INCIDENT MANAGEMENT INFORMATION SHARING

DHS S&T First Responders Group

Contents

Executive Summary

In many situations, federal, state, local, tribal and territorial government agencies; non-governmental organizations; and private sector partners in the incident management community do not have clear direction on the most optimal ways to discover or share mission-critical information and to objectively assess their capabilities. Although there are general guidance materials available, none provide details specific to an entity's maturity level as it relates to Incident Management Information Sharing (IMIS). The IMIS Capability Maturity Model (CMM) is being developed by the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) First Responders Group (FRG) in partnership with the DHS Office of Emergency Communication's SAFECOM program and local first responder communities.

An after action report (AAR) following the Central U.S. Earthquake Consortium Capstone-14 Exercise clearly identified the requirement for an IMIS CMM. The report stated that "a Capabilities Maturity Model would help agencies measure their maturity along a continuum and help to guide their path forward" and further said that a CMM "could result in significant opportunities to eliminate redundant data entry processes, reduce data entry errors and collect more detailed information." FRG leads the IMIS CMM effort to identify and understand gaps in information sharing. By leading this effort, FRG also aims to increase IMIS capabilities and prepare for future data-related initiatives.

The basis of the IMIS CMM are the core elements, derived from the five inter-dependent elements of the SAFECOM Interoperability Continuum[1] (Governance, Technology, Standard Operating Procedures, Training and Exercises, and Usage). Additional details are collected through the IMIS CMM attributes, specific to each of the core elements. These core elements and attributes are used extensively to measure the maturity of an organization's incident management and information sharing capabilities.

Overall, the development and deployment of the IMIS CMM will help entities measure their specific maturity related to IMIS. The assessment will provide opportunities for the entity to compare its current-state against proposed future-state objectives. The derived information can also serve a role in the identification of specific deficiencies and support requests for required funding.

[1] http://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2.pdf

PART I – THE CASE FOR THE INCIDENT MANAGEMENT INFORMATION SHARING CAPABILITY MATURITY MODEL

1.1 Capability Maturity Model Introduction

A Capability Maturity Model (CMM) is a framework that describes the key elements of an effective practice. It describes an evolutionary improvement path from an ad hoc, immature process to a mature and disciplined process. A CMM establishes a means for strategic measurement by which it is possible to judge, in a repeatable way, the maturity of an organization's processes, compare it to the state of the practice of the industry, and/or serve as the basis for an organization to plan improvements to its processes. Overall, a CMM is comprised of a collection of best practice-based characteristics that assist an organization in identifying competencies and support the improvement of its processes.

As explained in The Open Group for Architecture Frameworks (TOGAF) Architecture Maturity Models, in recent years the industry has witnessed significant growth in the area of maturity models. The multiplicity of models available has led to problems of its own, in terms of how to integrate all of the different models to produce a meaningful metric for overall process maturity.

In response to this requirement, the Software Engineering Institute (SEI) developed a framework called the Capability Maturity Model Integration (CMMI). According to the SEI, the use of the CMMI model improves on the best practices of previous models in many important ways. In particular, it enables organizations to:

- More explicitly link management and engineering activities to business objectives;
- Expand the scope and visibility of the product lifecycle and engineering activities to ensure that the product or service meets customer expectations;
- Incorporate lessons learned from other best practice areas (e.g., measurement, risk management and supplier management);
- Implement more robust high-maturity practices;
- Address additional organizational functions critical to its products and services; and
- Comply more fully with relevant International Organization for Standards.

1.2 Purpose of the Incident Management Information Sharing CMM

The Incident Management Information Sharing (IMIS) CMM will enable the maturation of incident management-related information sharing processes and capabilities. It is intended to improve and broaden the sharing of specific information that originates within episodes of incident response and support. In addition, it addresses IMIS abilities at all levels of government, as well as non-governmental organizations (NGOs) and private sector partners.

The IMIS CMM will enable the creation and progressive enhancement of an information sharing environment (ISE) that enables users to locate the people, services and data/information necessary to perform the job of emergency and incident management. A mature IMIS environment will define:

- What information is available;
- What services are available;
- What authorizations are required;

- The rules under which information is made discoverable and can be shared; and
- How to access to or deliver requested information on a sustainable basis.

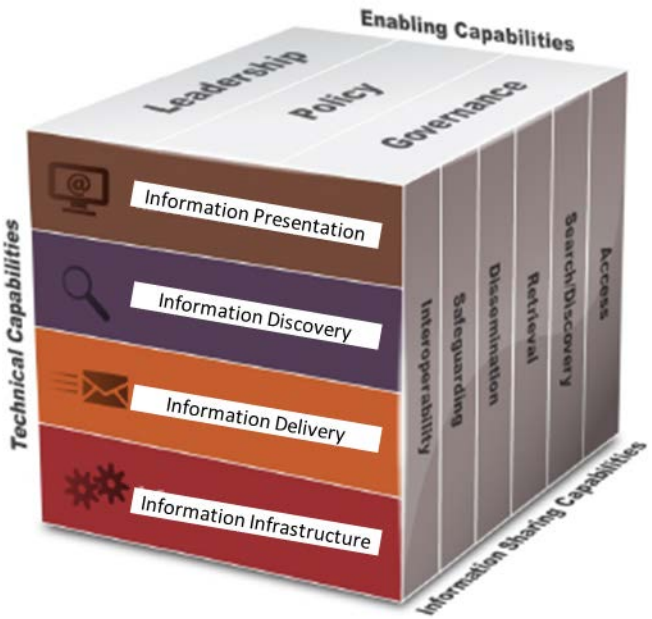
1.3 Intended Benefits and Uses of an IMIS CMM

1.3.1 Benefit of the IMIS CMM

The IMIS CMM will assist the mission of incident management to continue to improve technical, operational and strategic enhancements to the maturity level of processes within jurisdictions at all levels of government. A diagram of the various capabilities addressed across the IMIS CMM is depicted in Figure 1 below. Over time, the IMIS CMM is intended to:

- Lead to better informed first responders through improved interoperability and information agility;
- Provide a logical pathway to technical and functional advancements in IMIS;
- Assist organizations in creating a consistent, nation-wide IMIS governance approach while deriving value from their IMIS investments;
- Support resourcing requests and return on investment analysis; and
- Improve information security and integrity while increasing the technical abilities of incident response.

Figure 1: IMIS CMM Diagram



1.3.2 Uses of the IMIS CMM

Just as the use of disciplined processes have been shown to enable more predictable implementation of projects and programs, they also produce higher quality services and information systems. Overall business performance of organizations involved in incident management can be improved by applying the concepts defined in the IMIS CMM.

For internal use, the IMIS CMM provides a clear ranking of an entity's current state. By exploring the requirements to advance to the next maturity level, funding, staffing, changes in policies and technology can be easily identified for improvement. With the opportunity for an entity to compare itself with another of similar demographics, the dialog between them is instantly open to compare and support one another in advancing areas of interest. Additionally, the results of the assessment may assist in supporting documented requests, internally and/or externally, for additional resource requirements.

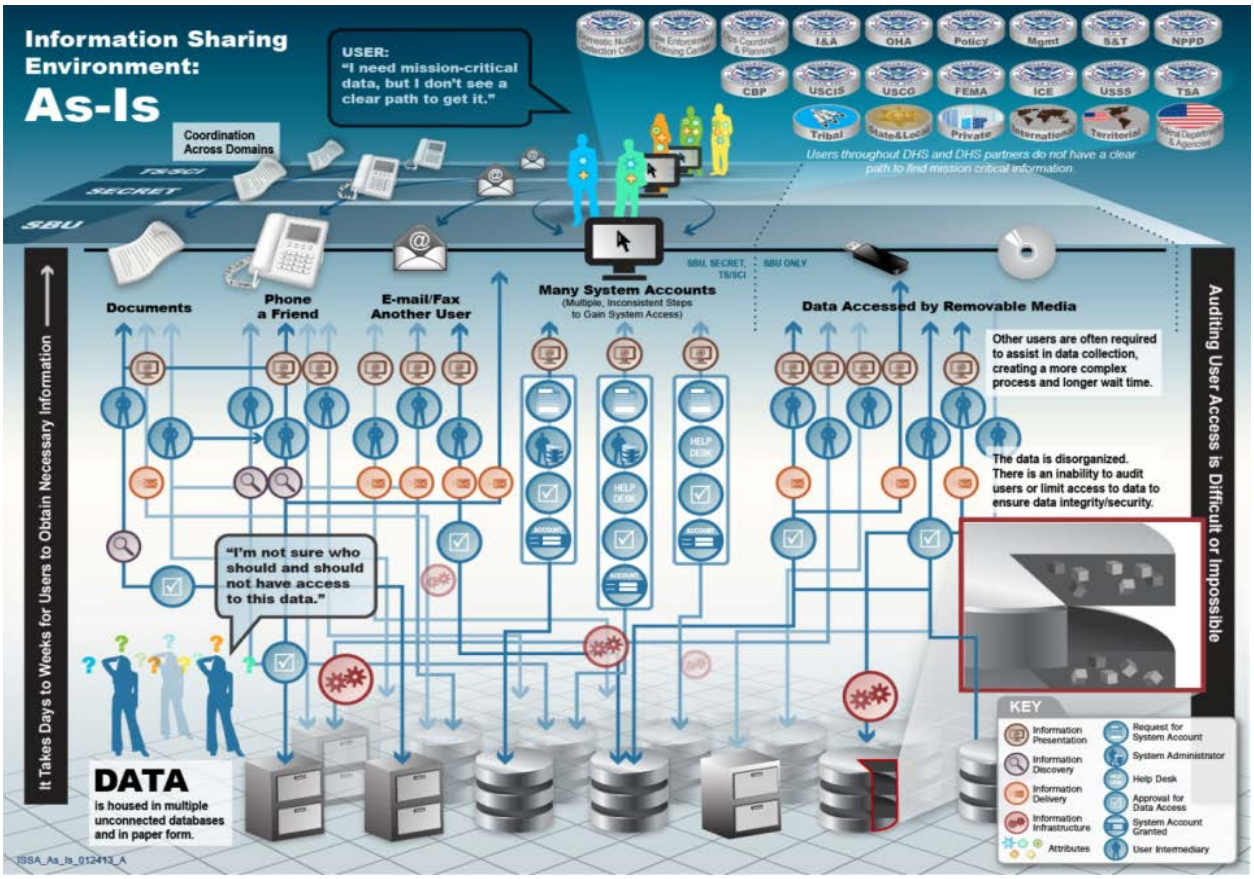
The implementation of the IMIS CMM will empower entities to provide strategic guidance and leadership in the area of incident management. Through the deployment of the Self-Assessment Tool, the IMIS will advance the national dialogue around which tools and methods can and should be deployed to improve situational awareness and information sharing capabilities at all levels of government.

PART II – IMIS CMM FRAMEWORK V1.1

2.1 Purpose

The IMIS CMM is intended to help state, local, tribal, and territorial (SLTT) agencies; federal entities; non-governmental organizations; and private sector partners in the incident management community access and share mission-critical data and information. Although general guidance materials are currently available, none provide details specific to an entity's maturity level as it relates to IMIS. At best, the as-is environment is often disconnected, as depicted in Figure 2, below.

Figure 2: As-Is ISE Graphic

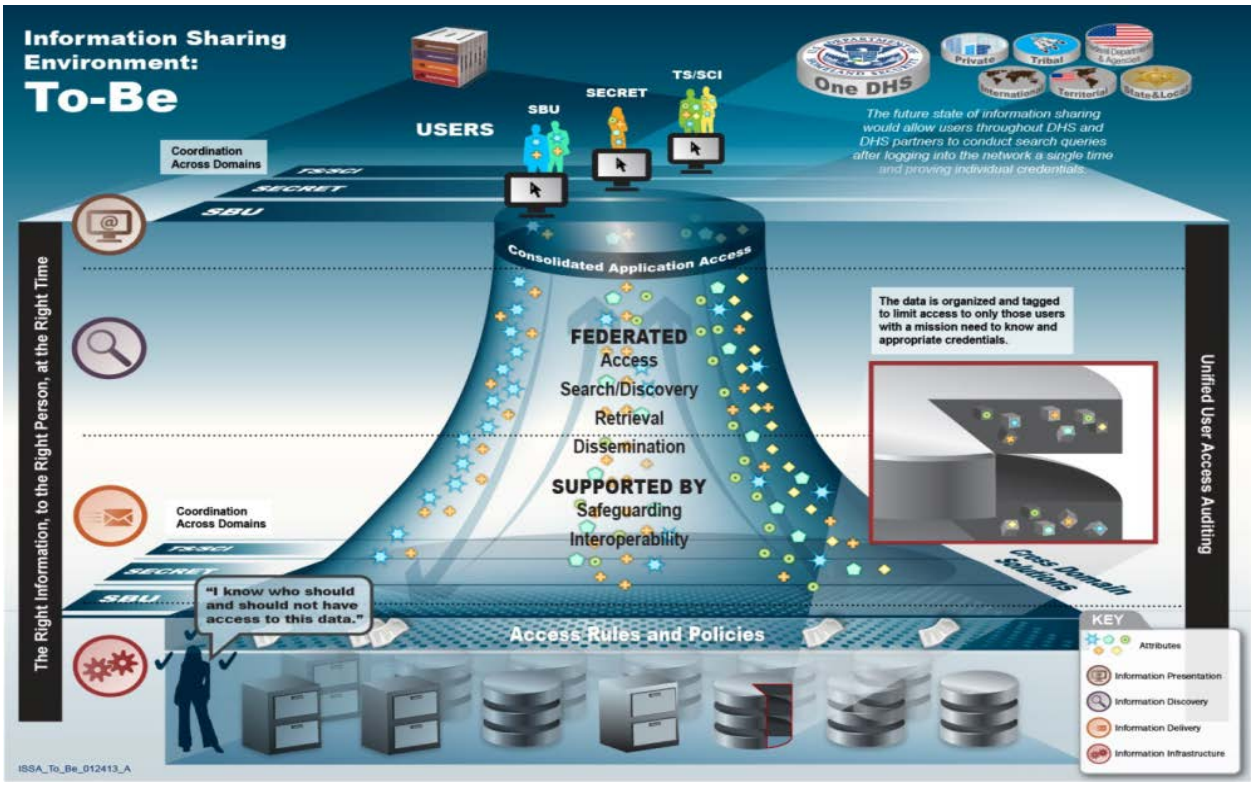


The IMIS CMM identifies the directives and authorities supporting the effort to include examples of CMM models referenced in the IMIS CMM design and details on its future development. The proposed IMIS environment depicted in Figure 3, below, will:

- Create a basis for comparing capabilities among diverse groups on a local, state, regional and national level;
- Provide a standard way of measuring progress across diverse organizations;
- Establish objective and performance-based criteria for the Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) and Science and Technology Directorate (S&T) funding and resource decisions;

- Create a focus for governance and coordination efforts;
- Provide a basis for assessing, monitoring and reporting outcomes;
- Support objective program management; and
- Establish methodology and a framework for ongoing assessment of evolving maturity of the IMIS environment.

Figure 3: Proposed To-Be ISE Graphic



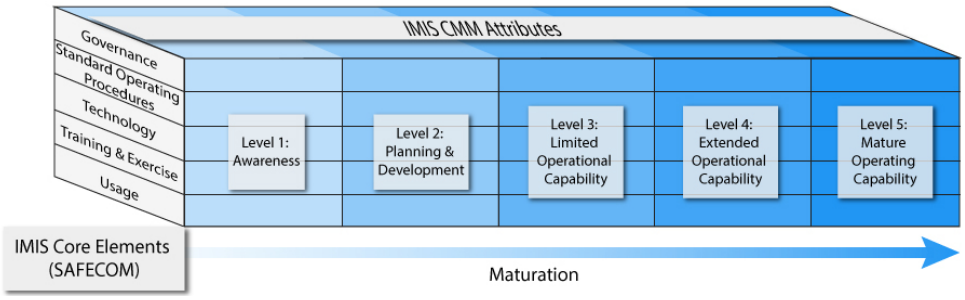
2.2 Defining the IMIS CMM

The IMIS CMM characterizes stages of maturity as they relate to an organization's incident management maturity levels and information sharing capabilities. The intent of the IMIS CMM is to evaluate an organization's capability against both of these maturity frameworks according to specific attribute descriptions provided from the Interoperability Continuum. The assessment process is organized around the five SAFECOM attributes and the related core elements.

The IMIS CMM is broken-down into three distinct layers of detail (as depicted in Figure 4, below):

- Core Elements – Adopted from SAFECOM, the core elements divide the overall IMIS mission into five manageable topics.
- Maturity Levels – The IMIS CMM Maturity Levels provide a simplistic tool for measuring maturity through the details presented within the attributes.
- Attributes – These are the finite detail of the IMIS CMM, breaking-down the core elements within the five maturity levels to convey a means to measure current status and progress within the IMIS CMM.

Figure 4: IMIS CMM Detail Graphic



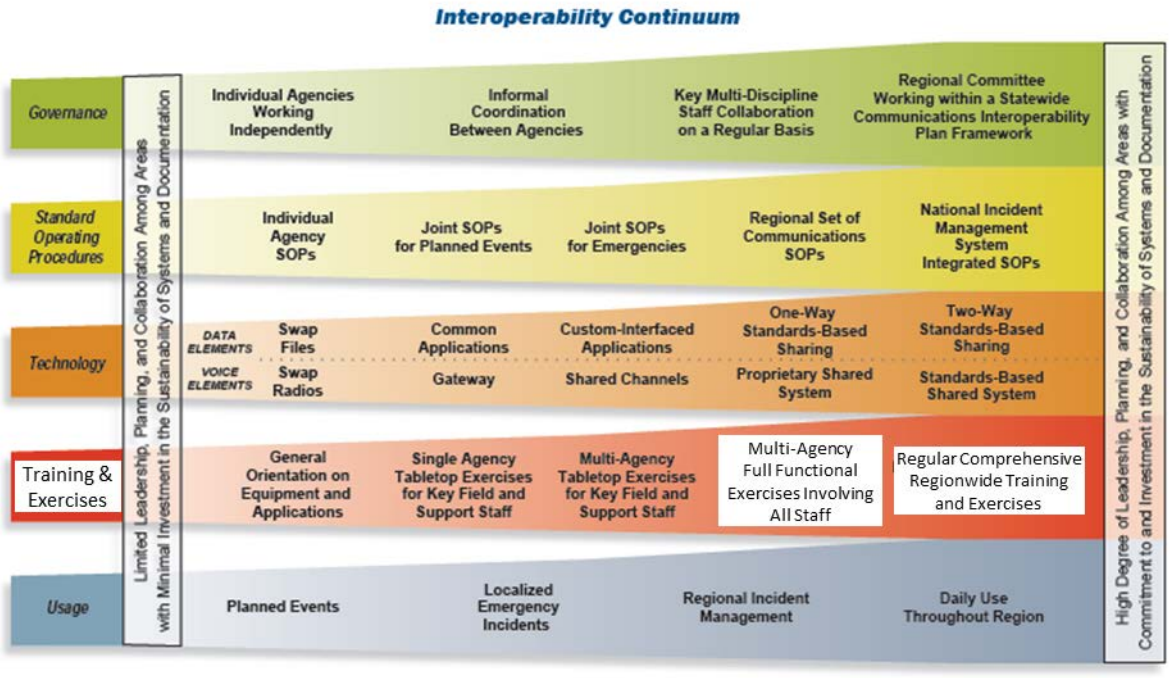
The IMIS CMM assessment results address both information management and information sharing stages to provide an accurate perspective on an entity's rating. Information management is critical to both effective availability and overall mission relevance. With regard to information sharing, the overall objective of the IMIS CMM is to empower entities with the ability to share information freely in a secure and collaborative environment. The IMIS CMM core elements, maturity levels, and attributes are discussed in detail below.

2.3 IMIS CMM Core Elements

The IMIS CMM core elements are derived from the five inter-dependent elements of the SAFECOM Interoperability Continuum[2] (Governance, Technology, Standard Operating Procedures, Training and Exercises, and Usage). These elements are used extensively to measure the maturity of an organization's incident management and information sharing capabilities.

[2] http://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2.pdf

Figure 5: SAFECOM Continuum Graphic



a. **Governance** - Establishing a common governing structure for solving issues related to incident management, information management and information sharing will improve the policies, processes and procedures of organization by: enhancing communication, coordination and cooperation; establishing guidelines and principles; clearly defining decision rights and roles and responsibilities; and reducing any internal jurisdictional conflicts. Governance structures provide the framework in which stakeholders can collaborate and make decisions that represent a common objective. It has become increasingly clear to the incident management and emergency response community that IMIS and communications interoperability cannot be solved by any one entity; achieving effective and efficient IMIS and communications interoperability capabilities requires a partnership among emergency response organizations across all levels of government. As such, a governing body should consist of SLTT and federal entities, as well as representatives from all pertinent emergency management and first response disciplines within an identified region.
b. **Technology** - Technology is a critical tool for improving IMIS and communications interoperability capabilities, but it is not the sole driver of an optimal solution. Successful implementation of technology/tools must be supported by strong governance and is highly dependent on effective collaboration and training among participating organizations and jurisdictions. Technologies should meet the interoperability requirements of practitioners on the front lines while addressing regional needs, existing infrastructure, cost vs. benefit and sustainability. The technologies organizations deploy must be scalable to effectively support day-to-day incidents as well as large-scale disasters. Often, a combination of technologies will be necessary. Security and authentication challenges are present in each technology and must be considered in all implementation decisions.
c. **Standard Operating Procedures** - Standard Operating Procedures (SOPs) are formal written guidelines or instructions for incident management, information management and information

sharing within and across jurisdictions; they typically have both operational and technical components. Established SOPs enable emergency management professionals and first responders to successfully coordinate an incident management/response across disciplines and jurisdictions. Clear and effective SOPs are essential for developing and deploying any IMIS and/or interoperable communications solution.

d. **Training and Exercises** - Implementing effective training and exercise programs to practice IMIS and communications interoperability is essential for ensuring that the technology works and responders are able to effectively share information and communicate via multiple methods (e.g., voice and data) during emergencies.
e. **Usage** - Usage refers to how often IMIS and interoperable communications technologies are used. Success in this element is contingent upon progress and interplay among the other four elements on the Interoperability Continuum.

2.4 IMIS Maturity Levels [3]

The IMIS maturity levels provide a maturity categorization across the IMIS core elements with the intention of rating an entity across a 0-5 scale within each element. The levels are defined below.

- **Level 0: No Capability**
- **Level 1**: **Awareness**
  The entity is somewhat aware of the data/information available from SLTT and federal partners and is not certain where or how to obtain access on a consistent or sustainable basis. They operate without established IMIS objectives and their processes and practices are inconsistent and unpredictable with a high risk of variation and deficiency. Deficiencies are not systematically identified and employees' roles and responsibilities and not defined or documented.
- **Level 2**: **Planning and Development**
  The entity is actively coordinating with a governing body to build operational capacity for IMIS. Formal planning activities and objectives are in place, but are not yet prioritized or implemented. Incident management processes and practices are dependent on the knowledge of individuals and their personal relationships with others. Initial discussions with information sharing partners regarding the establishment of formal information sharing agreements and protocols are underway, but are not yet documented. The entity is generally aware of the data/information available from SLTT and federal partners but has not developed formal relationships for access. Effectiveness is not adequately evaluated, and defined roles and responsibilities for information management may not be fully documented or understood by all employees.
- **Level 3**: **Limited Operational Capability**
  Objectives are in place, prioritized and adequately documented. Incident management processes and practices are evaluated on a periodic basis. The evaluation process is not well documented, however. The entity is aware of the data/information available from SLTT and federal partners; it has agreements in place and has documented and uses some formal information sharing agreements/protocols. The entity has defined the Essential Elements of Information (EEIs) required to support operations and is capable of using both static and dynamic EEIs to support daily internal operations. Employees are aware of their documented

[3] ***Note****: The stage definitions were inspired by the emergency management maturity level definitions discussed on page 12 of the 2008 Tiems Emergency Management Maturity Model prepared by Booz Allen Hamilton.*

IMIS roles and responsibilities and are capable of discovering, creating, consuming, publishing, sharing and securing data/information from various internal and external sources into a consolidated daily situational awareness view.

- **Level 4**: **Extended Operational Capability**
  The entity has an institutionally adopted enterprise-level capability to manage information internally and to share both static and dynamic information with external partners at various levels for operational use. Employees are aware of their documented roles and responsibilities, and technology is applied tactically to ensure the use of predictable and consistent IMIS processes and practices. IMIS objectives are in place, documented, prioritized and reviewed on a periodic basis. Incident management processes and practices are evaluated on a scheduled basis and consistent follow-up addresses identified process deficiencies. Formal information sharing agreements and protocols for all EEIs and other critical data/information are documented and used on a consistent basis.
- **Level 5**: **Mature Operating Capability**
  The entity is capable of adapting to unfolding incidents/events and providing the appropriate data discovery, sharing, analysis, and recommendation for decision making. Technology is strategically applied to ensure continuous assessment, monitoring and improvement of the IMIS processes and practices to optimize their enterprise-level capabilities. Employees are aware of their documented roles and responsibilities and are proactively involved in continuous process improvement. Objectives are in place, prioritized, reviewed on a scheduled/continual basis and documented. The evaluation process is well documented and consistent follow-up addresses identified process deficiencies.

2.5 IMIS CMM Attributes

The IMIS CMM Attributes in Tables 1-5, further define the core elements so as to refine an organization's understanding of the maturity level of its incident management operations, information management and information sharing capabilities. These attributes are utilized by the IMIS CMM to provide the means for an entity to complete the IMIS CMM self-assessment.

Table 1 – IMIS CMM Governance Attributes

IMIS CMM Governance Element
Level 0: No Capability
Level 1: Awareness
GV101 - The entity acknowledges the value of IMIS and the intention to establish working groups to implement the operational IMIS capabilities.
GV102 - Personal connections enable some information sharing and collaboration to occur.
GV103 - Technical staff implement ad hoc governance activities on behalf of the entity.
GV104 - The entity recognizes that IMIS activities will require dedicated staff and funding.
GV105 - The entity has internal executive-level support for the development of an IMIS program.
Level 2: Planning and Development
GV201 - An IMIS Executive Committee has been established. Members represent functions that include broad executive leadership (e.g., Emergency Management Director, Homeland Security Advisor, Geospatial Information Officer (GIO), Chief Information Officer (CIO) and Chief Financial Advisor).
GV202 - An IMIS Governance Working Group (EQV) has been established.
GV203 - IMIS working groups have been established to address SOPs, Technology, Training and Exercises, and Usage with defined cross-collaboration and meeting schedules.
GV204 - The entity has an IMIS strategy that aligns with various local and national strategies/policies.

IMIS CMM Governance Element
GV205 - The entity has an IMIS Action Plan in place to monitor its progress in attaining its desired to-be state.
GV206 - Written and approved entity policies exist for IMIS enterprise development, maintenance and use.
GV207 - IMIS Executive Committee takes proactive steps to identify, prioritize and address IMIS cultural barriers while socializing concepts across the community.
GV208 – The entity has developed a Work Breakdown Structure and schedule to implement the IMIS enterprise.
GV209 - The entity has initiated engagements with internal stakeholders to draft policies and procedures for IMIS coordination.
GV210 - The IMIS Executive Committee has a business plan to support budget and funding requirements related to geospatial programs and IMIS for the emergency management and first responder communities.
GV211 - An IMIS Enterprise Implementation Plan is in development to address relationships with other management disciplines.
Level 3: Limited Operational Capability
GV301 - The Governance Executive Committee is formally chartered.
GV302 - IMIS related risks are proactively identified, reported and mitigated.
GV303 - The entity has conducted a Privacy Impact Assessment.
GV304 - An IMIS Business Plan has been developed to support first responders, including budgeting and training/exercises.
GV305 - The Governance Executive Committee has reviewed/commented on budget/funding issues related to geospatial programs and information sharing for first responders.
GV306 - The entity has a system to address integration of new requirements and ensure minimal repetition of preventable issues.
GV307 - IMIS budgetary requirements are validated for funding.
GV308 - IMIS human capital plans exist and are met (where applicable).
GV309 - The IMIS Executive Committee is fully represented and is responsible and accountable for all aspects of the IMIS capability development.
GV310 - The IMIS Executive Committee has approved the draft IMIS Action Plan and directed it to the working groups for final approval specific to their respective workflow requirements.
GV311 - The entity has defined policies, procedures and protocols to enable IMIS coordination with internal stakeholders and external partners.
Level 4: Extended Operational Capability
GV401 - The entity has an information sharing strategy that is aligned with various local, regional, tribal and national strategies and policies.
GV402 - The entity coordinates the development of information sharing grant requests and oversees execution of scope for awards grants.
GV403 - The entity coordinates with regional SLTT partners, federal agencies, critical infrastructure/key resource (CIKR) partners and NGOs to develop and implement IMIS information sharing agreements.
GV404 - The entity has a published SOP inclusive of all EEI sharing aspects and the intended use/context of use for various functions.
GV405 - IMIS Human Capital capabilities are continuously improved.
GV406 - An IMIS Enterprise Program Office (EQV) has been established.
GV407 - The entity has legal frameworks (i.e., policies, procedures and protocols) in place that guide/enable IMIS with internal stakeholders and external partners.
GV408 - Technology recommendations are collected for information sharing standards and provided to the CIO for establishment and enforcement.
GV409 - The entity has established a privacy policy to include For Official Use Only, Law Enforcement Sensitive, Sensitive But Unclassified, Protected Critical Infrastructure Information, etc.
Level 5: Mature Operating Capability
GV501 - The entity is fully engaged at SLTT and national levels, governing standards for technology, budgets, grant requests, interoperability, business planning, training and usage.

IMIS CMM Governance Element
GV502 - The entity has an outreach program to build partnerships with SLTT, federal government, NGO and private sector partners, and to inform representatives, senior executives, political leaders and strategic partners on the IMIS capabilities available to them.
GV503 - A methodology is executed to ensure that governance activities are continuously monitored for improvements (continuous feedback loop).
GV504 - The entity's business plan is updated on annual basis to reflect lessons learned from training, exercises and incident response, and proposes budget incentives.
GV505 - IMIS inputs impact the entity's budget formulation and execution for first responder information sharing.
GV506 - The entity has appropriate business continuity plans (to include Continuity of Operations Planning (COOP) and Continuity of Government (COG)) developed that clearly identify how IMIS would be conducted in a degraded environment.

Table 2 – IMIS CMM SOP Attributes

IMIS CMM SOP Element
Level 0: No Capability
Level 1: Awareness
SO101 - Information requirements are generally understood among technical staff but are not systematically defined or documented.
SO102 - Information sharing processes are not currently repeatable and are dependent on the knowledge of a few individuals.
SO103 - Individual notes and processes have been collected in an effort to leverage existing contacts and shared data to support future documentation to be accessible to all staff.
SO104 - The entity has not formalized information sharing templates, job aids, SOPs or ad-hoc process documents.
Level 2: Planning and Development
SO201 - An IMIS SOP Working Group (EQV) has been established.
SO202 - SOPs for data sharing are in development between agencies for local hazards and threats.
SO203 - A targeted interoperability framework and architecture for IMIS exists, has been approved by the operations working group and executive committee, and is promoted by the CIO (or EQV).
SO204 - IMIS SOPs have been developed to address general data management, maintenance and currency.
SO205- SOPs for the collection of incident data fully address metadata requirements identified by the Usage Working Group.
SO206 - Data sharing agreements and use agreements have been initiated with internal and external partners.
SO207 - An IMIS SOP had been developed to reference policies for identification and documentation of authoritative information.
SO208 - Relevant SOPs include details on technical skills required by key staff.
Level 3: Limited Operational Capability
SO301 - Joint information sharing SOPs have been developed between some key agencies and have been reviewed and approved by the SOP working group.
SO302 - Standards have been documented for internal enterprise-level information sharing.
SO303 - A comprehensive plan is in place to ensure approval of IMIS SOPs by the Governance and other working groups.
SO304 - IMIS SOPs and products are being developed/deployed according to a documented methodology.
SO305 - IMIS methodologies and products are designed to support the EEI content management, sharing and analysis framework.
SO306 - The entity has identified and adopted IMIS standards for managing, publishing and sharing key information (i.e., file formats and metadata) within its SOPs.

IMIS CMM SOP Element
SO307 - IMIS methodologies have been collected from all working groups as SOPs.
SO308 - The entity has secured formal agreements with data custodians of the targeted EEIs.
Level 4: Extended Operational Capability
SO401 - Joint SOPs have been developed to include external SLTT and federal entities as required.
SO402 - SOPs have been approved by the governance body for all major relevant incident types.
SO403 - The entity's SOPs are aligned with key standards (i.e., National Incident Management System (NIMS), Homeland Security Geospatial Concept of Operations, Presidential Directive 8 (PPD-8), Federal Geographic Data Committee, National Spatial Data Infrastructure, National Information Exchange Model (NIEM), National Institute of Standards and Technology or EQV).
SO404 - The entity has published SOPs for IMIS use and standardization across its respective external partners.
SO405 - SOP Working Group membership has been extended to include SLTT partners.
SO406 - Innovation and technology advancement is incorporated into SOP updates.
SO407 - The entity's SOP planning includes an achievable feedback loop to collect and adjudicate edits and updates.
Level 5: Mature Operating Capability
SO501 - All SOPs are fully NIMS (EQV) compliant.
SO502 - The entity has a Catastrophic Response Plan (EQV) with an IMIS Annex.
SO503 - Post-event AARs are addressed across all related IMIS SOPs
SO504 - SOPS reference PPD-8 Mission Areas where appropriate.
SO505 - All SOPS are validated for accuracy, currency and relevancy on an annual schedule.

Table 3 – IMIS CMM Technology Attributes

IMIS CMM Technology Element
Level 0: No Capability
Level 1: Awareness
TC101 - Capabilities exist to share information on a case-by-case basis, but an agreed upon IMIS architecture does not exist.
TC102 - The entity is aware of the need to identify standards, system requirements, enterprise/technology architecture design, etc., but has yet to formally define these parameters.
TC103 - The entity has minimal standard methodologies to support the discovery of key information maintained internally (currently depend upon staff knowledge).
TC104 - Technology resources exist for complete backup and archival of existing data holdings. Limited cataloging of these archives makes discovery and efficient recoveries challenging.
Level 2: Planning and Development
TC201 - An IMIS Technology Working Group (EQV) has been established.
TC202 - The entity has an inventory of technologies, providers and points of contact for each of the EEIs identified.
TC203 - The entity identifies standards, system requirements and enterprise/technology design considerations to enable common operating standards.
TC204 - Standards for IMIS and communications interoperability include the utilization of NIEM and Geo4NIEM methodologies.
TC205 - The technology strategy includes a scalability plan to ensure resiliency and redundancy.
TC206 - Technology-specific enterprise-wide IMIS architecture plans have been established and adopted for implementation.
TC207 - An Identity Credentialing and Access Management (ICAM) plan exists, utilizing existing programs and standards (where applicable).
TC208 - One-way information sharing between common systems and applications is operational.

IMIS CMM Technology Element
TC209 - The entity's Technology Usage Plan aligns with the business process, agreements and operational pace defined by the Governance Working Group, Usage Working Group and operational staff.
Level 3: Limited Operational Capability
TC301 - IMIS technology products are being developed/deployed using available tools.
TC302 - Automated enterprise-wide and user-defined tools for IMIS exist.
TC303 - User interface(s) for IMIS technologies are operations-centric and user-friendly to the non-technical operations staff.
TC304 - The entity's system has the capability to create and save an event record when a call or report is introduced.
TC305 - The entity's technology suite provides a clear capability/pathway for operators to create, publish and share incident specific data (EEIs) to external partners using NIEM standards.
TC306 - Database schemas (both geographic information systems (GIS) and non-GIS databases) are updated to reflect the IMIS and metadata requirements to support operational decision making.
TC307 - Target architecture for IMIS activities is approved for implementation by the Governance Working Group to include standards for information sharing and ICAM.
TC308 - The entity is beginning to consume EEI data provided from numerous internal and external sources into a consolidated situational awareness viewer for operations.
TC309 - An architecture transition plan exists and has been approved by appropriate working groups, CIO and GIO (EQV).
TC310 - An enterprise-wide IMIS development plan and maintenance methodology exists.
Level 4: Extended Operational Capability
TC401 - IMIS Data Sharing Agreements are expanded to include sharing with SLTT, federal and other key partners.
TC402 - Two-way sharing between common systems and applications fully operational.
TC403 - The entity's technology suite enables operators with the capability to manage, analyze and use incident-specific data for operations-specific decision making.
TC404 - The entity has a technology deployment, training and usage action plan inclusive of appropriate COOP and COG considerations.
TC405 - A transition plan is in-place to target architecture, including a funding plan, completed and adopted by the GIO and CIO or equivalents.
TC406 - The technology suite is owned and/or licensed, and operated within the entity's resource network environment (where applicable).
TC407 - Appropriate system and network security is in place for the level of sensitivity of the data and operations conducted on a daily basis.
TC408 - The data publication schema aligns with local, state, regional and/or national metadata requirements.
TC409 - Methodologies and tools exist to determine investment compliance with operational architectures and related tools available locally, regionally or nationally.
TC410 - The IMIS enterprise-wide technology suite and architecture framework is sustainably funded to include a suite of incident management systems, databases, systems of record, geospatial capabilities and information management practices.
Level 5: Mature Operating Capability
TC501 - The entity's technology suite integrates data directly from external database resources and external identity management providers (where applicable).
TC502 - Integrated repository tools and common IMIS framework and methodologies are used across the enterprise.
TC503 - Information sharing architecture operations and maintenance levels are fully funded.
TC504 - The entity maintains full resiliency and redundancy to ensure information accessibility should they be directly impacted by an event.
TC505 - IMIS architecture and human resource plans are fully funded and sustainable.

IMIS CMM Technology Element
TC506 - The entity's technology investments are informed by the IMIS strategy and action plan identified by the governing bodies (i.e., IMIS Executive Committee and Governance Working Group).

Table 4 – IMIS CMM Training and Exercise Attributes

IMIS CMM Training and Exercise Element
Level 0: No Capability
Level 1: Awareness
TE101 - Staff have an awareness/understanding of IMIS-related events, demonstrations, exercises or situational awareness tools (i.e., Virtual USA).
TE102 - Lessons learned documents are available from past events and exercises but seldom compiled or incorporated into a formal improvement plan.
TE103 - Information sharing staff have experience participating in past events and exercises with limited exposure to the management of exercise design and control functions.
TE104 - IMIS subjects are in discussion concerning training and exercise plans but have not been formally prioritized across the entity.
Level 2: Planning and Development
TE201 - An IMIS Training and Exercises Working Group (EQV) has been established.
TE202 - Outreach materials have been developed around general information sharing to include brochures, white-papers, presentations and/or Web content.
TE203 - The entity has included considerations for technology deployment, training and a usage action plan to include COOP and COG.
TE204 - Training materials are in development to address information sharing activities to include use cases.
TE205 - The entity's tabletop exercises incorporate specific references to IMIS activities.
TE206 - Operations staff are trained in IMIS enterprise framework, methodology, tools and usage.
TE207 - Post-event hot-wash findings are captured within AARs and provided to appropriate working groups.
TE208 - IMIS Executive Committee members are trained in IMIS principles and concepts.
Level 3: Limited Operational Capability
TE301 - Information sharing is incorporated into exercise planning.
TE302 - Internal outreach efforts have been conducted across the entity concerning IMIS efforts.
TE303 - IMIS technology elements are included with all exercise events.
TE304 - Initial versions of IMIS training materials are implemented.
TE305 - Technology training relevant to IMIS capability subject areas has been developed and deployed.
TE306 - The entity has developed a multiyear IMIS Training and Exercise Plan.
TE307 - AAR findings are incorporated into the entity's improvement plan for execution.
TE308 - The entity has two or more specific event type training and exercise scenarios with IMIS objectives (connected to SOPs).
TE309 - Approved SOPs are exercised on an annual basis with additional SOPs under development.
Level 4: Extended Operational Capability
TE401 - Training materials reflect all hazards and all threats, and integrate all phases of the emergency lifecycle.
TE402 - Operational and technical staff are fully trained on the use of enterprise-wide IMIS applications.
TE403 - The entity conducts training and exercise functions regularly in a coordinated effort to test and evaluate its operational capability as it relates to the use of EEIs and enabling technologies.
TE404 - The entity leads or participates in annual multiagency full-functional exercise(s).
TE405 - The entity participates with external entities on large-scale exercises.
TE406 - The entity conducts one annual tabletop exercise specific to IMIS activities.
TE407 - The entity has an annual technology stress-test, usage reporting statistics and impact analysis on the use of technology to support operations.

IMIS CMM Training and Exercise Element
Level 5: Mature Operating Capability
TE501 - The entity has a multi-year exercise plan inclusive of domain specific, cross-domain and national-level exercises.
TE502 - Training programs and materials are updated and published to include compliance with NIMS (EQV).
TE503 - Regular comprehensive regional training and exercises are completed annually.
TE504 - The entity participates in national-level exercises where available.

Table 5 – IMIS CMM Usage Attributes

IMIS CMM Usage Element
Level 0: No Capability
Level 1: Awareness
US101 - Incident information requirements are currently notional and requires further discussion and assessment.
US102 - The entity understands that information sharing is currently based upon individual knowledge and must be documented for functionality to be fully repeatable.
US103 - The entity engages in ad hoc first responder information sharing and coordination between other entities and individuals.
US104 - The entity has identified its general data requirements but has not formalized reliable access to them.
Level 2: Planning and Development
US201 - An IMIS Usage Working Group (EQV) has been established.
US202 - Limited information sharing routinely occurs for planned events with some repeatable processes and methods in place.
US203 - Relevant internal (core) data is fully available across the enterprise.
US204 - Internal applications utilize shared data resources.
US205 - The entity is aware of data/information available to it from SLTT, federal government, NGO and private sector partners but does not have agreements or systems to ensure optimal access.
US206 - Data for key operational activities has been identified and is being collected as EEIs.
US207 - A data validation/verification criteria and process has been developed to ensure information accuracy.
US208 - Baseline data is utilized internally to demonstrate added value to future investments.
US209 - EEI's are being identified and developed into the EEI SOP.
US210 - The entity has distributed an internal end-user survey or conducted a work-shop to assess overall data usage and performance.
Level 3: Limited Operational Capability
US301 - The entity has defined non-event data to be published/shared internally and externally.
US302 - The entity has defined event-specific data to be published/shared internally and externally.
US303 - The entity's identified EEI information requirements are met.
US304 - The entity's incident event records include a geographic representation for address verification and event mapping.
US305 - IMIS-based data usage is routine for localized events.
US306 - The entity's incident event records include the originating and target IP addresses where available.
US307 - The entity has a strategy for collecting event log files (to include network traffic) to ensure accurate chronology tracing of event progress.
US308 - The entity has established a formal plan and capabilities to monitor usage and provide feedback to the Governance Working Group for action.
US309 - Internal coordination is in place with the DHS GII.
Level 4: Extended Operational Capability
US401 - Daily usage of IMIS data for local incidents the norm.
US402 - Capabilities to support external IMIS data sharing are utilized.

IMIS CMM Usage Element
US403 - The entity's key data is actively shared with its external community through a live connection.
US404 - The entity is documenting success stories and providing them to the IMIS Executive Committee to validate overall efforts.
US405 - Information sharing issues are identified and resolved across all levels of security access.
US406 - A usage survey has been developed and distributed to stakeholders to derive operational enhancements in the provision of IMIS services.
Level 5: Mature Operating Capability
US501 - Daily usage of IMIS data is in place for incidents ranging from local events to incidents of national significance.
US502 - External partners have access to the entity's data through shared services.
US503 - The entity has a system in place to submit Requests for Information to discover and secure new information requirements and sources.
US504 - A suite of technology generated products (i.e., reports) has been identified and implemented for use by various internal and external functions (i.e., Emergency Support Functions, executive, other agencies) as defined by the SOP Working Group.
US505 - IMIS methodologies and tools are continuously monitored and improved.
US506 - The entity’s executive and operations staff regularly interact with the technologies available to them for decision making.

PART III – IMIS CMM IMPLEMENTATION

3.1 Overview of IMIS CMM Implementation Assessment Framework

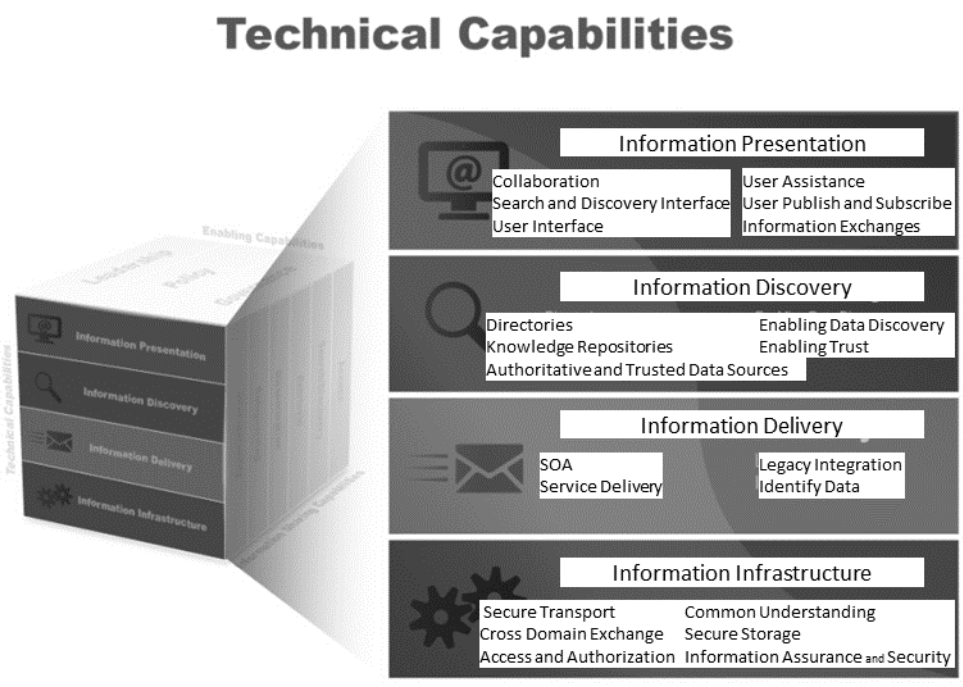
With reference to the SAFECOM Elements (Governance, Standard Operating Procedures, Technology, Training and Exercise, and Usage), the IMIS CMM Attributes will provide the mechanism for self-assessment. The IMIS CMM Self–Assessment Tool will facilitate an entity in defining its existing capability maturity stage and guide it in advancing its overall IMIS abilities.

Implementation of the IMIS CMM will be accommodated through the distribution of the IMIS CMM Self-Assessment Tool across the SAFECOM, homeland security, first responder and related communities. Entities will have the opportunity to review their results internally as well as provide them to the IMIS CMM team for review and comment with the output information supporting the identification of current capabilities at the community level.

Target Technical Capabilities

The IMIS CMM will enable an assessed entity to progressively implement/deploy the IMIS technical capabilities across its IMIS environment. Key elements addressed by the IMIS CMM are further described in Figure 6 below.

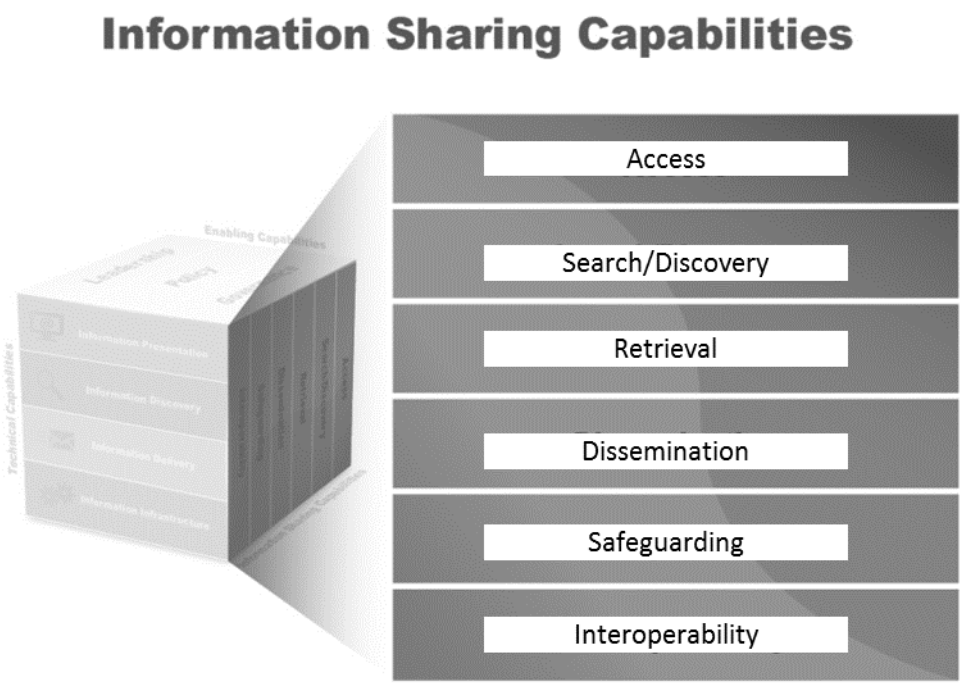
Figure 6: IMIS CMM Target Technical Capabilities Graphic



3.2 Target Information Sharing Capabilities

Improved information sharing is a critical outcome of the IMIS CMM effort. Through the implementation of the IMIS CMM, entities will be able to identify a progressive path to improvements across their IMIS environments. Key elements addressed by the IMIS CMM are further described in Figure 7 below.

Figure 7: IMIS CMM Target Information Sharing Capabilities Graphic



3.3 IMIS CMM Self-Assessment

The IMIS CMM Self-Assessment Tool provides a flexible rating system to assist an entity in measuring its maturity levels as they relate to IMIS. The tool operates as a stand-alone application and provides a simple output identifying maturity as it relates to the SAFECOM Continuum. Entities are free to share the results internally as a mechanism to validate their abilities and externally to compare themselves to similar entities across the country.

The results are displayed in both textual and graphic formats to facilitate the best use of the information. Entities should use the information as a validation discussion tool with their internal partners to determine if the results properly reflect their abilities. After clarification on any misunderstood questions or capabilities, the tool can be run again to provide full and proper representation of the entity's rating.

The results can then be utilized to determine the required steps for advancement and future goals. In addition, ratings can be compared with those of entities of similar population and/or similar desired IMIS abilities.

The Self-Assessment Users Guide is found in Appendix B of this document.

Appendix A: Acronyms

AAR	After Action Report
CIO	Chief Information Officer
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
COG	Continuity of Government
COOP	Continuity of Operations Planning
EEI	Essential Elements of Information
EQV	Equivalent
GII	Geospatial Information Infrastructure
GIO	Geospatial Information Officer
ICAM	Identity, Credential and Access Management
IMIS	Incident Management Information Sharing
ISE	Information Sharing Environment
ISSA	Information Sharing Segment Architecture
NIEM	National Information Exchange Model
NIMS	National Incident Management System
PPD-8	Presidential Policy Directive – 8 National Preparedness
SEI	Software Engineering Institute
SLTT	State, Local, Tribal, Territorial
SOP	Standard Operating Procedure

Appendix B: Incident Management Information Sharing Capability Maturity Model Self-Assessment Implementation Guide

This guide provides basic direction on utilization of the Incident Management Information Sharing (IMIS) Self-Assessment Tool (SAT). The goal of the IMIS self-assessment is to support an entity's effort to rate themselves within the IMIS Capability Maturity Model (CMM). The IMIS CMM SAT provides the opportunity to identify the IMIS CMM Attributes an entity has completed and provides an output report identifying the entity's current IMIS maturity levels within each of the core elements. Once completed, the derived IMIS CMM Self-Assessment Report can further assist decision making about future activities, funding and capability requirements.

A. Planning for Implementation

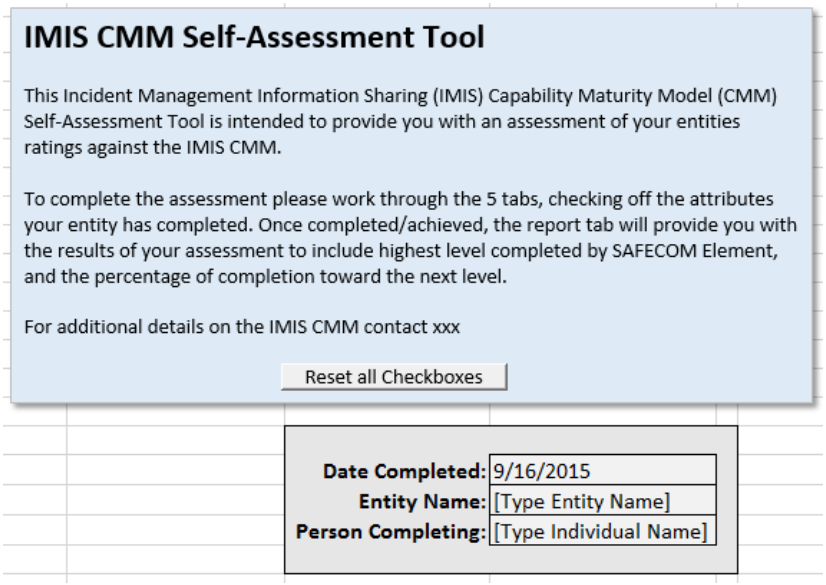
The most important factor in conducting an IMIS CMM Self-Assessment is ensuring that an entity has full representation from its IMIS-related community. Participants should include executive leadership (e.g., Chief Information Officer, Chief Technology Officer), IMIS-specific functional managers and IMIS practitioners (e.g., law enforcement, fire and emergency medical services). This broad participation ensures that all aspects of IMIS tools, methodologies and data/information factors are fully addressed.

It is recommended that the self-assessment be completed during a 2-4 hour facilitated group session. This setting will support open discussions concerning each of the IMIS CMM Attributes and ensure accurate and relevant results.

B. The Self-Assessment Process

The IMIS CMM SAT is a simple Microsoft Excel Workbook. To complete an assessment, the entity representatives work across each of the IMIS CMM core element Tabs to identify attributes that have been achieved. The tool provides an output identifying the highest level completed within each core element and also provides the percentage completed to the next level to track progress.

Step 1: Enter the entity's information.



Step 2: Work through each of the five tabs (by core element) and select the IMIS CMM Attribute completed by the entity.

IMIS CMM Governance Element	
Level 0: No Capability	
Level 1: Awareness	
GV101-Entity acknowledges the value of Incident Management Information Sharing and the intention to establish working groups to implement the operational IMIS capabilities.	☑
GV102-Personal connections enable some information sharing and collaboration to occur.	☑
GV103-Select technical staff are relied upon to implement ad hoc governance activities on behalf of the entity.	☑
GV104-Entity recognizes that IMIS activities will require dedicated staff and funding.	☑
GV105-Entity has Internal Executive-Level support for the development of an IMIS program.	☑
Level 2: Planning & Development	
GV201-IMIS Executive Committee has been established. Members represent functions that include broad executive leadership (i.e. Emergency Management Director, Homeland Security Advisor (HSA), Geospatial Information Officer (GIO), Chief Financial Advisor (CFO), and Chief Information Officer (CIO)).	☑
GV202-IMIS Governance Working Group has been established.	☐
GV203-IMIS Working Groups have been established to address SOPs, Technology, Training and Exercises, and Usage with defined	☐

Step 3: View and save the entity's output report.

IMIS CMM Self-Assessment Report v1

Entity Name: Sample Entity
Person Completing: Sample Employee
Date Completed: 9/16/2015

Governance	Level % Complete	% to Next Level
Level 1: Awareness	100	
Level 2: Planning & Development	64	
Level 3: Limited Operational Capability	0	
Level 4: Extended Operational Capability	0	
Level 5: Mature Operating Capability	0	36%

Standard Operating Procedures	Level % Complete	% to Next Level
Level 1: Awareness	100	
Level 2: Planning & Development	25	
Level 3: Limited Operational Capability	0	
Level 4: Extended Operational Capability	0	
Level 5: Mature Operating Capability	0	75%

Technology	Level % Complete	% to Next Level
Level 1: Awareness	100	
Level 2: Planning & Development	100	

Once the assessment is completed, the SAT can be saved, noting the current date for future reference. By reviewing the unselected attributes, an entity can quickly identify areas for improvement and thereby plan to achieve a higher maturity rating.