in measuring overall community capability to interoperate during an exercise or operation. Some care will be taken to assure that the resulting assessments target a measure of progress versus stated goals of community wide capability management activities; and not specifically pointing a specific challenges. There are many contributing factors underlying the performance of a specific agency, organization and/or unit – including: legislated mandate, business and operational priorities, available technology, and resources availability. The metric and assessment short focus on overall challenges and where resources, if applied, could provide the most benefit, to the broadest cross section of the community.

Of primary interest is the identification of areas where Science and Technology resource could be most effective in mitigating risk (business, operational and technical) for the community as a whole.

2.5.3 Continuum Dashboard

The capability and performance metric will be developed in a manner that facilitates the presentation of capability and capability targets against the PSC Interoperability Continuum. Figure 2-5 illustrates what a dashboard might look like.

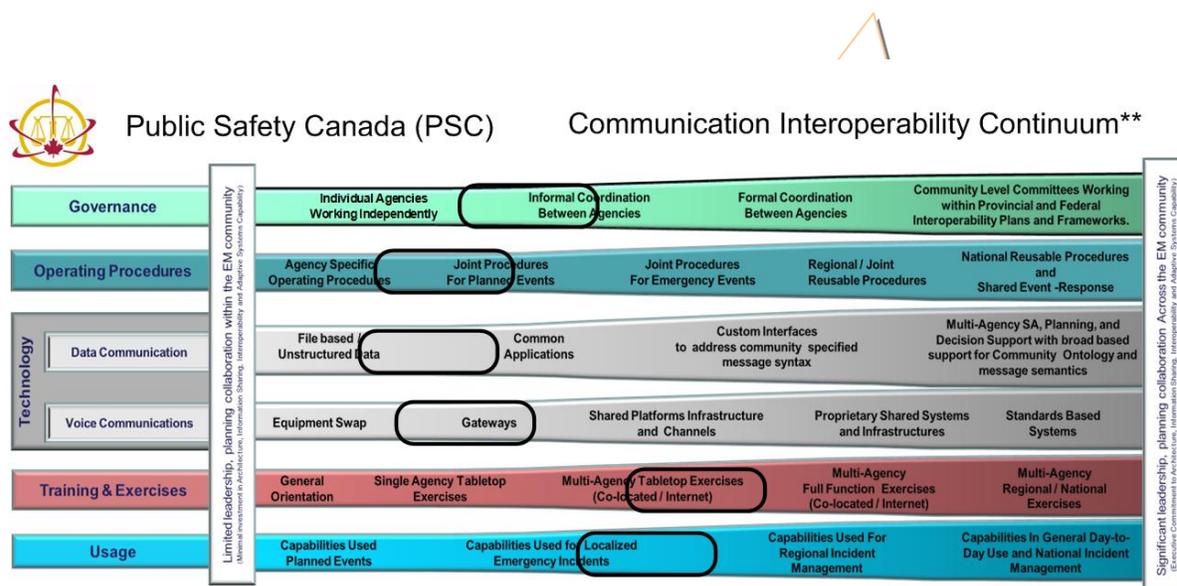


Figure 2-6 - EMSI Communication Interoperability Continuum

2.6 Architecture Framework

From the onset of the EMSIF effort, it was clear the cornerstone of the framework would be the processes and artefacts that are collated as part of the knowledge base that:

- Describe what interoperability meant to each of the communities of interest and practice comprising the EM and PS communities.
- Describe the current state of capability (ability for community members to interoperate).
- Describe a target (or vision) state for interoperability for the community (ies).
- Identify the inter-agency gaps between the current and target states.
- Develop a science and technology road map that addresses the identified gaps.
- Mitigates RISK.

Architecture was identified a cornerstone for these objectives: as it provides a conceptual blueprint that defines the structure and operation of an architectural element (e.g., organization, capability, system or service). It also documents how architectural elements can most effectively achieve its current and future business (/operational) objectives.

An architecture framework is a detailed set of practices, methods and tools for developing architecture artefacts (models, views and view points). The EMSIF focuses on blending of three international efforts in the area architecture:

Element	Role / Description
<p>The Open Group Architecture Framework</p>	<p>TOGAF provides a detailed approach to the design, planning, implementation, and governance of an enterprise, system and application architectures. These are modeled at four levels of abstraction or domains: Business, system, Data, and Technology. This set of foundation architectures is provided to enable the architecture team to envision the current and future state of the architecture.</p> <p>TOGAF defines a set of processes (tools) that can be used for developing a broad range of architectures. Like other AFs, TOGAF:</p> <ul style="list-style-type: none"> • Describes a methods for defining information systems and services in terms of a reusable set of building blocks • Illustrates how the building blocks fit together • Captures and maintains a common vocabulary • Captures and maintains a list of recommended standards • Captures and maintains a list of compliant products that can be used to implement the building blocks
<p>Department of Defence Architecture Framework (DODAF)</p>	<p>DoDAF defines a set of products (views and viewpoints) that provide mechanisms for visualizing, understanding, and assimilating the broad scope and complexities of an enterprise, system or service architecture description through graphic, tabular, or textual means.</p> <p>DoDAF extends the reach of TOGAF by formalizing the specifications for products of artifacts resulting from architecture activities. DoDAF also extends the foundation of the Public Safety Architecture Framework (PSAF) described on the Department of Homeland Security (DHS) SAFECOM. DHS is currently investigating the use of the DODAF 2.0 Specification.</p> <p>DODAF 2.0 defines specification for the following architecture viewpoint:</p> <ul style="list-style-type: none"> • The All Viewpoint describes the overarching aspects of architecture context that relate to all viewpoints. • The Capability Viewpoint articulates the capability

requirements, the delivery timing, and the deployed capability.

- The **Data and Information Viewpoint** articulates the data relationships and alignment structures in the architecture content for the capability and operational requirements, system engineering processes, and systems and services.
- The **Operational Viewpoint** includes the operational scenarios, activities, and requirements that support capabilities.
- The **Project Viewpoint** describes the relationships between operational and capability requirements and the various projects being implemented. The Project Viewpoint also details dependencies among capability and operational requirements, system engineering processes, systems design, and services design within the Defense Acquisition System process.
- The **Services Viewpoint** is the design for solutions articulating the Performers, Activities, Services, and their Exchanges, providing for or supporting operational and capability functions.
- The **Standards Viewpoint** articulates the applicable operational, business, technical, and industry policies, standards, guidance, constraints, and forecasts that apply to capability and operational requirements, system engineering processes, and systems and services.
- The **Systems Viewpoint**, for Legacy support, is the design for solutions articulating the systems, their composition, interconnectivity, and context providing for or supporting operational and capability functions.

DODAF provides a richer set of viewpoints than those supported by PSAF.

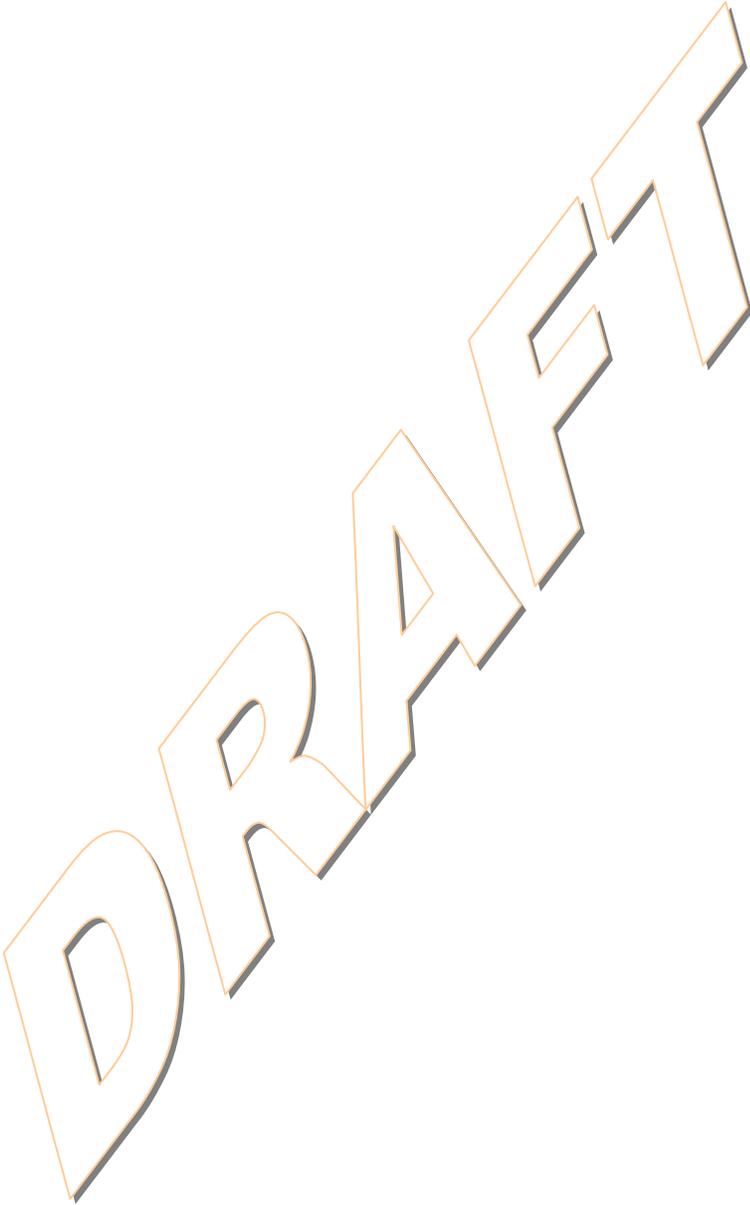
Unified Profile for DODAF and MODAF

UPDM is an international initiative to standardize how UML and UML dialects (e.g., SysML, SOAML, BPMN) can be used to represent the architectural views defined for both the US Department of Defense Architecture Framework (DoDAF) and the UK's Ministry of Defence Architecture Framework (MODAF). The standardization is expected to result in significant improvements in the consistency, quality, and tool interoperability of enterprise architectures that comply with these frameworks.

UPDM will be extending Architecture coverage to the NATO AF (NAF).

In addition to improvements in architecture product consistency and quality, the adoption of the standards assures that there will be multiple commercial off the shelf tools supporting the core elements of EMSIF architecture requirements.

Figure 2-6 illustrate an alignment between TOGAF, DoDAF and UPDM.





Public Safety Canada (PSC)

EMSI Framework Application of Architecture

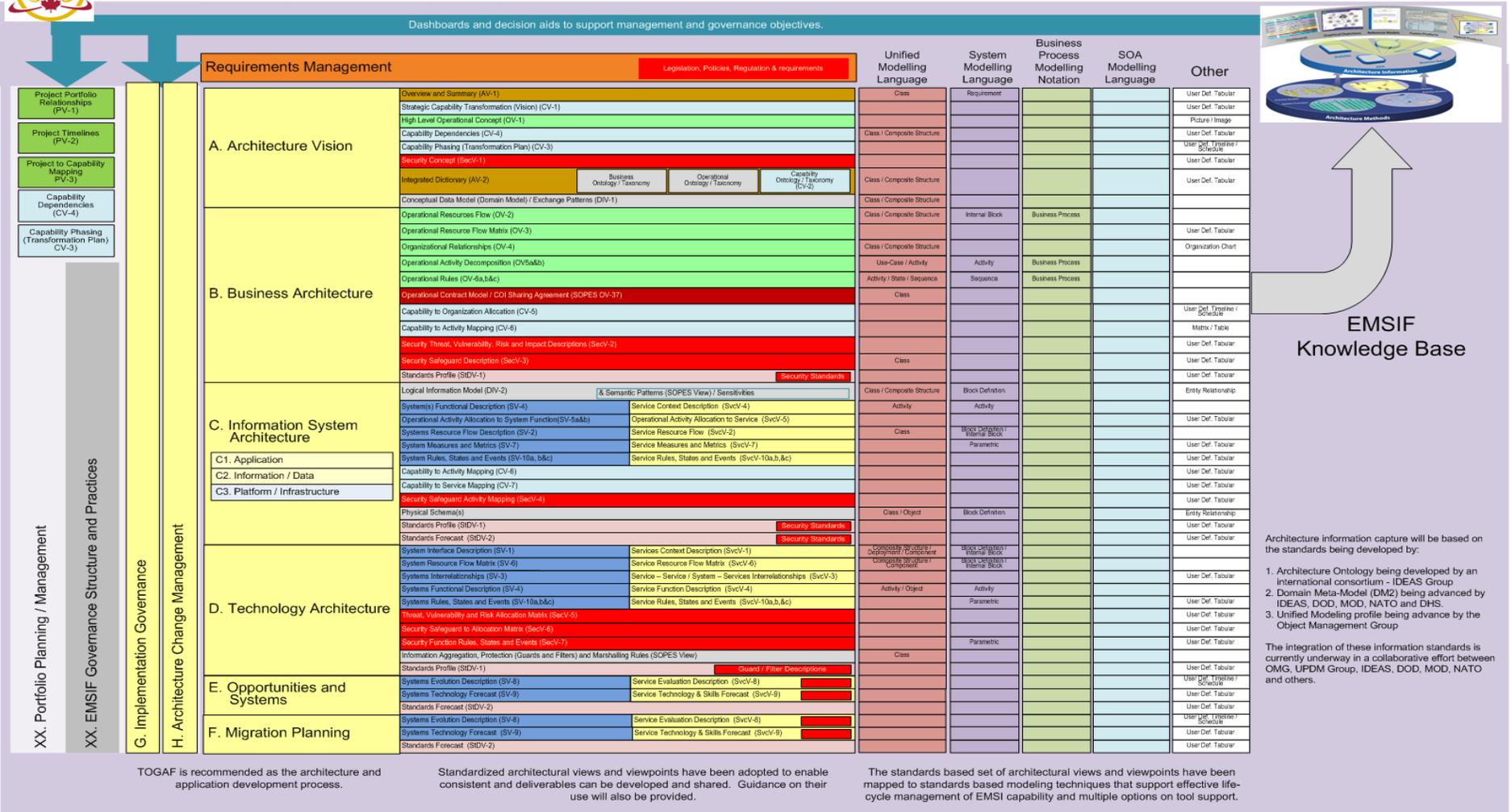


Figure 2-7 - Architecture Frameworks

3 Implementation support

The development, acquisition and integration of capability, systems and services will be performed by the individual community agencies and supporting Science and Technology agencies like the Centre for Security Sciences (CSS) out of Defence Research and Development Canada (DRDC). The decision to use and the responsibility for aligning EM Systems to the EMSIF is that of the participating agencies. The EMSIF working group will develop policy, standards and best practices that will guide and support an agency’s decision to align their processes and systems with the capabilities of the wider emergency management and public security community.

Where needed, Public Safety Canada will support the development (acquisition) and integrations of backbone infrastructure and core services that further facilitate alignment. This section outlines the areas where PSC will actively support the deployment of common or shared capability.

3.1 Working Groups

The EMSIF defines one working group (EMSIF WG), which will be supported by community staffed working parties. The WG will be responsible to reviewing and recommending shared architecture components, standards, specifications and technologies

3.1.1 WG Activities

3.1.2 Working Parties (WP)

3.1.2.1 Communications and Networks (WP)

TBD – SAFECOM Approach - Get information on current Canadian efforts from Scott Milton.

3.1.2.2 Middleware WP

3.1.2.3 Information Services WP

3.1.2.4 Domain Model WP

A domain model is a conceptual description of concepts and the vocabulary use in a specific or set of overlapping domains (A sphere of activity, concern, or function). The model identifies the relationships among major entities within the domain, and identifies their applied methods and attributes. The model provides a structural view of the domain that can be complemented by other dynamic views (e.g., Use Cases).

An important benefit of a domain model is that it describes and constrains the system of the discussion. It is used to verify and validate the understanding of the problem domain among

stakeholders. It is especially helpful as a communication tool; focusing business and technical teams on the key concepts of a development. E.g.: The definition of the functions (methods / processes), objects, information, requirements, relationships and variations in a particular domain. The domain model results of analysis activities, which provides a representation of the requirements of the domain. The domain model identifies and describes the structure of data, flow of information, functions, constraints and controls within the domain of interest.

The following are information domains that do not have formal specifications within the EM and PS communities. The lack of clarity adds complexity and risk to supporting activities.

- Architecture Domain
- Situational Awareness (Common Operational picture) comprises several overlapping domain which need to be integrated:
 - Common Alerting
 - Communications
 - Resource Planning and Tracking
 - Materiel and Supply
 - Geospatial
 - Planning and tasking
 - Critical Information Protection
 - Cyber Security (/SA)
- Decisions Support
- Collaborative Planning

Development of a shared understanding, amongst stakeholders, will be critical scoping and eventually validating and verifying capability.

The Domain Model WP will develop and execute a plan to develop and document a shared community understanding of the domains that comprise emergency management and public security.

3.1.3 **Semantic Specification WP**

NIEM

CAP

EDXL

3.1.4 *Shared Applications WP*

TO BE COMPLETED

3.2 *EMSI Metadata Standards*

The EMSIF will specify metadata standards for architecture, information sharing and storage. The Metadata WG in consultation with federal, provincial and municipal agencies defines the structure and rules governing metadata for the EMSI domain. The standardization of metadata is essential if systems and data are to be interoperable, and if EM managers and responders are to be able to find, use and share information and IM/IT services.

The EMSI standards will be based on ISO/IEC-19502 (Meta Object Facility (MOF)) and ISO 15836 (Dublin Core) but has additional elements and refinements to meet the specialist needs of the EM sector. It will be developed further as needs arise and encoding schemes become available. It can be found at **(ADD WEB SITE)**.

The Metadata standards will be developed further and maintained according to the following principles.

- They will be based on open architecture and standards and application or project-based.
- There will be tools to aid those with widely varying experience of preparing resource descriptions.
- Core elements of the standards will remain stable. Changes to the core elements will require considerable effort, time and resources to implement across the EM environment
- Additional element refinements can be added where it can be shown that these are essential or do not affect the core elements and capabilities provided by the standard. A balance will need to be struck between the need for extensibility and the need for stability.
- They will be inclusive, taking into account the many existing metadata schemes, with the aim of minimising the need to rework existing products.
- They will meet the information retrieval, aggregation, protection and exchange needs of EM community.

3.3 *EMSIF Development Timeframe*

TO BE COMPLETED – should look to a 5 year window for core capability

4 Roles and Responsibilities

The roles and responsibilities of central government and other public sector and industry organisations are outlined below. Whilst this is not meant to be exhaustive, it does indicate the main functions.

4.1 *PS Interoperability Directorate*

The Public Safety Canada Interoperability Directorate is the lead agency for the definition and implementation of this framework. In collaboration with other departments, local authorities and other EM, public Safety and First Responder communities, the interoperability Directorate will:

- Lead the development and maintenance of the EMSIF and provide the management infrastructure to support the processes.
- Act as the focal point for co-ordinating interoperability efforts throughout community and ensure rapid response to community proposals and priorities
- Coordinate effort with Treasury Board and Legislators
- Coordinate policy development efforts
- Coordinate effort with other governments and international bodies
- Coordinate the development and maintenance of EMSIF Support Environment:
- Manage the EMSIF website and support infrastructure
- Co-Chair EMSI Working Groups (Section 5.5)
- Manage interaction with similar initiatives and specifications bodies elsewhere across the world, including NEIM, OMG, W3C, OASIS and others.

4.2 *DRDC CSS*

TO BE COMPLETED

4.3 *Public sector organisations*

The full participation of GC PS agencies, devolved administrations and local authorities is essential to successfully deliver interoperability across the EM, CM and MEM agencies. Although central coordination will be provided where required, much of the direct action and development will take place in individual public sector agencies that will need to:

- Contribute to the continuous development and improvement of this framework
- Ensure that EMSIF alignment is a central part of their IM/IT strategies
- Produce a ‘roadmap’ for implementing their organisation’s alignment with EMSIF
- Identify which of their capabilities and services can be useful more broadly in the community
- Ensure they develop the skills needed to develop interoperable capabilities and services

- Establish a point of contact who can assess the impact change requests and can respond within the stated time period
- Budget for and supply resources to support the development and delivery of EMSI
- Take the opportunity to rationalise processes (as a result of increased interoperability) to improve the quality of services and reduce the cost of provision.

4.4 **Senior IM/IT Committees**

This section will describe the GC will outline the committees and the role of these committees in the delivery and governance of EMSI.

TO BE COMPLETED

4.5 **Working Groups** (Terms of Reference for Each WG need to be developed)

4.5.1 **EMSIF Working Group**

The EMSIF Management Group, comprising community stakeholders, is responsible for all aspects of the EMSIF. It is the management group that prioritises EMSIF activities, establishes priorities and approves the inclusion policies, specifications into the framework.

Membership of the group is open to all EM community agencies. Additionally, industry members may participate in the group on a permanent or call-off basis.

The EMSI WG will be co- chaired by Public Safety Canada and **TBD**.

Terms of reference for the group can be found at (**web-site URL**).

4.5.1.1 **Architecture Working Party (AWP)**

The Architecture Working Party is responsible for compiling and maintaining the overall EMSI Architecture as specified by the community. This WP will also establish a tools and information environment through which participating community members can contribute architectural concepts and designs. These contributions will be integrated into a set of architectural views that accurately describe operational and system alignment to a government(s) of Canada EMS.

Membership of the party is open to all EM community agencies. Additionally, industry members may participate in the party on a permanent or call-off basis.

The EMSI WP will be co- chaired by Public Safety Canada and **TBD**.

Terms of reference for the party can be found at (**web-site URL**).

4.5.2 **XML Schema Working Party (XSWP)**

The XML WP will develop the specifications for and co-ordinate the production of, the shared community XML schemas. The WP, which reports to the EMSI Management Party, draws together

representatives from across the EM Community to develop and endorse schemas for the EMSIF. Schemas produced and endorsed by this working party pass through the EMSIF approval process and are published on the EMSI Website.

Membership of the party is open to all EM community agencies. Additionally, industry members may participate in the party on a permanent or call-off basis.

The EMSI WP will be co- chaired by Public Safety Canada and **TBD**.

Terms of reference for the party can be found at **(web-site URL)**.

4.5.3 **Information and Metadata Management Working Party (IMMWP)**

The Information and Metadata Working Party, which reports to the System Architecture WP, provides advice and comments on all metadata aspects of the EMSIF, and develops and maintains the EMMS and ADMM. The IMMWP will be responsible for.

- > Governance Domain Model
- > PSBP Domain Model
- > Enterprise Architecture Domain Model
- > System Architecture Domain Model
- > Technology Architecture Domain Model
- > Information/Information-Sharing Architecture Domain Model
- > Security/Information-Protection Architecture Domain Model
- > Application Domain Model

Membership of the party is open to all EM community agencies. Additionally, industry members may participate in the party on a permanent or call-off basis.

The EMSI WP will be co- chaired by Public Safety Canada and **TBD**.

Terms of reference for the party can be found at **(web-site URL)**.

4.5.4 **Testing and Demonstration Working Party (TDWP)**

The Testing and Demonstration WP, which reports to the System Architecture WP, will develop a test, demonstration and training program for agencies participating in the GC EMSI effort. TDWP will be responsible for developing the test plans, scenarios, cases, data, metric, ... for the test and demonstration program for EMSI. The TDWP will also plan and coordinate the development of a demonstration facility, web –based testing capability and test reference systems.

Membership of the party is open to all EM community agencies. Additionally, industry members may participate in the party on a permanent or call-off basis.

The EMSI WP will be co- chaired by Public Safety Canada and **TBD**.

Terms of reference for the party can be found at **(web-site URL)**.

4.5.5 Other working parties

Specific working parties are set up for particular projects. Details of any parties and their terms of reference are available on EMSI Web Site.

The EMSI WP will be co- chaired by Public Safety Canada and **TBD**.
Terms of reference for the party can be found at **(web-site URL)**.

DRAFT

5 Change management

The EMSIF architecture, standards and specifications will inevitably change over time and will have the capability to change quickly when required. The change management process must ensure that the EMSIF remains up to date and is aligned to the requirements of stakeholders and to the potential of new technology and market developments. The following paragraphs describe an inclusive Internet-based consultation process that will encourage participation and innovation. They also describe how changes to resources specifications will be managed.

5.1 Change Cycle

The EMSIF is seeking to introduce a change management cycle of 4-5 years; where major integrations in concepts and technologies can be explored, architectures and designs generated and implementations developed and tested. This timescale aligns well with the timeframes of standards development and other interoperability initiatives. Although technologies advance more rapidly, organizations of any size cannot. Planning, resourcing and development cycles of government will be taxed to evolve in this proposed rate of change.

The cycle illustrated in Figure 6.1 is based on a four year cycle making accommodations for the development of a new or enhanced open standard to support the next cycle of capability deployment.

ADD DIAGRAM

Figure 6.1 – EMSIF Change Cycle

A more detailed description of EMSIF Change Management strategy can be found in the EMSIF Transition Plan and EMSIF Change Management Plan.

Minor or none intrusive could be added to the EMSIF and EMSI Architecture during the 4 year cycle based on approvals from the EMSI Management Group. These changes or additions cannot effect Service level agreements, function or performance of the established capability for the major cycle.

5.2 Management of Change

The Emergency Management community is continually forced to address change in its operating environment and the expectations of Canadians. Risk, threats and available capability are in a continual state of change and the EM community needs a systematic approach of addressing this change within its capability envelop. All changes, whether major or minor, will be approved by the EMSI Management Group.

5.3 Compatibility with Legacy

The EMSIF expects to maintain a three (3) cycle backwards compatibility for core capability in all architecture, design and technology innovations. This compatibility constraint will enable an evolutionary roll-out of capability across the community within a reasonable cost, schedule, performance envelop.

5.4 Open Standards and Architecture

The change cycle for the EMSIF is consistent with the development cycles for

5.5 Agency Specific and Peer-to-Peer Adaptations

The EMSIF provides a set of guidelines which allow for the extension for domain specific capability to support specific community needs.

5.6 XML Message Schemas

XML schemas will be treated as special cases. XML schemas will need to undergo a test programme before being used in an electronic service. Changes to XML schemas will also have to be carefully assessed, as potentially they can have a high impact. Such changes are particularly difficult to manage in large organisations. In some organisations it is estimated that a year is needed to implement a change to a core schema. As a consequence, changes to agreed XML schemas need to be managed carefully, with proper processes in place to ensure that all involved parties to the change are properly consulted and agree to the change. A formal change control procedure will

reduce the impact of change on an existing service.

Also, given that the XML schemas carry data that forms part of an organisation’s business information exchange processes, there is the potential for mutual dependency between the business processes of a number of organisations encapsulated in the agreed XML schemas.

XML schemas also have interdependency with the GDSC, and so changes to both should be carefully co-ordinated.

5.7 **EMS resource owner**

Every EMSIF identified resource must have a designated owner (a role or organisation, not a named person). The ownership of the changes should be vested in the organisation(s) that own(s) the. However, the change may not affect just the owning organisation(s), so it is essential that ‘user’ or peer level organisations have the opportunity to contribute to the change process in a structured and formal way.

5.8 **Consultation and innovation**

The overall strategy for transforming EMSI identifies three basic forms of dialogue: public sector to public sector; public sector to industry; and public sector to the citizen. If interoperability specifications are to fully support the strategy, then they must be open to the widest form of consultation that involves all these players. The EMSIF consultation process will target organisations that are known to be interested in the specific specifications, having been identified as participants in the service or users of existing specifications, but will be open to all. Unsolicited comments and suggestions will be encouraged over the website.

Request for Comments

All draft policies, specifications and XML schemas will be posted on the EMSI Web Site with a Request for Comments (RFC) on the proposed draft or change. Registered stakeholders, and members of the appropriate WG will be notified by email of the RFC, but the EMSI website offers an invitation to anyone to comment on the draft document. All comments received will be acknowledged and the outcome of the RFC will be published on the site. The consultation process does not preclude unsolicited comments on currently agreed policies and decisions, which are also encouraged.

Request for Proposals

Whereas the RFC process asks for comments on proposed solutions, the government also requests innovative solutions to problems where the solutions are not clear. In this case, a Request for Proposals (RFP) will be posted on the EMSIF website, a, outlining the requirement. These RFPs will also be published on the DRDC CSS and MERX web sites. The aim is to attract innovation and the

most cost-effective solution to the problem, using the worldwide industry and the population base. If a particular proposal is taken forward, this will be published on the site.

DRAFT

6 Aligning to EMSIF

The EMSIF requires alignment by EM, CM and MEM communities to be truly effective. The EMSIF provides general guidance on what alignment means and how it will be evaluated. It is intended to inform all those involved in the development and provision of EMS capability of their requirements are to make you of the EMSIF and its core components. Throughout this section, use of the term ‘system’ is taken to include its interfaces, which are the prime focus of EMSIF policies, standards and specifications.

6.1 *What does Alignment Mean?*

At the highest level, alignment means:

- Providing a browser interface or Program interface to access the core elements of the EMSIF.
- Providing system interfaces that produce and process XML documents that conform to the adopted XML Schemas.
- Preserve the semantics (meaning) of exchanged XML documents and other EM information.
- Using Architecture to specify and design EMS capability.
- Using metadata for content management and protection.
- Publishing architecture models for the community in accordance with the EMSIF architecture framework.

6.2 *Alignment Timetable*

In practice, it is expected that organisations will not be able to participate effectively and at minimum cost in future data interchange processes unless they align with the EMSIF policies and specifications. The Alignment rules and timetable are:

- TBD

6.3 *Stakeholders*

The stakeholders who need to know and understand what aligning to the EMSIF means.

Stakeholders include:

Business Analysts and Strategists

Ensure that their EM, CM and MEM strategies align to EMSI mandates. They should be aware alignment with

EMSIF is a desired capability for all members of the EM community and the alignment will be validated and verified.

Business owners/ project managers/sponsors	Responsible for ensuring that the relevant EMSIF policies and specifications are applied.
Project Governance and approval bodies	Responsible for ensuring that their approvals process includes a sign-off for EMSIF alignment.
Procurement Officers	Responsible for ensuring that EMSIF Alignment is incorporated in into EMS procurement procedures and contracts.
Suppliers, Vendors and Consultants	Required to supply products and services aligning to EMSIF policies and specifications.
Project and departmental auditors, Auditor General’s Office, and Parliamentary Committees	Need to ensure that audits and reviews include a check for EM environment alignment to EMSIF.

6.4 ***Alignment responsibilities***

The ultimate responsibility for alignment with the EMSIF rests with a system’s owner or sponsor. Alignment is by self-regulation using normal departmental validation and verification arrangements throughout the system development lifecycle. PSC will provide network testing and test reference systems to support community member with this activity.

It will be for EM organisations to consider how their operational capability can be enhanced by taking advantage of the opportunities provided by increased interoperability.

6.5 ***Aligning to new versions of the EMSI Framework***

The EMSI Framework is relatively new and will evolve for some considerable time as new policies and specifications are adopted and new areas of interoperability addressed. This will make it difficult, if not impossible, for communities of interest, agencies and systems fully align to evolving framework. The EMSIF interoperability working group will provide migration strategies for agencies to evolve to expanding capabilities.

The EMSIF is formally updated, as part of that formal update cycle. The EM community will be consulted, through the Interoperability Working Group and the public consultation processes, on

the changes to be made during each cycle. The governance structures will be used to introduce new policies and specifications following these full consultations with the community and other stakeholders. This will seek to minimise the burden of change on EM partners while maintaining the principle of effective and open interoperability.

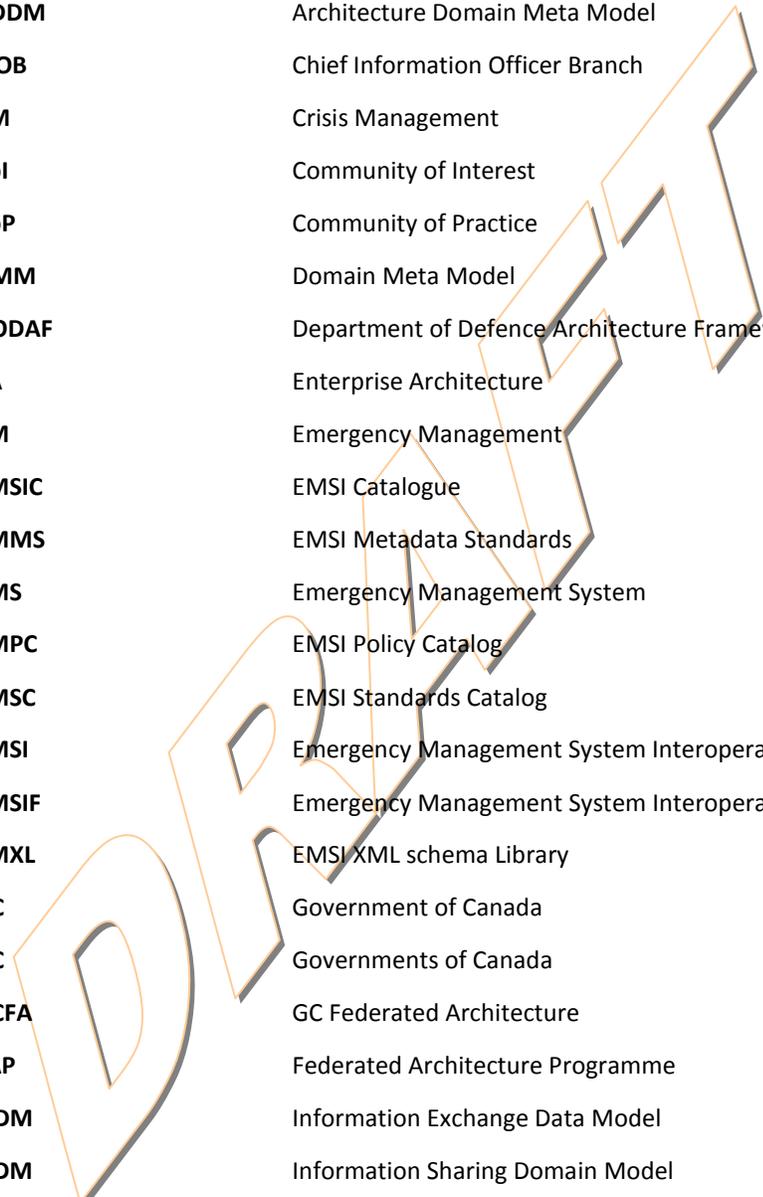
6.6 **Additional guidance**

An EMSI Advisory Service is provided by Public Safety Canada Interoperability Directorate and Centre for Security Sciences EMSI. The service provides a structured, web-based commentary about the EMSIF and the five-year vision. Full details of the service are available at the EMSIF Web-site (**web-site URL**).

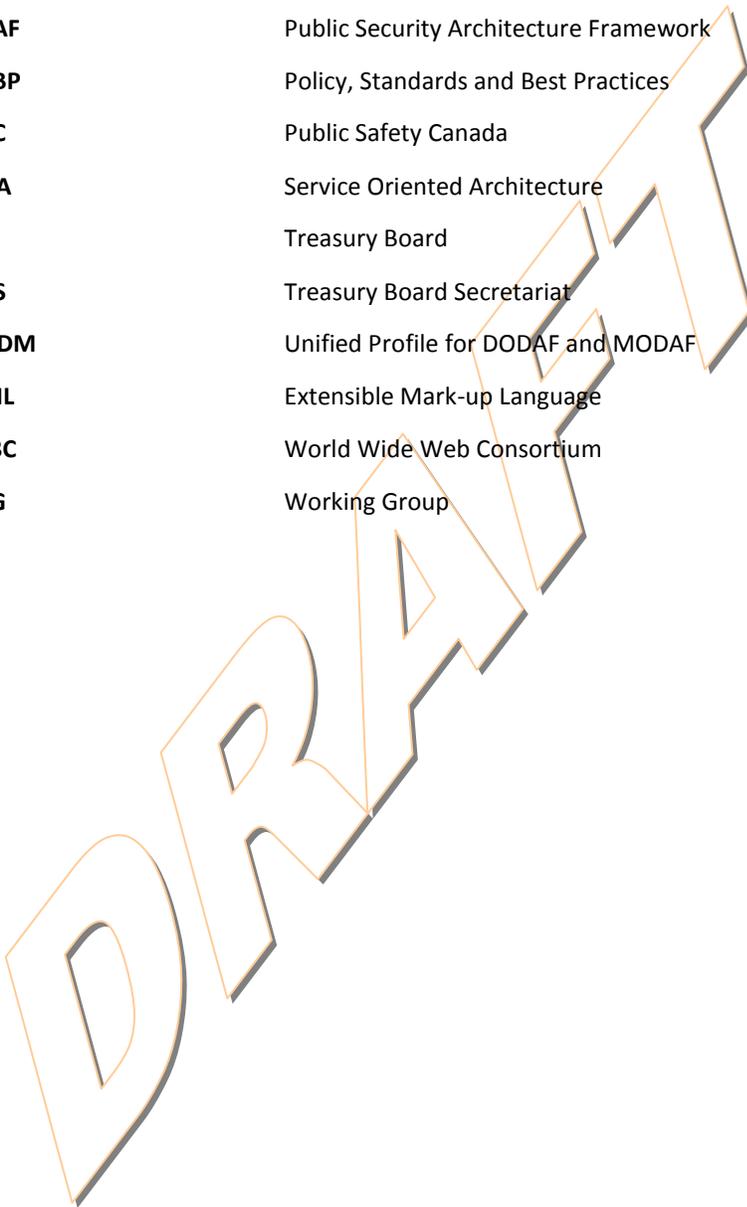
While the above service provides general guidance on the EMSIF policy architecture and standards, much of the guidance will be provided on a case-by-case basis, and detailed needs of specific agency or community of interest. . Additional guidance, FAQs and architectural components will be made available in the form of best practice, Case Studies and FAQs on the (**web-site URL**).

DRAFT

7 Glossary



ADDM	Architecture Domain Meta Model
CIOB	Chief Information Officer Branch
CM	Crisis Management
CoI	Community of Interest
CoP	Community of Practice
DMM	Domain Meta Model
DODAF	Department of Defence Architecture Framework
EA	Enterprise Architecture
EM	Emergency Management
EMSIC	EMSI Catalogue
EMMS	EMSI Metadata Standards
EMS	Emergency Management System
EMPC	EMSI Policy Catalog
EMSC	EMSI Standards Catalog
EMSI	Emergency Management System Interoperability
EMSIF	Emergency Management System Interoperability Framework
EMXL	EMSI XML schema Library
GC	Government of Canada
GC	Governments of Canada
GCFA	GC Federated Architecture
FAP	Federated Architecture Programme
IEDM	Information Exchange Data Model
ISDM	Information Sharing Domain Model
MEM	Major Event Management
MODAF	Ministry of Defence Architecture Framework
MOF	Meta Object Facility
NIEM	Nations Information Exchange Model
OASIS	Organization for the Advancement of Structured Information Standards



OGC	Open Geospatial Consortium
OMG	Object Management Group
PAS	Publicly Accepted Specifications
PSAF	Public Security Architecture Framework
PSBP	Policy, Standards and Best Practices
PSC	Public Safety Canada
SOA	Service Oriented Architecture
TB	Treasury Board
TBS	Treasury Board Secretariat
UPDM	Unified Profile for DODAF and MODAF
XML	Extensible Mark-up Language
W3C	World Wide Web Consortium
WG	Working Group

8 Attachment 2: Definitions



Levels of Interoperability

Communications and Network Interoperability

The lowest level of an interoperability reference model can be defined by ability of heterogeneous systems to interconnect. Communications networks, including their physical carrier (e.g., radio, Ethernet, WIFI and fiber optics) are a prerequisite to any form of higher interoperability. PSC is investigating the SAFECOM⁸ program as a template for addressing EMCI communication and network interoperability.

One can collapse the bottom five layers (Physical, Data Link, Network, Transport and Session) from the ISO Reference Model into this layer of the Interoperability Reference Model.

Service Interoperability

The Service Layer addresses the services that link information systems and applications to the Communication and network infrastructure (above). The EMSI is seeking a uniform set of services that provide a common form, fit, function interface between the IS or applications and the underlying infrastructure. This common interface will allow for timely adaptation of changes in environment and/or operational requirements.

This layer encompasses things as Middleware, Service Busses and WEB services.

Data Interoperability

Data element interoperability is the first level of interoperability beyond voice, fax and unstructured email based capability which is prevalent in the current environment. The data layer represents a set of common definitions for the data exchanged between systems, including: vocabularies, taxonomies, tags and label, meta-data, and entity relationships. On its own, the data layer does not provide commonality in understanding or actions between the communicating parties. It is however a necessary foundation for the following layer in the reference model.

The Data Layer relies on the application of sound data and metadata management practices.

Shared processes

The Shared Processes Layer (or Shared Services Layer) integrates software engineering best practices that seek to promote shared development and reuse of software code. As it matures it provides mobile code bases and

⁸ Additional Information on SAFECOM can be found at <http://www.safecomprogram.gov/SAFECOM/>

portable software services. Most recently, these practices have been incorporated into the Service Oriented Architecture (SOA) and WEB Service Models and in the underpinnings of the Open-Source community.

**Procedural
Interoperability**

The Procedural Layer (or Operating Procedures Layer) aligns systems engineering and human factors within the Reference Model. This is the domain long inhabited by Standard Operating Procedures (SOPs). This layer defined the processes and use-cases upon which information requirements between agencies can be defined and EM services can be specified and automated.

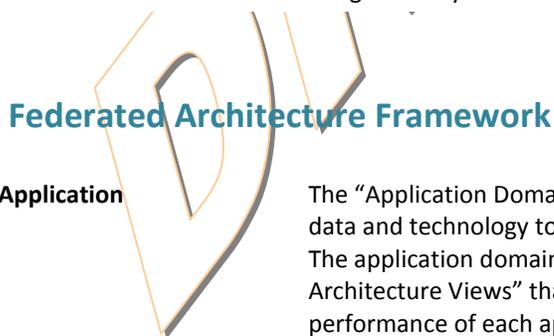
**Cognitive
interoperability**

The Cognitive layer (focus of this document) addresses the specification of information (Data in Context) elements and the business rules related to the capture, storage, integration, processing, protection and sharing of information within the community. It is this layer that seeks to describe the EM information rules and services that provide shared situation awareness, collaborative planning and decisions support for an environment. Information systems are interoperable at this layer if decision makers in two different systems are seeing coherent pictures of the information presented.

**Doctrinal
interoperability**

The Doctrinal layer addresses the Human, social and other factors that lead to coherency and uniformity of action within the community. Different decision makers, when presented with the same information will be making similar decisions. The usual doctrinal tensions of uniformity versus creativity are still present and certainly not resolved by this model. The Model only serves to illustrate the level of abstraction where such discussion belongs.

Doctrinal thinkers will tend to divide this layer into tactical, operational and strategic sub-layers.



Application

The “Application Domain” combines business processes with data and technology to perform a business function or service. The application domain is documented as part of “Application Architecture Views” that describes the function and performance of each application and how it integrates into the shared or common Infrastructure of the Federated Architecture. The Application Architecture specifies how applications comprising an agency’s or community of Interest’s align to deliver IM services.

**Information
Management**

The “Information Management” encompassed the policies, procedures, systems, services and infrastructure enabling the capture, storage, protection, processing, maintenance and

dissemination of information. It also includes the services and technologies needed to maintain the quality and integrity of information holdings over their life cycle. The Information Management Architecture provides standards for defining/designing information content, and, if appropriate, business objects.

**Network and
Communications**

The “Network Domain” is describes as a Network Architecture that defines the technologies and standards comprising the physical connectivity in the IM/IT infrastructure. These views of architecture describe the logical elements (structure, topology, bandwidth and management), physical hardware components (wiring, LANs, hubs, routers, switches), remote access technologies (dial-up, Virtual Private Networks), perimeter security (firewalls, proxy servers) and network protocols.

The EMSI Framework adds a “Communication Domain” to the architecture to address the specific characteristics of networks comprising Radio, WIFI and Satellite links; prevalent in Emergency and Crisis Operations

Platform

The Platform Domain describes the technical components of computer platforms including the hardware, operating systems and interfaces. A “Platform Architecture” describes technical computing components of an IM/IT infrastructure, such as: client and server hardware platforms, the operating systems (including separation kernels) used on these platforms, and interfaces that they support.

Presentation

This domain includes all technologies that facilitate access to the IM/IT infrastructure at the "front end." The Presentation Architecture defines the components and standards that enable the interface between one or more applications and the human user. This architecture is primarily concerned with the human-computer interface provided through an application or system, such as PDF, XSL and voice recognition.

Security

The “Security domain” describes security components for and IM/IT environment, as required to support operations with partners, citizens and businesses having varying trust relationships. The Security Architecture Views describe the information protection and IT security policies, strategies and solutions designed to protect the confidentiality, integrity and availability of IM/IT assets, and enable secure electronic service delivery. The EMSI identifies two distinct areas of security:

- Platform and Network Security; and
- Information Protection.

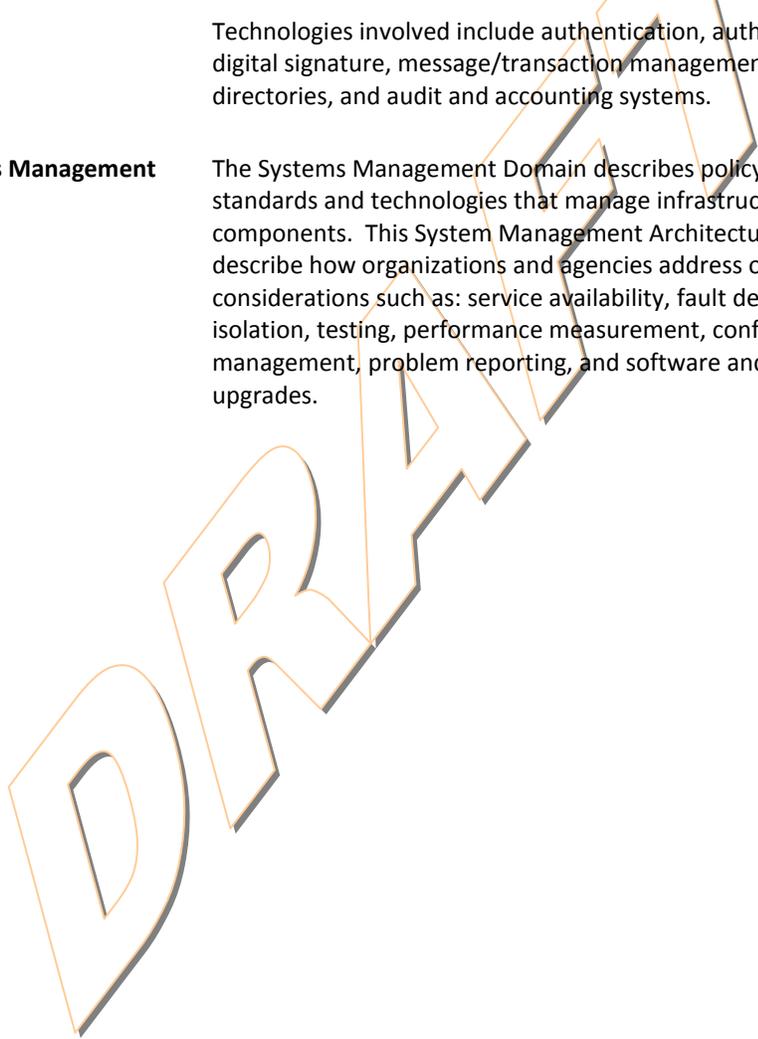
Services

The Services Domain includes the technologies that link front-end applications (i.e. what users see and use) with back-end/legacy systems (i.e. the government's internal management systems). This domain architecture defines the technologies, standards, and guidelines for seamless, platform-independent, inter-enterprise and intra-enterprise business communications and universal access to business information, with a special focus on supporting the electronic commerce and electronic service delivery objectives of Government On-Line.

Technologies involved include authentication, authorization, digital signature, message/transaction management tools, directories, and audit and accounting systems.

Systems Management

The Systems Management Domain describes policy, procedures, standards and technologies that manage infrastructure components. This System Management Architecture Views describe how organizations and agencies address operational considerations such as: service availability, fault detection and isolation, testing, performance measurement, configuration management, problem reporting, and software and hardware upgrades.



8.1.1.1 Network, Infrastructure and Communication Interoperability

Network Interoperability is the continuous ability to send and receive data between interconnected networks providing the level of quality expected by the end user without any negative impact to the sending and or receiving networks. Specifically: Network Interoperability is the functional inter working of a service across or between multi-vendor, multi-carrier inter-connections (i.e., node-to-node, or network-to-network) working under normal and stress conditions, and per the applicable standers, requirements, and specifications

Communication Interoperability relates to the compatibility of communication paths (frequencies, wave-forms, signaling), coverage or adequate signal strength, and; scalable capacity. More often this relates to the ability of two or more heterogeneous (multi-vendor) radios to exchange voice and data transmissions.

Both communication and network interoperability are required for any attempts of further interoperability Information Interoperability.

8.1.1.2 Information Interoperability

Information interoperability refers to the ability of organizations, systems, services to exchange quality information. as characterized by:

- **Accuracy:** semantics to accurately convey the perceived situation.
- **Relevance:** information tailored to specific requirements of the mission, role, task or situation at hand.
- **Timeliness:** information flow required to support key processes, including decision making.
- **Usability:** information presented in a common, easily understood format.
- **Completeness:** information that provides all necessary (or available) information needed to make decisions.
- **Brevity:** information tailored to the level-of-detail required to make decisions and reduces data overload.
- **Trustworthiness:** information quality and content can be trusted by stakeholders, decision makers and users.
- **Protected:** Information is protected from inadvertent or Malicious Release

8.1.1.3 Syntactic Interoperability

Syntactic interoperability is achieved when two or more systems are capable of communicating and exchanging data, they are exhibiting syntactic interoperability. Specified data formats, communication protocols and the like are fundamental. In general, XML or SQL standards provide

syntactic interoperability. Syntactical interoperability is required for any attempts of further interoperability.

8.1.1.4 Semantic Interoperability

Beyond the ability of two or more heterogeneous computer systems, applications and/or services to exchange information, semantic interoperability is the ability to automatically interpret meaningful and accurate information exchanged. To achieve semantic interoperability, both sides must defer to a common information exchange reference model and share business rules for the processing of the exchanged information. The content of the information exchange requests are unambiguously defined: what is sent is the same as what is understood.

Semantic interoperability is the target of the Public Safety community, as it is this form of interoperability that will enable the adaptive situational awareness, collaboration and decision support desired by legislators, stakeholders and decision makers.

8.1.1.5 Information Protection

Information protection related to an information management capability to process and share information based on its inherent sensitivity (e.g., classification, privacy, confidentiality). Current system focus on platform and network security, to the exclusion of the information sensitivity, is not well understood by the IM community.

As data is processed, integrated and exchanged by information systems, the aggregated often transition between sensitivity, if not security levels. Providing EMSI across multiple agencies with varying levels of trust (security regimes) and legislative mandates will require extensions to architecture, engineering and Information management practices and technologies. Areas to be addressed by the EMSIF include:

- Information protection policy (rules) specification;
- Information protection policy enforcement by applications, platforms and networks;
- Metadata (security) tag and label allocation and processing;
- Subscriber and community specific filters and guards which address security, privacy and confidentiality;
- Data Identification (Global Unique Identifiers); and
- Data Ownership.

EMSI requires the capability to selectively exchange semantically complete information, governed by its sensitivity and the subscriber to that information. EMSI also needs the ability to dynamically adjust information sharing based on the context of the emergency and the roles of the agencies in that emergency; designing for every eventuality (emergency situation) is neither practical nor reasonable. Dynamically adaptive systems must be the target, and Information and information protection is central to this as well as other defence in-depth approaches.

8.1.2 **Application Interoperability**

With respect to applications, the term interoperability is used to describe the capability of different software programs to exchange data via a common exchange format. The application must be designed to read and write common file formats, and use the same protocols. The lack of interoperability can be a consequence of a lack of attention to standardization during the design of a program. Indeed, interoperability is not taken for granted in the non-standards-based portion of the computing world.

Maintaining application interoperability has proven very difficult in highly dynamic environment such as Emergency and Crisis Management where detailed operational considerations cannot always be determined in advance. Extended development cycles for software exacerbate this challenge. Reliance on application (product) interoperability has proven too brittle and rigid to address dynamic real-world environments such as emergency of crisis management. Early successes typically do not scale to the complexity or variation in the scenarios, and applications relegated to the storeroom shelves with the community reverting back to informal lines of communication.

The shortfalls in application interoperability need to be address by a separation of operating logic (business rules) from the software and the ability for agencies to optimise information sharing and communications through changes in policy and properties without software change.

8.1.3 **Security Interoperability**

As organization seek greater levels of interoperability and information sharing, issues of security, privacy and trust are playing a more prominent role in discussions pertaining to interoperability. Elements of security and information protection are central to an effective interoperability strategy. Interoperability of security elements with increased the level of trust between agencies and stakeholders and promotes greater levels of interoperability.

8.1.4 **SOP Interoperability**

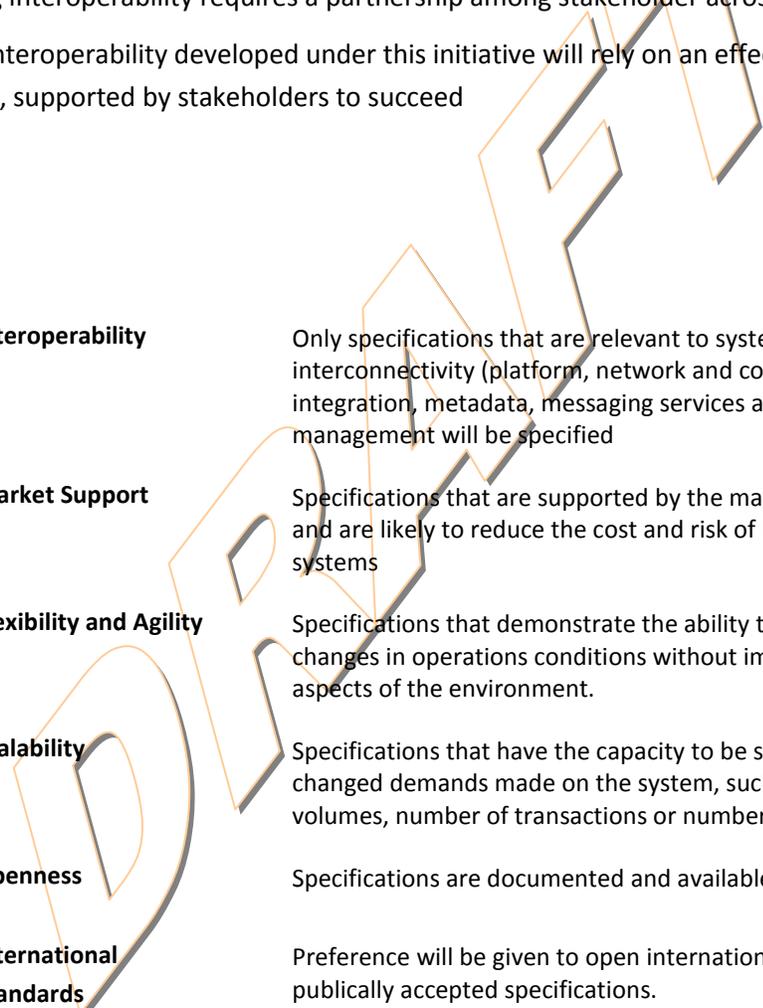
Standard operating procedures (SOPs) represent formal guidelines or instructions to decision makers. SOPs typically have both operational and technical components. Clear and effective SOPs are essential in the development and deployment of any interoperability environment for EMSI. The target is an environment where Policies and SOPs are translated into executable rules that are enforces by EM applications and infrastructure components.

Having stakeholder agreement o on policies and SOPs in areas of shared interest will facilitate the alignment of applications and information sharing agreements.

8.1.5 **Governance Interoperability**

Establishing a common governing structure for solving interoperability issues will improve the policies, processes, and procedures of any major project by enhancing communication, coordination, and cooperation; establishing guidelines and principles; and reducing any internal jurisdictional conflicts. Governance structures provide the framework in which federal, Provincial and municipal stakeholders can collaborate and make decisions that represent a common objective. It has become increasingly clear to the EM community that interoperability cannot be solved by any single entity; achieving interoperability requires a partnership among stakeholder across all levels of government.

System Interoperability developed under this initiative will rely on an effective governance structure, supported by stakeholders to succeed



Interoperability	Only specifications that are relevant to systems' interconnectivity (platform, network and communications), data integration, metadata, messaging services access and content management will be specified
Market Support	Specifications that are supported by the market and vendors, and are likely to reduce the cost and risk of EM information systems
Flexibility and Agility	Specifications that demonstrate the ability to adapt to rapid changes in operations conditions without impact to other aspects of the environment.
Scalability	Specifications that have the capacity to be scaled to satisfy changed demands made on the system, such as changes in data volumes, number of transactions or number of users
Openness	Specifications are documented and available to the public
International Standards	Preference will be given to open international standards and publicly accepted specifications.