USMC

MCTP 3-30B

Information Knowledge Management

U.S. Marine Corps

PCN 147 000030 01

USMC

A no-cost copy of this document is available at:
https://www.marines.mil/News/Publications/MCPEL/

Report urgent changes, routine changes, and administrative discrepancies by letter to the Doctrine Branch at:

Commanding General
United States Marine Corps
Training and Education Command
ATTN: Training Standards Division, Doctrine Branch
2007 Elliot Road
Quantico, VA 22134-5010

or by email to: usmc_doctrine@usmc.mil

Please include the following information in your correspondence:

Location of change, publication number and title, current page number, and, if applicable, paragraph and line number.
Figure or table number (if applicable).
Nature of change.
Text addition or deletion.
Proposed new text.

Copyright Information

UNITED STATES MARINE CORPS

1 July 2026

FOREWORD

Marine Corps Tactical Publication (MCTP) 3-30B, *Information Knowledge Management*, builds on the doctrinal foundation established in Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control*. Since the original publication of MCDP 6, technology improvements have led to more effective command and control (C2) capabilities; yet, with an ever-increasing volume of data combined with overly complex information processes, warfighters face a slew of new challenges. The shift from information management to information and knowledge management (IKM) reflects an expanded focus—from simply handling and distributing information to effectively leveraging it for decision making and gaining operational advantage.

This publication provides an overview and definition of IKM, presents examples and guidance for strategies, suggests best practices, details responsibilities, and presents organizational constructs for planning and execution. Its focus is at the tactical and operational levels, and it refers to relevant theater strategic issues as necessary. This publication is organized around the pillars of C2 information, people, tools, and support structure because IKM is key to command and control, which is integral to a learning organization.

As stated in MCDP 6, command and control is essential to all military operations and activities. There is no substitute for effective command and control and the leadership responsibilities that come with staff organization and collaboration. This publication serves as the authoritative reference for IKM concepts, highlighting its relationship to command and control. The intended audience is commanders, staffs, IKM officers, operations officers, communication officers, and all users of information technology. This publication supersedes MCTP 3-30B, *Information Management*, dated 18 June 2014, erratum dated 2 May 2016, and Change 1, dated 4 April 2018.

Reviewed and approved this date.

RORY D. KENT
Colonel, U.S. Marine Corps
Director, Marine Air Ground Task Force Staff Training Program

Publication Control Number: 147 000030 01

Table of Contents

Chapter 4. Information and Knowledge Management Processes and Procedures

Appendicies

Glossary

References and Related Publications

Chapter 1.
Information and Knowledge Management Fundamentals

Vital Command and Control Enabler

Information management is an enabler of command and control (C2) rather than a discrete element of it. The pillars of command and control are people; information; and the C2 support structure, which includes organizations, procedures, equipment, facilities, training, education, and doctrine. Although information management has been a factor of C2 planning for many years, with the 2022 release of Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5780.01, *Joint Knowledge Management Program*, information management has become an inseparable part of command success. Information and knowledge management integrates people and processes throughout the information lifecycle to create shared understanding, improve decision making, and increase organizational performance. The convergence of information and knowledge management (IKM) relies on the transformation and maturation of data for the decision maker. It focuses on decision-cycle effectiveness, shared understanding through collaboration, mission and organizational performance, agile learning, and capturing knowledge. This is achieved by designing the battle rhythm, using tools to optimize staff processes and their harmonization across the command as part of the joint force.

As emphasized in Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control*, warfighters function in environments of uncertainty. Combat is by nature chaotic, disruptive, and unpredictable. Data collected and processed in combat and potential combat environments can be inaccurate or misleading and the resulting information could be too late, unimportant, or irrelevant to be useful. A commander who understands the correlation between quality information and the ability to make timely and effective decisions can build a reliable understanding of the challenges they face. However, advances in data science, computing, communication technologies, and generative artificial intelligence have exponentially increased the volume of available information. The demands of war have often led to an effort to combine new technology with tactics, techniques, and procedures (TTP) to build warfighting capabilities. Combining technology, procedures, and human involvement provides a tactical advantage against adversary and enemy vulnerabilities, allowing friendly forces to defeat enemy strengths to achieve the desired end state. Just as a lever provides the force to move the heaviest weight, information and knowledge are the "levers" that increase the commander's speed of action, allowing the commander to capitalize on an information advantage and influence the environment or the adversary. Today's battlespace can be characterized by smaller, technology-enabled military forces; near-peer or agile unconventional adversaries; interorganizational and multinational relationships; and a fast-moving

global information environment. Various factors contribute to an increasingly dynamic, complex, and interrelated arena in which Marines must operate, which requires adjustments in IKM TTP to provide necessary operational agility.

Information and Knowledge Management Pillars

Conceptually, IKM provides the right information to the right people at the right time, in the right format, and right classification for situational awareness and decision making. It consists of three mutually supporting pillars: people, process, and technology. People (users and data processors) are the ultimate consumers of information and the priority of IKM attention; they provide expectation, policy, and guidance for the end product. Process (procedures and policy) is the implementation of best practices that integrate the three pillars, provide efficiency, and eliminate duplication for an effective information flow according to the operational requirement. Technology (hardware and software) is the physical network and systems used by people to collect and process data, enabling information and knowledge transfer to takes place among a geographically dispersed Marine air-ground task force (MAGTF). Aligning the three pillars focuses the collaboration or C2 capability (technology) for its intended effect and helps implement any necessary alternative solutions for integration shortfalls, while concurrently sustaining a learning force.

Information Environment

As discussed in MCDP 8, *Information*, the information environment is a global competitive space that spans all warfighting domains, where all operations depend on information. It includes information and relevant social, cultural, psychological, technical, and physical factors that can affect the employment of forces and influence the commanders' decision making. Information serves a vital role in every activity that Marines undertake. It is fundamental to intelligence, command and control, situational understanding, decision making, and all forms of behavior. The information environment can be a source of exploitable advantage and a potential source of disadvantage to overcome. The information group, who serves as the purveyor of the information warfighting function, synthesizes and synchronizes information in this environment using IKM. However, IKM distinguishes itself from the information environment, because it serves an entire command, supporting staff action across all warfighting and staff functions. Refer to Chapter 3 for additional information.

Evolution of Technology

The evolution of information technology has exponentially increased the complexity and quantity of data that must be viewed, sorted, collated, disseminated, and managed by military

forces. Operational-level headquarters can no longer rely solely on the electronic correspondence (referred to as e-mail) to understand, visualize, plan, and direct operations. Organizations that do not adapt to technological advances can become overwhelmed or distracted, losing their ability to maintain relevant situational awareness and make timely and informed decisions.

To compensate for modern warfare realities, commanders and their staffs gain battlespace perspective from situation maps, text documents (e.g., messages, reports, status boards), and voice reports. The situation map and text information, combined with the commander's experience, intuitive reasoning, judgment, and personal contact with front-line units, enables the commander to attain a level of understanding necessary to make informed decisions. Contending with the complexity characterized by conflict in the 21st century, warfighters need integrated systems, along with structured policy and guidance. Direction should be combined with procedures that collect, process, and safeguard data and thereby facilitate efficient knowledge generation, assimilation, sharing, and collaboration. The aggregate of people, processes, and technology must provide shared situational awareness and decision support across distributed networks in dynamic and chaotic arenas.

Warfighter Impact

Information and knowledge management enable operational functions and organizational learning to improve mission performance across the Marine Corps. Marine Corps Order 5400.52, *Department of the Navy Deputy Chief Information Officer Marine Corps Roles, and Responsibilities*, recognizes the inherent relationship between information and knowledge, which is integral to the information warfighting function (for additional information refer to Chapter 2). The Deputy Commandant for Information, through the Service Data Office, provides direction and oversight to the IKM functional area. Advancing technology has changed the way the Marine Corps leverages its IKM and C2 applications to synergize the operational environment. Timely, quality information provides required situational awareness to commanders and adds value to the decision-making process—both of which impact mission accomplishment. The management of the flow and access to this information is critical. Information and knowledge management helps commanders to effectively focus people, processes, and technology to meet challenges and leverage fleeting opportunities.

Information is a valuable commodity, bringing with it an added dimension of both situational context and technical complexity. Knowledge provides value and competitive advantage that can create increased tempo, improved operational performance, and decisive action.

Chapter 2.
Information and Knowledge Management Terms and Constructs

Information Management Definition

Information management is, "the function of managing an organization's information resources for the handling of data and information acquired by one or many different systems, individuals, and organizations" (*Department of Defense Dictionary of Military and Associated Terms*, hereafter referred to as the, *DoD Dictionary*).

Information management—

- Is the sum of the processes for collaborating and sharing information.
- Enables commanders to formulate and analyze courses of action, make decisions, execute those decisions and adjust plans accordingly.
- Is a commodity. More than control of data flowing across technical networks, it covers the entire lifespan of information, with a focus on commanders and their information requirements.

Information and Knowledge Management Principles

Information management principles are as follows:

- Information management is a C2 enabler that allows commanders to effectively convey guidance and direction to their staffs. Unfocused information management is just a process refinement with no direction. Commander influence is essential.
- Effective information management must be a deliberate and proactive effort driven by commanders to align the actions of people, enabled by technology, to support the timely development of a common understanding of the environment.
- Information management contributes to better analyzed and formulated recommended courses of action, providing information for decision making and execution as well as feedback and assessment on actions.
- Information management is more than the sum of its three pillars and involves procedural improvements to incorporate technology and personnel requirements.
- Achieving common understanding requires refining information using people, technology, and processes enabled by improved collaboration, concurrent planning, and focused execution.
- To be effective, decision makers must have the mental agility to render accurate decisions in recognition of existing social and political systems, customs, and norms.

Knowledge Management Definition

Knowledge management is "the integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance" (*Marine Corps Supplement to the DoD Dictionary of Military and Associated Terms,* hereafter referred to as the *USMC Dictionary*). It is focused on managing what the commander needs to know, facilitating knowledge and information flows within and across organizations, and ensuring the information products are appropriately sequenced and available to build shared situational awareness and common understanding of the commander's intent.

Knowledge Management Principles

The following are widely accepted knowledge management principles (see International Organization for Standardization 30401, *Knowledge Management Systems-Requirements*):

- Knowledge is intangible, complex, and discoverable.
- Knowledge is a valuable and key asset for organizations.
- Knowledge management serves organizational objectives, strategies, and needs.
- Knowledge management is adaptive. There is no single knowledge management solution that fits all organizations within all contexts.
- People create their own knowledge through shared understanding of what they receive. For shared understanding, knowledge management should include interactions between people using applicable content, processes, and technologies.
- Knowledge management focuses on managing the working environment, thus nurturing the knowledge lifecycle.
- Understanding culture is a critical aspect to the effectiveness of knowledge management.
- Knowledge management is iterative. It should be phased, incorporating learning and feedback cycles.

Information Management Supports Decision Making

Decision making is one key indicator of organizational capability. Organizational decision making depends on several resources integrated to generate the conditions that enable optimal decisions. Information management is both a critical resource and an integral component of decisions, and, in today's information-rich environment, the management of information resources can enhance decision making.

Organizational effectiveness can be measured in terms of goal accomplishment, competitive advantage, and efficiency, which heavily depend on decision making. The number of decisions made across the force span the spectrum, from routine to strategic, is nearly impossible to count. Marine Corps, Navy, and civilian leaders pride themselves on their ability to swiftly analyze a situation and decide, despite facing myriad decision-making challenges.

The following challenges constitute the problem:

- Varied approaches.
- Missing or incomplete data.
- Mission scope creep.
- Multi-tasked leaders with limited engagement capability.
- Poor communication.
- Geographic and time separation.
- Multiple stakeholders.
- Competition for limited resources.

When uninformed decisions are made, the deciding organization is ill-equipped to enable follow-on analysis to achieve intent or effectiveness.

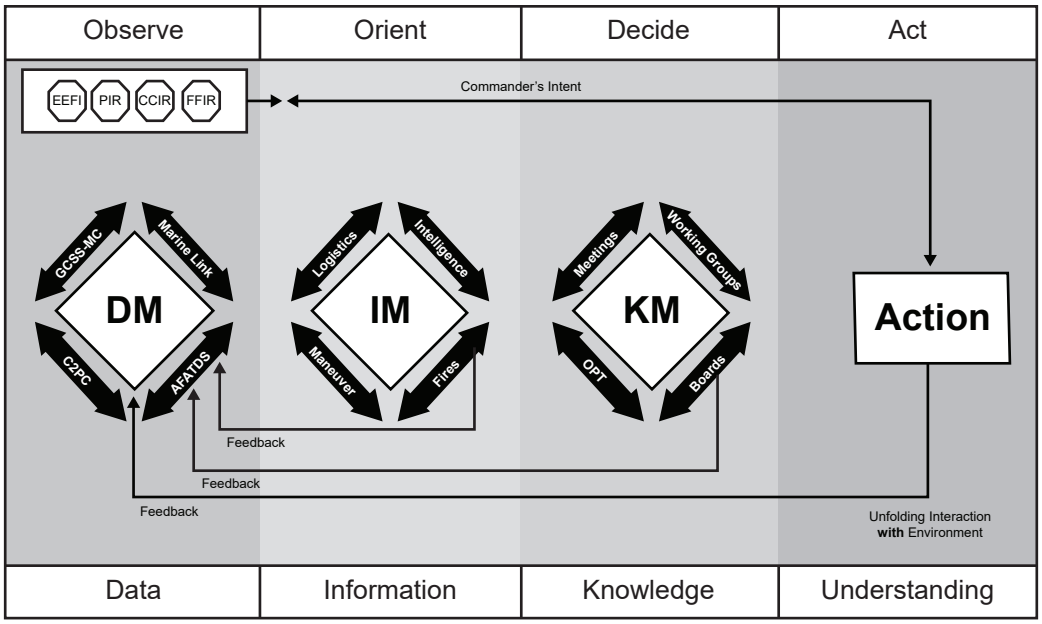
Value Proposition

Augmenting the decision maker with effective information management, analytical, and empirical substance necessary for critical leadership decisions, increases knowledge, confidence, and speed of decision making within the organization. Leaders possessing reliable, valid, and descriptive qualitative information and quantitative data are able to enact organizational changes more effectively, thereby reducing organizational inefficiencies, dead time or missed opportunities. Improved decision making improves organizational effectiveness.

Knowledge Management Supports Organizational Performance

Figure 2-1 depicts the IKM concept of transforming data to a commander's decision through the lens of a cycle known as observe, orient, decide, act (OODA) loop. Using C2 systems technology, this process provides data, which people contextualize into information, and cross-functional processes that help transform the collective information into knowledge for action; feedback loops continually update and improve the cycle.

By applying IKM principles throughout the planning, decision, execution, and assessment cycle, commanders and staffs gain a more refined understanding of the elements of a dynamic battlespace faster. As stated in MCDP 6, "there are two basic uses for information. The first is to help create situational awareness as the basis for a decision. The second is to direct and coordinate actions in the execution of a decision." Simply put, information is critical to the decision-making process and the success of campaigns, operations, and tactical actions.



LEGEND

AFATDS	Advanced Field Artillery Tactical Data System	**GCSS-MC**	Global Combat Support System-Marine Corps
C2PC	command and control personal computer	**IM**	information management
CCIR	commander's critical information requirement	**KM**	knowledge management
DM	data management	**OPT**	operational planning team
EEFI	essential elements of friendly information	**PIR**	priority intelligence requirement
FFIR	friendly force information requirement		

Figure 2-1. OODA Loop—Data to Decision Concept.

Knowledge Sharing

As stated in Joint Publicatoin (JP) 3-0, *Joint Operations*, "knowledge sharing complements the value of [information management] with processes to create an organizational culture that encourages and rewards knowledge and information sharing to achieve shared understanding. It supports team learning activities and a supporting environment. While information can be collected, processed, and stored as structured or unstructured content, such as in reports and databases, knowledge is acquired through a cognitive process and exists in the minds of individuals." Knowledge sharing, as it is referred to in this context, demonstrates an overlap of information management and the discipline of knowledge management. The Marine Corps information enterprise strategy calls attention to the need to institutionalize information management and knowledge management practices across the Marine Corps.

The excerpt above is consistent with what is presented in the Department of the Navy Knowledge Management Strategy. Beyond the scope of information management, knowledge management leverages the collective human, intellectual, social, and structural capitals to create knowledge-based organizations. Such organizations are aimed at accomplishing organizational goals and missions while sustaining a dynamic strategic advantage across the Marine Corps (see Figure 2-2).

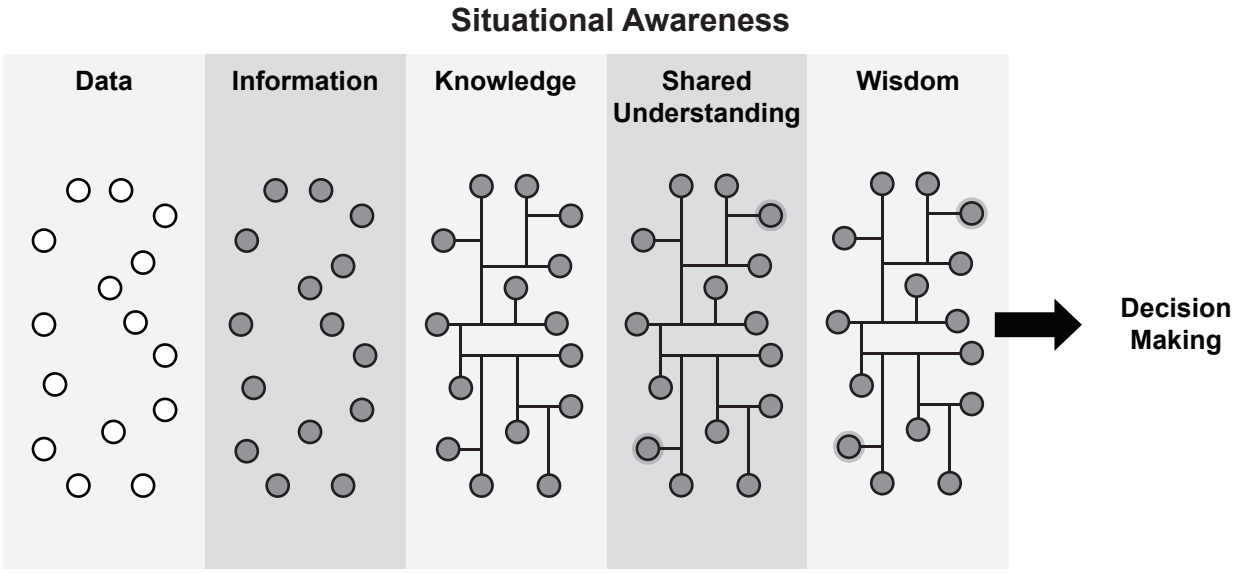


Figure 2-2. The Information and Knowledge Management Interrelationship.

THE RELATIONSHIP BETWEEN INFORMATION MANAGEMENT AND KNOWLEDGE SHARING

Information management facilitates knowledge sharing as it relates to collecting, filtering, fusing, processing, focusing, disseminating, storing, and using information, which is then internalized by the individual and fused with personal insights and experiences. In essence, information that is difficult to articulate (e.g., wisdom, insight, skillsets) combines with institutional knowledge to create a foundation for collaboration, which can lead to shared understanding. This understanding can enhance a leader's situational awareness, and thereby shape sound decision making.

Data, information, knowledge, and shared understanding, merged with the situational awareness to provide leaders the wisdom needed to produce sound decisions. Without quality information management, the exchange of knowledge would be flawed and would degrade the decision-making outcome. Figure 2-2 depicts the interrelationship between information and knowledge.

Creating Shared Understanding

Decisions are important products of the C2 function because they guide the force toward defined objectives and mission accomplishment. A platform of shared understanding consists of five major categories: data, information, knowledge, understanding, and wisdom. Each category contributes to the decision-making process (see Figure 2-3). The gradations between the categories might not always be clear, but data becomes more valuable as it is refined and focused.

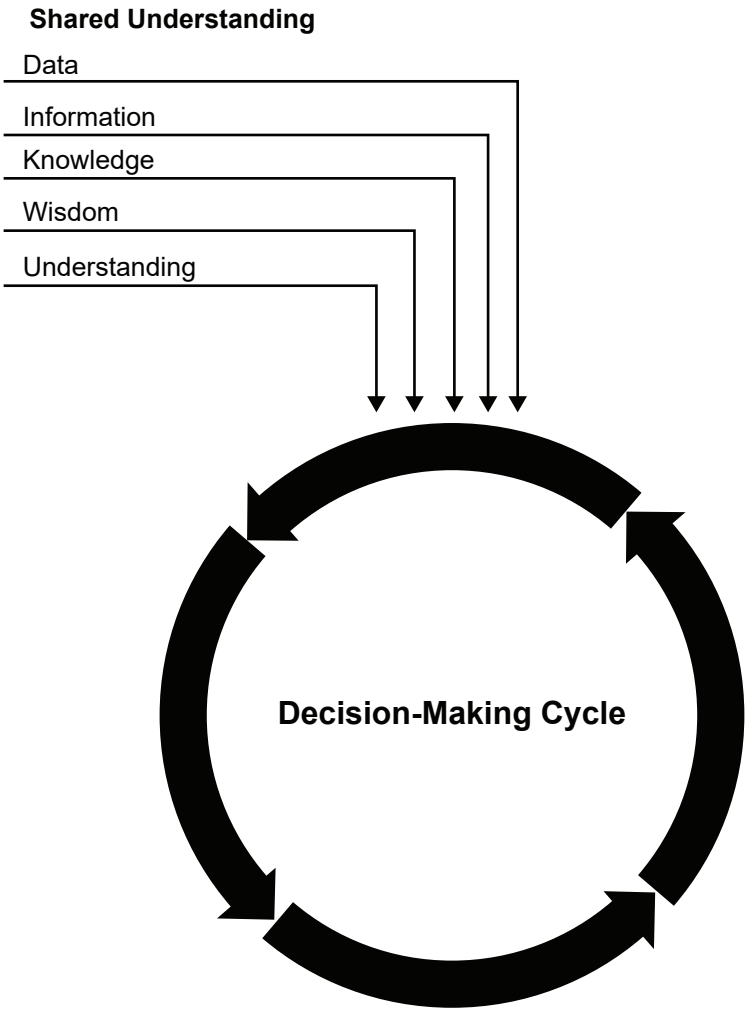


Figure 2-3. Creating Shared Understanding.

Data

Raw data was originally considered just a building block to processed information. Within the past few years, however, the Department of Defense (DoD), the Department of the Navy, and the Marine Corps have released strategies propelling data to the level of a strategic asset. With increased network speeds and common access to information, a transformation from a network-centric focus is giving way to data-centricity where the speed and scale of data increases efficiency delivering an operational advantage to the warfighter.

The *DoD Data Strategy's* emphasis in the operational space focuses on the following:

- Joint all-domain operations: using data to attain an advantage in the battlespace.
- Senior leader decision support: using data to improve DoD management.
- Business analytics: using data to drive informed decisions at all echelons.

The seven goals to become a data-centric DoD, applying the mnemonic, VAULTIS, which guides the process of making data—

- **V**isible. Consumers can locate the needed data.
- **A**ccessible. Consumers can retrieve the data.
- **U**nderstandable. Consumers can recognize the content, context, and applicability.
- **L**inked. Consumers can exploit data elements through innate relationships.
- **T**rustworthy. Consumers can be confident in all aspects of data for decision making.
- **I**nteroperable. Consumers have a common representation and comprehension of data.
- **S**ecure. Consumers know that data is protected from unauthorized use and manipulation.

Information

Information is managed to frame its value and relevance as it is refined and focused to develop the commander's knowledge, understanding, and situational awareness. Information comes from organizing, correlating, comparing, processing, and filtering raw data, and then rendering the data understandable to the potential user. Processing information can provide limited value. Processed data might have some immediate, tactical value; however, it has not generally been evaluated or analyzed to determine its long-term or operational significance.

Knowledge

Knowledge is required to—

- Exercise the human capacity (potential and actual ability) to take effective action in varied and uncertain situations.
- Understand a situation.
- Find meaning in a situation.
- Have insights into a situation.
- Create ideas related to a situation.
- Have intuition about a situation.
- Make effective judgments.
- Anticipate the consequences of actions.
- Recognize the who, what, when, where, why, and how.

Knowledge includes facts, beliefs, truths and laws, concepts, methodologies, know-how, know-why, judgments and expectations, insights, relationships, leverage points, intuition, feelings, meaning, and sense-making. Knowledge results from analyzing, integrating, and interpreting information; it provides value to an event or situation by linking and refining internalized information and data. Types of knowledge can be further defined as explicit or tacit.

Explicit Knowledge

Explicit knowledge can be called up from memory, put into words, and shared (also called declarative knowledge). Often, it is placed into standing operating procedures (SOPs), lessons learned, intelligence reports, standing orders, and contingency plans. Explicit knowledge can be organized, applied, and transferred in digital or non-digital form. It lends itself to understanding rules, limits, and other precise meanings, and allows an individual to develop and understand personal world views or mental models.

Tacit Knowledge

Tacit knowledge is the intangible understanding that exist in an individual's mind. It is formed by connections that cannot be easily put into words, such as intuition, wisdom, innate skills, etc. The implicit form of this knowledge is often pulled or triggered by memories and portrayed as our visceral reactions to certain stimuli. In the metaphysical sense, it is like an individual's ability to perform fine motor functions or even walk. All individuals have a unique store of experience gained through life, training, and education and can be impacted by formal and informal social networks. Even though tacit knowledge cannot be readily described by the individual it can be observed through role playing, mentorship, and analyzing situational outcomes. If it is documented or verbalized, tacit knowledge can shape explicit knowledge, to be shared and promoted to enhance education and training.

Humans develop tacit knowledge by internalizing explicit knowledge through practical application, feedback from experienced practitioners, and through personal reflection. One example of this technique is the OODA loop. Once observed and identified, individuals can use the OODA loop to train and practice, developing their immediate responses in given situations.

Understanding

Understanding provides knowledge context or framing. Understanding is an appreciation for not just what is happening, but more importantly, why it is happening. Understanding occurs when knowledge is combined with experience, judgment, and intuition in a collaborative environment. Collaboration and debate allow decision makers the opportunity to reduce gaps generated by uncertainty and to fully apply insights and situational awareness to form a complete mental image of the situation.

Wisdom

With understanding and clarity of the mental image, the commander can better anticipate future events and make sound decisions, even in the face of uncertainty. While data and information can be created and handled without human intervention, knowledge and understanding explicitly require human involvement. To create knowledge, an individual must participate in the process and move processed data from the physical to the cognitive realm. To create understanding, a person must integrate knowledge with judgment and experience that leads to developing wisdom. While knowledge exists at the boundary between the physical and cognitive realms, understanding exists only in the cognitive realm.

Action

Knowledge alone is insufficient. Knowledge enables action, whereas action drives performance. It is through unit performance that mission success is measured and realized, supporting a competitive advantage. Therefore, once knowledge is acquired through the data-to-decision concept, as depicted in Figure 2-1, it becomes imperative that action be taken, where knowledge and decisions deliver the critical competitive resources.

High-Quality Data, Information, and Knowledge Characteristics

Using the VAULTIS mnemonic assessment guide, data owners can categorize data sets at different levels of quality over time by considering its age, prioritization, initial condition, and other factors. Therefore, data quality dimensions are relative. A good list of factors to consider when assessing the level of quality across the data's lifecycle is described in Table 2-1.

Table 2-1. Data Characteristics.

Data Quality Factors	Descripton	
Accuracy	Data that correctly reflects proven true values or specified action, person, or entity. It includes data structure and variability. Information that conveys a true situation.	How closely does the data reflect proven true values or specified actions, people, or entities?
Completeness	The data present at a specified time containing the expected information or statistics, as measured at the data set, row, or column level. All necessary information required by the decision maker is available.	Does the data contain the expected information or statistics as measured…?
Conformity	Do the data sets follow agreed upon internal policies, standards, procedures, and architectural requirements?	
Consistency	Is the data uniformly represented within and across data sets?	
Uniqueness	Is there a one-to-one alignment between each observed event and the record that describes such an event?	
Integrity	Are the data set's provenance and lineage known and aligned with relevant business rules?	
Timeliness	Information that is available in time to make decisions.	Is there sufficient time before the event takes place for the data to be useful?

Knowledge quality refers to the relevance, accuracy, and usefulness of the knowledge. It focuses on knowledge within a repository as crucial and is often related to the content management plan. Knowledge of high quality contributes to better decision making and problem solving, ensuring that personnel have access to the same reliable and valuable knowledge.

SITUATIONAL AWARENESS

Situational awareness is "knowledge and understanding of the current situation that promotes timely, relevant, and accurate assessment of friendly, enemy, and other operations within the battlespace to facilitate decision making. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding" (*USMC Dictionary*). Situational awareness includes—

- Understanding of the physical environment.
- Comprehension of people's purposes and movements relative to their physical environment.
- The ability to anticipate the impact of future actions within the environment.

Some level of situational awareness can be attained with information, but its scope tends to improve as information is refined and processed into knowledge and understanding through refinement and focus. As situational awareness improves, commanders can better anticipate future conditions, visualize courses of action, provide guidance, and accurately assess outcomes. Developing situational awareness with limited and uncertain information under pressing time constraints is one of the fundamental C2 challenges. Two basic aspects of situational awareness are information and skill. The staff and subordinate unit commanders provide the information component and feedback. The skill component comes from the commander's personal experience, judgment, intuition, and ability to assimilate and understand the surrounding environment.

Shared Situational Awareness

In shared situational awareness, the commander conveys operational intent and assessment of a situation to distributed organizations to influence efforts of the organization and to guide the outcome of operations. Command and control must be aligned so information is readily shared and subordinate commanders receive common near-real-time information with sufficient time to respond.

Shared situational awareness impacts IKM best practices and, thereby, technology. Neither knowledge nor understanding can exist without an individual assimilating and processing information. Knowledge requires that an individual process and analyze information. Understanding requires an individual to assimilate information, elevate it to knowledge, and then apply judgment and experience to fill gaps and form a mental image. Information managers must seek to deliver information in forms that facilitate and accelerate sharing, knowledge, and understanding.

Organizational Processes

Processes are identified and derived through review and analysis of command and section mission-essential tasks (METs) and each task's associated information requirements. Once identified and documented, processes are codified in the command information knowledge management plan (IKMP). Together these processes drive a staff's action and ultimately determine how information and knowledge will flow to accomplish a section's or command's assigned mission in concert.

Processes require analysis of cross-functional sequencing and the associated steps to ensure all involved in a staff process action are performing their functional area requirements with the timeliness, accuracy, and sense of urgency required. The information knowledge management officer (IKMO) can help sections or the command deck identify and resolve bottlenecks, delays, or errors as part of a process improvement effort, which might include identifying program of record software deficiencies or limitations. Commanders, executive officers, and chiefs of staff (C/Ss) should put processes in place to ensure the unit personnel and organizational point-of-contact information remains up to date and available to higher, adjacent, and subordinate units. Permissions related to IKM should be assigned, as applicable, as part of

the check-in process with staff members being granted access to other relevant units' shared files collaborative spaces in support of developing a shared command understanding and situational awareness. Through synchronizing all processes and sequencing of events, often found in a battle rhythm and command calendar, a unit can begin to measure its level of performance. When measures of effectiveness, measures of performance and Marine Corps combat readiness evaluations combine, a full performance picture emerges.

Information and Knowledge Management Program Maturity

After a unit establishes an IKM program and incorporates decision making and organizational performance techniques, it can begin to regulate its progress, evaluating itself against the four phases of maturity in IKM. In the first phase, an organization achieves shared understanding through cross-functional communication increasing organizational identity while reducing constraints of information. In the second phase, the organization improves the decision-making cycle, reducing the need to make decisions while increasing the quality of decisions and improving their impact to the mission. In the third phase of program maturity, an organization enhances mission performance, creates efficiencies, and reduces waste of resources. In the fourth phase, an organization becomes agile by continuously evolving through collaboration, implementation of timely solutions, application of feedback, and progression.

Summary

Decisions drive organizations, and organizational decision-making capability is determined by many factors. One such factor an organization's ability to manage its processes for finding, accumulating, filtering, analyzing, and reporting information to the decision maker at the optimal time. Information management is a key to knowledge management, and critical to both is the contextualization of transactional and analytical data sources. Information management technology continues to evolve as illustrated by the latest advances in designing advanced data warehouses, developing, and employing business intelligence strategies, and venturing into the use of artificial intelligence.

Chapter 3.
Information and Knowledge Management Personnel and Duties

People comprise the second element of command and control and the most crucial pillar of IKM. The people push and pull information and leverage collaboration tools that ultimately enable commanders to access high-quality information for timely decision making. Information and knowledge management exists to improve information flow by using technology to better integrate people and processes. Consequently, if commanders are responsible for C2 systems and IKM processes, then they must understand command and control and collaborative systems, the impact C2 systems have on information flow, and the roles and responsibilities people have for producing essential information products. Technical and operational responsibilities must be properly aligned and coordinated for timely content refinement, production, delivery, and consumption. Defining the duties of key personnel establishes their relationship to IKM functions and highlights their contribution to effective information flow.

Although certain individuals are labeled as key personnel with specific IKM-related duties, every member of a command has an inherent responsibility to assist with the functions of collecting, managing, filtering, fusing, disseminating, protecting, and storing information. To accomplish the IKM mission, in a personnel-constrained environment, the command's personnel serves multiple roles and provides expertise to numerous functional areas such as boards, centers, cells, working groups and staffs. Information users must align with mainline IKM procedures to enhance the flow of information and the generation of knowledge and understanding. An organizational chart, battle roster, operational battle rhythm, C2 system diagram, and list of information exchange requirements (IERs) are products typically developed to enable alignment for operational effectiveness. Detailed C2 planning includes the process of highlighting individual responsibilities (see Figure 3-1) and provides the relationships between information managers and key command and battle staff personnel. The C2 diagram depicts the critical need for the coordination of people, processes, and technology to support and integrate battlespace awareness, mission readiness, and command decision making.

The IKMO, typically working for the C/S or executive officer (XO) at lower echelons, develops and refines the processes and procedures necessary to harness information for the command and guide daily staff actions (see Figure 3-2). The IKMO works with staff section knowledge management representatives to understand, facilitate, and improve information flow. Critical to the IKM processes and procedures is the underlying communication architecture and hardware, which is provided by the G-6/S-6.

Relative levels of effort are reflected in Figure 3-3. Although key personnel with specific IKM duties are important, all information users have a duty to facilitate information management and support knowledge-based decision making.

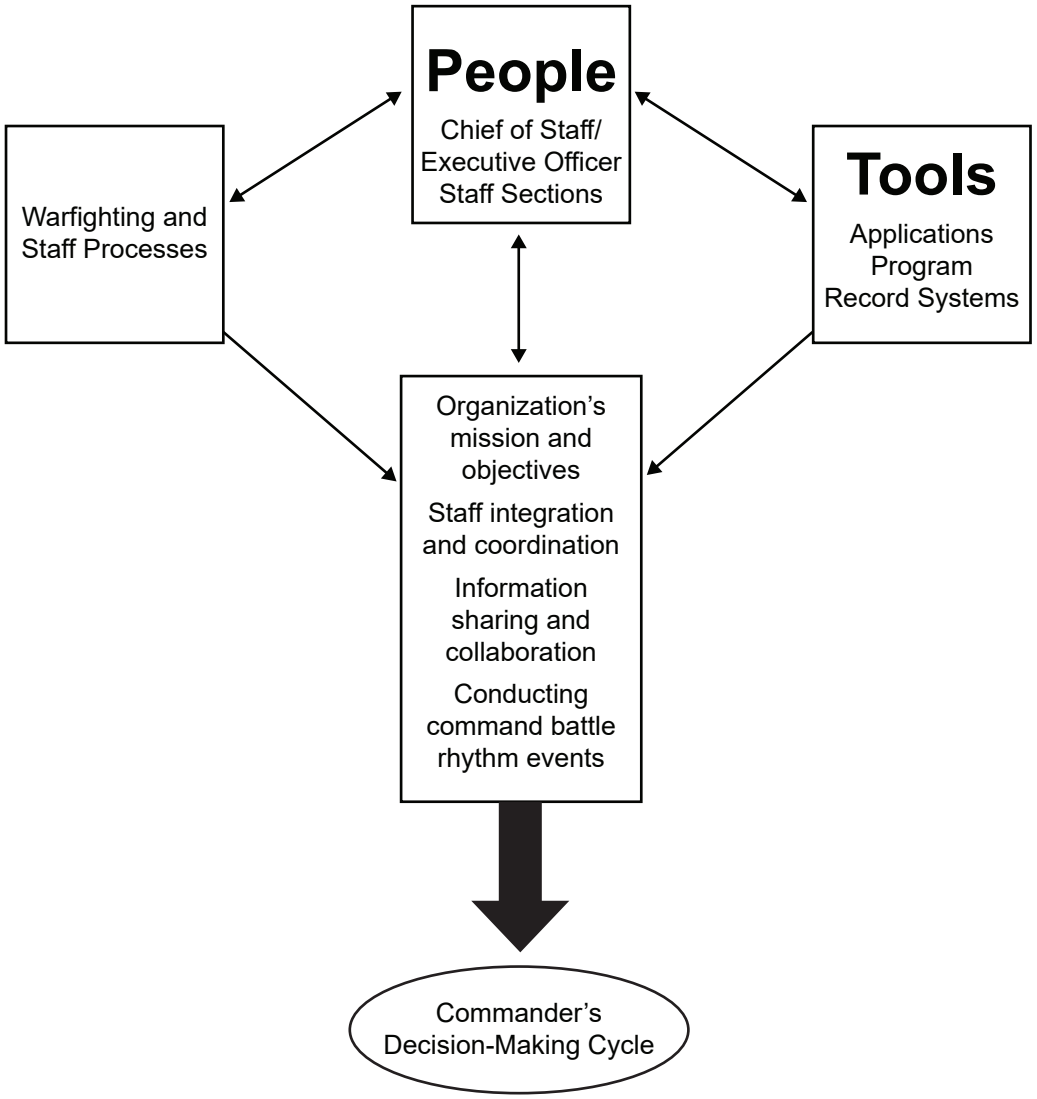


Figure 3-1. People, Processes, and Technology in Support of Commander's Decision Making.

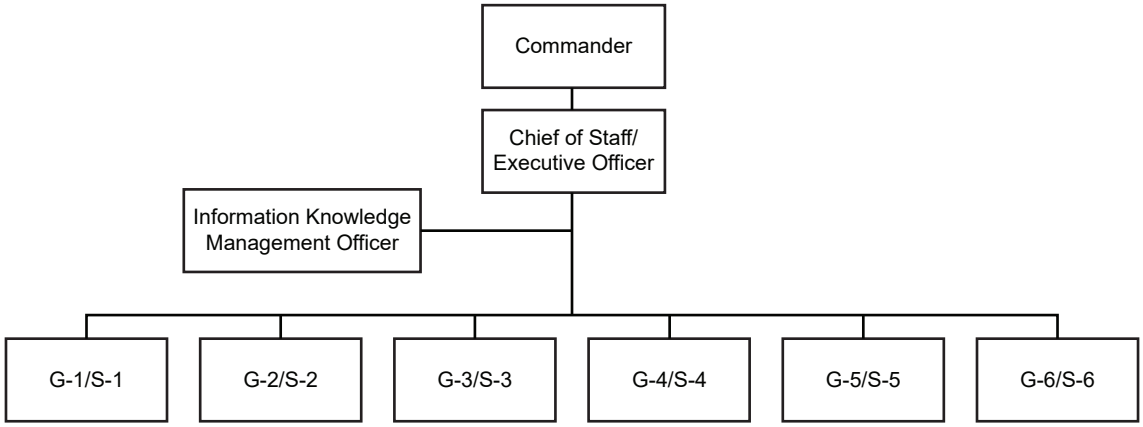


Figure 3-2. Staff Organizational Chart.

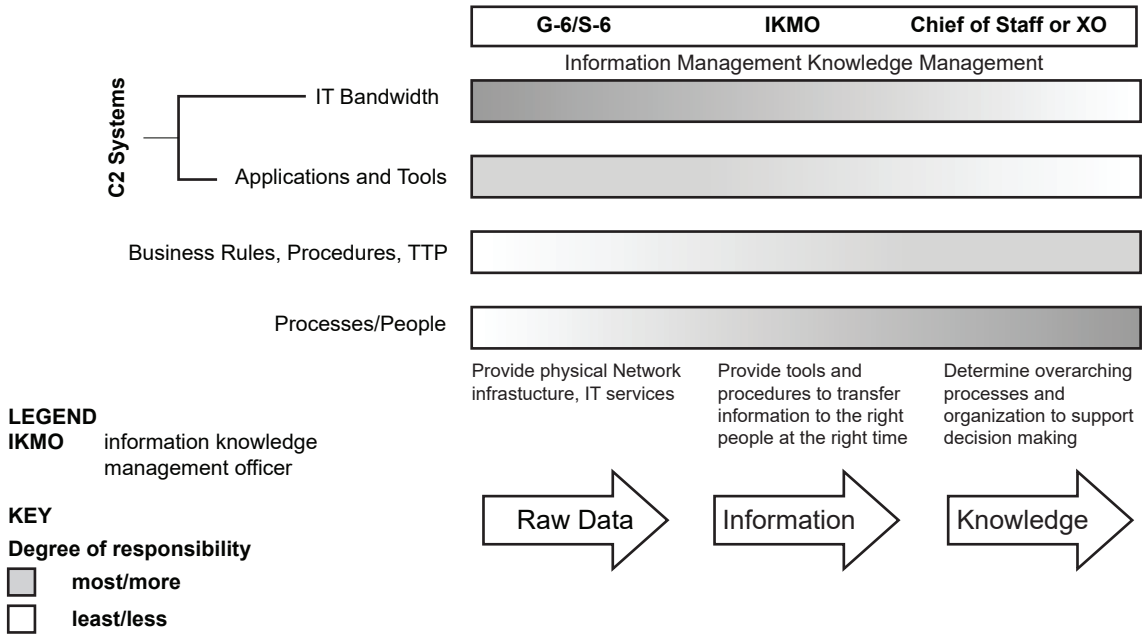


Figure 3-3. Levels of Responsibility.

Key Information and Knowledge Management Personnel

Commander

The commander aligns command priorities and drives the planning process. The commander's intent and guidance are foundational elements to planning and execution. The commander uses the Marine Corps Planning Process to gain understanding and situational awareness to support decision making, establishing priorities for gathering and reporting information. Clear guidance, commander's intent, and commander's critical information requirements (CCIRs) enable the staff to focus on identifying information used to support and make key decisions. The commander—

- Sets expectations for staff and subordinate command's knowledge and information needs,including defining acceptable shared situational awareness.
- Provides commander's guidance for information management.
- Approves the command IKMP.
- Approves the command communications plan that complements and supports the IKMP.
- Develops and approves CCIRs.

Chief of Staff or Executive Officer

The C/S or XO is responsible for coordinating staff actions and ensuring the commander has the necessary information and knowledge to make informed decisions. As the principal supervisor of staff processes, the C/S or XO is uniquely positioned to view and influence the process that binds the staff into a cohesive and productive organization.

The C/S or XO—

- Appoints and supervises the IKMO.
- Implements the IKMP by providing the mechanisms to coordinate the staff.
- Directs development of, approves, and owns the battle rhythm.
- Appoints and assigns event facilitators and responsibilities to functional areas and working groups.
- Ensures IKM processes yield the quality and actionable information needed to support the commander's decision-making cycle.
- Ensures information is properly classified and that steps are in place to protect sensitive information.

Principal and Special Staff

Principal staff members serve as the eyes and ears of the commander. The staff receives the commander's guidance, intent, priorities, and CCIRs. The staff uses this input to collect, filter, analyze and transform data into focused and contextualized information, knowledge, and understanding for the commander. Principal staff members—

- Appoint a staff knowledge management representative (KMR as a point of contact for IKM matters).
- Appoint personnel responsible for maintaining section specific information technology and network infrastructure used to share quality information.
- Appoint site managers and alternate site managers to manage the section's portion of the MAGTF collaborative environment (workspace, chat, web conferencing).
- Identify pertinent information and activities used to support the organization's battle rhythm.
- Establish internal staff section procedures with concurrence from the IKMO to share high-quality information through the use of appropriate technologies, requests for information, and suspense control measures.
- Ensure basic IKM training is completed for appropriate personnel in each staff section.
- Evaluate IKM procedures to assure efficient flow of quality information.
- Establish benchmarks and subjective analysis to evaluate efficiency and effectiveness of IKM processes in support of knowledge-based decision making.
- Work closely with the IKMO to develop architectures that identify functional tools, applications, procedures, and processes required to share quality information with those who need it in a format that is clearly understood.
- At times, might be called to work in a coalition and joint environment where the flow of information is from different sources.

Information Knowledge Management Officer

The IKMO works closely with personnel within the command and in joint, coalition, or multinational environments to develop and coordinate procedures necessary to share information. The IKMO facilitates the flow of information, synchronizing C2 technologies and battlespace technologies through the IKMP. Information management processes and procedures must promote development and exchange of information required by the commander, staff, and unit personnel to make informed decisions consistent with the commander's intent.

The IKMO must be aware of—

- Key decisions the commander is expected to make in pursuit of desired results.
- Such decisions are typically reflected in CCIRs and the decision support matrix (DSM).
- Information required to set conditions for tactical operations, maintain commander situational awareness, and daily reporting.
- Information that the commander requires to reduce uncertainty about the friendly force, the enemy, and the environment. Information must be effectively provided in a format, rhythm, and context to facilitate making sound, timely decisions to satisfy CCIRs.

The IKMO performs the following IKM tasks:

- Develop and publish the command IKMP and corresponding IKM annex or appendix to operation orders (OPORDs) or plans.
- Determine IERs that impact networks, systems, and applications required to plan for and integrate collaborative and C2 systems.
- Publish the command reports matrix to the collaborative workspace.
- Develop the battle rhythm and support and facilitate functional area execution.
- Coordinate additional training required by staff and component elements to support production of high-quality information and delivery of knowledge through effective IKM procedures.
- Ensure effective information exchange throughout MAGTF.
- Work closely with staff principles, staff section KMRs, and subordinate and higher headquarters (HHQ) IKMOs to ensure IKM procedures and processes are published and understood.
- Recommend information flow improvements and enhancements to the C/S or XO for evaluation and possible implementation.
- Prepare and coordinate plans for changes to established IKM processes and procedures.
- Determine metadata requirements to allow for high-quality enterprise search for information.
- Support continuous process improvement within the command.

Staff Section Knowledge Management Representatives

The staff section KMR facilitates IKM procedures and must be aware of what information and knowledge is required by the commander, when it is required, and how it should be formatted. The staff section KMR is typically a collateral responsibility. The KMR is expected to—

- Monitor the information flows and processes to, from, and within the respective staff sections.
- Ensure the command IKMO is aware of information produced by each staff section to satisfy CCIRs.
- Provide routine daily updates that the commander requires to make informed, timely decisions.
- Provide the G-6 or S-6 daily updates of command-level information development and share requirements that might require network infrastructure and equipment to support functional needs.
- Ensure compliance with IKM procedures used to share information on electronic correspondence, chat, data storage and access, and other network capabilities.
- Coordinate and conduct IKM training for internal staff section members.
- Conduct internal self-assessments.

The knowledge management representative—

- Lists the IKM policies and procedures within the department (if none, state none on hand), lists the warfighting and staff processes and establishes flow charts for each process, and ensures regular attendance as the functional area KMR.
- Evaluates processes, focusing on optimizing internal processes, leveraging technology and automation in efforts to streamline completion of department tasks, creating knowledge, distributing high-quality information generated by the department and responding to the commander's information requirements for decision making. Works with the command IKMO to document all department processes and develop automated and electronic solutions where practical.
- Represents the department and staff function at IKM functional areas and working groups, which primarily focuses on the command information and knowledge management working group (IKMWG). Knowledge management representatives form the majority of the IKMWG membership and provide unique insight and contributions in resolving the IKM and C2 issues within the command. Furthermore, the KMR's presence allows for the introduction of department or functional IKM matters, which can compete for resources when approved by the information management board that is chaired by the C/S or XO. In all cases, KMRs back brief the IKMWG and functional areas and working group activities and actions to department leadership, fostering effective communication and a well-coordinated staff.
- Identifies the department's collaborative environment manager. A collaborative environment manager stores knowledge generated by the department to satisfy commander's information requirements (planning, decide, execute, assess). This manager also ensures department knowledge complies with the command information management plan and knowledge is organized and readily accessible to members of the department staff and across the command. The collaborative manger identifies shortcomings or complex requirements to the command IKMO requesting assistance.
- Supervises department's collaborative workspace site manager . The site manager is the technical point of contact for the department's collaborative workspace page(s). Reports to the KMR. The site manager is formally trained and an experienced member of the department, who manages access to unique or "need-to-know" content. The site manager oversees and approves each page layout and design; and assists department staff by explaining collaborative workspace application functions, and how to best harness the application's "out-of-the-box" capabilities. Formal training for the site manager is required by NAVMC 3500.54F, *Command and Control Training and Readiness Manual*.
- Identifies the C2 systems officer for the department and lists all programs of record systems and applications aligned to the staff functional area. The KMR supervises and coordinates the planning, installing, operating, maintaining, and reporting availability of function's C2 systems in accordance with architecture, essential to support assigned battlespace function, decision making, situational awareness, common operating picture. The KMR also interfaces with the Marine Corps functional area manager for function's systems to both report issues and understand future plans for function's C2 systems portfolio in accordance with Marine Corps Order 5230.21.
- Identifies the department data manager or data steward and the last time data audits occurred in assigned program of record systems. The KMR conducts samplings to verify accuracy of data contained in assigned C2 systems; report discrepancies to commands, or in the case of

database discrepancies to the functional area manager, as required. The KMR also ensures authoritative data sources retain highest level of quality. In cases of numerous systems, data chiefs can be assigned to single systems and report to the KMR, as required.

Self-Assessment Checklist

The KMR can evaluate the health of functional area IKM by answering the following questions:

- Does the primary staff section have an assigned KMR?
- Is a functional area knowledge mangement (KM) program established and documented within the section?
- Are METs and supporting information requirements maintained within either the primary staff section or as presented in the command IKMP?
- Do section system operators possess required qualifications to operate priority functional area systems or are currently scheduled for system training?
- Does the section incorporate collaborative services within the daily routines on the Nonclassified Internet Protocol Router Network (NIPRNET) or SECRET Internet Protocol Router Network (SIPRNET)?
- Has the staff section KMR completed an internal assessment within the last twelve months, and is a copy on hand?

Reports Manager

At the MAGTF level, numerous significant command and functional area reports are generated to inform the joint task force (JTF), the combatant command; Headquarters, Marine Corps; etc. Proper accounting and timely submission of reports conducted daily, which includes the situation report and intel report. Accounting and access to these reports is handled by a reports officer assigned to the operations section. The IKMO, specifically the collaborative services manager, works with the reports manager to create page and web content to facilitate their duties and serves as a reference for quick access to existing command reports. For example, the reports page can be a table linked to the operation landing page, which consists of the following data elements:

- Report name, title.
- Due date and time NLT [no later than].
- Last report submitted date and time.
- Unit point of contact.
- Transmission Type.
- Tactical phone number.

Request for Information Manager

Requests for information (RFIs) are questions that cannot be satisfied by organic staff personnel. They are consolidated among the staff and forwarded to HHQ. The RFIs are staff to staff interactions designed to facilitate an explicit response, usually within an agreed upon time frame. Responses to RFIs are shared with the requestor and staff to promote the understanding required to support the commander and to reduce uncertainty within the command.

Requests-for-information managers—

- Receive, validate, prioritize, and submit RFIs to the appropriate authority for resolution.
- Develop and manage RFI tracking systems to ensure RFIs are processed and responses are expeditiously disseminated to the requester and made accessible to all personnel.

Common Tactical Picture Manager

The common tactical picture (CTP) manager is responsible for reporting and displaying situational awareness information, including friendly and enemy unit tracks. An accurate, integrated tactical or operational picture is valuable in that it displays near-real time unit location, intelligence, and operational information using a standard symbol set. A properly managed CTP provides a visual depiction or model of the operational environment, allowing commanders to proactively assess and control the subordinate actions for a predictable outcome. The CTP is crucial to the concept of shared situational awareness. The CTP manager is responsible for—

- Understanding and following the combatant commander's common operational picture (COP) reporting and management guidance and policy.
- Coordinating and deconflicting all tracks from all sources with all major subordinate commands (MSCs) and HHQ using joint standard automated data formats.
- Working closely with the senior watch officer (SWO) and relevant picture providers to ensure the location and disposition of friendly and enemy ground units is visually updated as required.
- Emphasizing the proper use and deconfliction of automated position location information data.

Collaborative Services Manager

The collaborative services manager is responsible for all facets of the collaborative services environment, enabling inter- and intra-command information flow, supporting the MAGTF staff's information exchange and flow irrespective of bandwidth limitations at lower echelons. The collaborative services manager—

- Establishes, configures, and maintains the collaborative services environment, which includes collaborative workspace, chat services, and conferencing on all assigned networks.
- Provides for the staff's information exchange, to include an operationalized workspace, RFI, reports matrix and other operation-related workspaces.
- Implements and maintains performance metrics relating to collaborative workspaces, chatroom usage, web-conferencing utilization, content management, and conducting performance audits.
- Establishes and maintains data management policies and procedures.

Collaborative Services Manager Duties in the Collaborative Workspace

Internet and intranets are valuable resources used to share high-quality information internal and external to the staff. Creating and maintaining a unit collaborative workspace is the responsibility of the collaborative services manager.

Specifically, in the collaborative workspace, the collaborative services manager—

- Serves as the hub manager for MAGTF or MSC internet sites. Unit IKMOs ensure the role of hub manager is filled, where applicable. The hub manager is placed within the site collection administrator, who have full control of all sites in their respective hubs.
- Creates command portals or site collections to support information sharing. The portal should support internal and external reporting requirements, and ability to perform recurring tasks within the workspace.
- Communicates the locations of CCIRs, RFIs, reports matrix, the commander's daily brief, and current battle rhythm.
- Maintains workspaces across all assigned networks to ensure changes to information requirements are posted in a timely manner and ensures information contained therein is available to appropriate personnel.
- Maintains user access to portals and information in deployed environments.
- Ensures procedures are developed, disseminated, and understood for access, information upload, updates, and changes.
- Advises and assists staff section site managers, develops formatting standards, creates initial pages for each staff section, and provides training to help maintain uniformity of design between sections.
- Maintains links to external workspaces or sites of interest to the staff.
- Supports the development and timely release of custom web parts as required.

Collaborative Services Manager Duties in Chat

Chat is mainly designed for group communication in discussion forums, which is called channels. It also allows one-to-one communication via private message, as well as, data transfer, and file sharing. A chat guard chart, similar to a radio guard chart, serves as an effective tool to align chat rooms with the agencies that are involved in creating, controlling, sending, and responding to traffic with a specific chat room, while guiding chat users to the appropriate channel. Chatrooms facilitate information and knowledge transfer between mobile forward elements. The IKMWG discusses chat applications and protocol. The collaborative services manager's duties for chat services include—

- Coordinating and collecting chat room requirements from across the MAGTF during IKM planning and IER development.
- Following an IER analysis, determining the chatroom application(s) to support MAGTF operations with full consideration given to all mission partners.
- Drafting and staffing the chatroom guard chart for inclusion in Annex U.

Collaborative Services Manager Duties in Web Conferencing

Web-conferencing allows information users the ability to share desktops, documents, whiteboard, text chat, polling and voting, record, and playback sessions, along with voice and camera access. Website conferencing applications depend on the mission partners and the network being used. However, deployed bandwidth places limitations on the number of secure video teleconferencing suites available. Consequently, web conferencing becomes a viable alternative for conducting battle rhythm events, operational planning, event coordination, and update briefs with dispersed units.

The collaborative services manager provides web conferencing capabilities by completing the following:

- Determines the appropriate and approved web-conferencing application during IKM planning.
- Builds out the physical or virtual server, when required.
- Creates and configures the conference rooms aligned to battle rhythm events and other command directed web-conferencing requirements.
- Assist user access and placement of hot buttons for rapid battle rhythm event access.
- Monitors usage and extracts associated metrics pertaining to web-conferencing bandwidth utilization (overall and by event), total event attendees, total number of users, etc.
- Enables limitations on website conference room access or bandwidth restrictions, when directed.

Staff Section Site Managers

Site managers and alternate site managers are required by all staff sections and the command deck for managing the content for the sections and sharing it across the MAGTF as required. All site managers must complete training and certification at the MAGTF Information Systems Training Center (MISTC) or at a location approved by the collaborative services manager. Services managers are appointed by site owners (referred to as site administrators). They are trained and are considered the command's subject matter expert for the unit and section's NIPRNET and SIPRNET collaborative workspaces. Site managers—

- Complete certification and attend quarterly workshops and annual training.
- Ensure sites are properly formatted according to Marine Corps and local policy.
- Add and remove content managers in groups as needed.
- Ensure all posted content complies with guidance.
- Maintain copies of the site manager's training certification and appointment letters.
- Provide local training to their assigned section.
- Provide fellow Marines assistance to their assigned section.
- Report significant issues to the hub manager or MAGTF collaborative services manager.

Information and Knowledge Management Service Desk Manager

The IKM service desk manager serves as the primary point of contact within the discipline of IKM, establishing a single method to communicate needs of the MAGTF staff and IKM staff. The IKM staff and manager's goal is to satisfy both MAGTF and MSC staff objectives in delivering IKM and C2 solutions, which improve staff action and decision making. The IKM service desk manager coordinates with the G6 help desk, focusing on issues with information processes, shared situational awareness, and collaboration.

Information and Knowledge Management Coordination

To ensure IKM procedures comply with procedures established by a JTF, IKM functional areas and working groups are recommended at the MAGTF and component levels. The functional areas can also be established at lower levels of command and are convened to facilitate coordination among users, service providers, and technology maintainers as required. A board, bureau, center, cell, or working group can also be activated at the JTF to enable IKM procedures at the component level.

Information and Knowledge Management Working Group

The IKMWG is the initiating point for IKM issues within the command. In a battle rhythm, the IKMWG convenes upon initiation of staff planning and is required through the duration of the information management lifecycle (IMLC) of an operation. The IKMWG, chaired by the command or MAGTF IKMO, is composed of the senior IKMO from each MSC, mission partner, and KMRs from appropriate staff sections. The IKMWG is actively involved in completing the IKM planning process, constructing Annex U, and ensuring the information architecture supports knowledge exchange among higher adjacent and subordinate commands. Personnel who administer information exchange technologies or program of record systems (i.e., G-3/S-3, G-4/S-4, G-6/S-6) also attend. At a minimum, outputs from the IKMWG provide inputs to the IKM board, and higher headquarters IKMWG as part of the battle rhythm.

Information and Knowledge Management Board

The IKM board is the focal point for coordinating IKM issues within the command and its elements. It is part of the battle rhythm and operates under the supervision of the C/S or XO or the appropriate staff directorate to meet the commander's mission needs. Facilitated by the command IKMO, the board is composed of the senior representatives from each MSC, their IKMOs, and staff principals with IKMO representatives from appropriate MAGTF command element staff sections. The IKM board addresses cross functional and contentious IKM issues and proposes possible solutions.

Common Tactical Picture Board

The CTP board acts as the focal point for coordinating the CTP within the command. It is convened by the CTP manager, who works with the IKMO, the primary battle staff, and subordinate and HHQ IKMOs to develop CTP procedures to maintain a near-real-time picture of friendly and enemy forces. The CTP board operates closely with appropriate staff sections, IKMO, combat operations center (COC), and combat intelligence center watch officers. It is composed of friendly air, land, maritime, and enemy force track managers and is actively involved in resolving all cross-functional CTP issues. All personnel must take appropriate actions to safeguard information.

Information Security Personnel

While the personnel filling the billets of foreign disclosure officer, information security manager, special security officer, information assurance manager, information assurance officer, and operations security officer do not work for the IKMO, they are integral to the command's management and security of its information and information systems. In some cases, the IKMO appoints or assigns personnel to coordinate with information security personnel and the G-6/S-6 on information security issues.

Foreign Disclosure Officer

Military information is a national security asset that must be protected. Sharing information with foreign representatives within a coalition environment is complex and further complicated by national and international laws, treaties, and alliances. Only designated foreign disclosure officers can approve the disclosure of classified military information and controlled unclassified information to foreign representatives.

Information Security Manager

The information security manager is responsible for the proper accountability, control, personnel access, and physical security and storage of non-compartmented classified data that is in both hard and soft copy forms. This includes the top-secret control officer's responsibility for the JTF top secret registry's accountability, control, and access.

Special Security Officer

The special security officer is responsible for sensitive compartmented information management, control, and access. This function is typically executed by the G-2/S-2.

Cyber Security Manager

The cyber security manager is the primary staff officer charged with computer network defense. The cyber security manager develops plans, policies, and procedures to ensure the reliability, availability, integrity, confidentiality, and protection of data and information. They also verify the authenticity and nonrepudiation of personnel accessing data and information. As a member of the G-6 staff, the cyber security manager's primary responsibilities include:

- Information assurance.
- Managing network security.
- Detecting network intrusion.
- Assessing network vulnerability.
- Assisting in the network accreditation

Information Assurance Officer

The information assurance officer is responsible for safeguarding the command information systems . This is done by conducting site surveys and accrediting systems to process classified and sensitive information. The information assurance officer also enhances the information security knowledge, skills, and abilities of the command through education and training programs.

The information assurance officer performs the following IKM functions:

- Develops and maintains a plan for site security.
- Ensures the information system is operated, used, maintained, and disposed of according to security policies and practices.
- Ensures the information system is accredited and certified if it processes sensitive information.
- Ensures users and system support personnel have the required security clearances, authorization, and need to know; are indoctrinated; and are familiar with internal security practices before access to the information system is granted.
- Enforces security policies and safeguards on all personnel having access to information systems which the information systems security officer is responsible for.

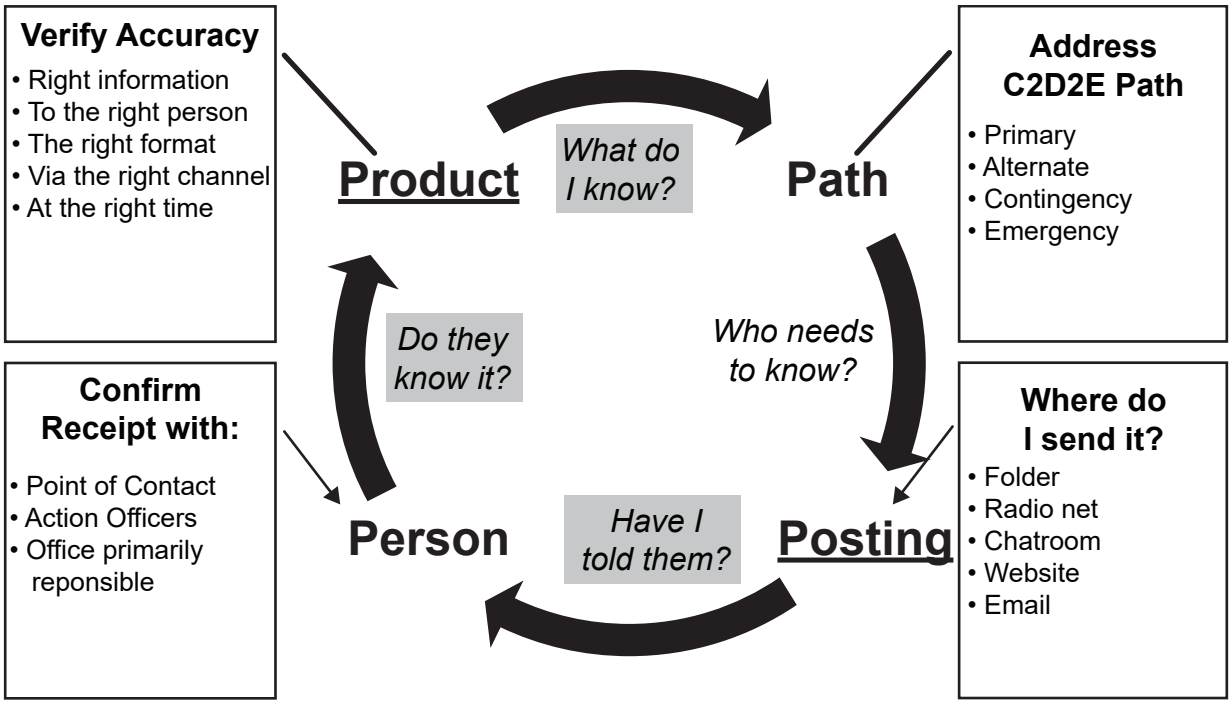
Operations Security Officer

The operations security officer is responsible for the oversight and implementation of the command operations security program, ensuring the protection against compromise of friendly force information. This position is normally a G-3/S-3 function and receives support from the G-2/S-2 (counterintelligence officer).

Information System User Responsibilities

It is incumbent upon all users of information to ensure the proper flow of information. The users' duties and responsibilities for information and information systems include the following:

- Report information as required by the command CCIR.
- Ensure accuracy and relevance of information before further dissemination. Clearly differentiate between original information and previously reported information to avoid duplicative reporting.
- Properly control, classify, protect, and archive all information and information systems for which they are responsible, maintaining a clear understanding of approved control measures for various classifications of information.
- Read and comply with the information requirements published by the IKMP.
- Properly control information throughout the entire information lifecycle, including proper disposal. When conducting an initial analysis and correlation of data, set aside but do not destroy irrelevant or conflicting data and re-introduce if it becomes useful when combined with additional facts.
- Continuously apply the "Four P's" (product, path, posting, person) of the push/pull information loop (see Figure 3-4); provide information to those that need it, when they need it, or pulling information as required. Refer to Chapter 4 for additional information on the push/pull information loop.



LEGEND
C2D2E command and control in a denied or degraded environment

Figure 3-4. The Push/Pull Information Loop.

Information and Knowledge Management Levels of Training

Every user has an inherent responsibility to filter and fuse information related to their individual duties for use by those supported. By learning proper IKM procedures, users enhance results made throughout the decision-making cycle.

Directing IKM requires an understanding of the assigned command, including its mission, organization, network architectures, hardware, software, command relationships, staff functions, and staff processes. It also requires experience in MAGTF, and joint and coalition operations. Information and knowledge management training is not just for the IKMO, but includes unit leadership, action officers, KMRs, and technical support personnel who create, validate, and disseminate the right information to the right person, at the right time, in the right format, with the right classification. This requires both collective and individual skills, not only within the MAGTF, but at the operational and strategic levels to complete assigned missions. Training opportunities exist at all levels of command and all units to best harness the benefits of sound IKM.

Tactical Information and Knowledge Management Courses

The MAGTF Information Systems Training Center provides qualification on various C2 program of record systems and unit combat operation centers. Perspective students coordinate with their unit's G-3 training officer, who enrolls the students in the Marine Corps Training Information Management System. General courses include the following:

- Operator Courses. Entry level classes designed to expose Marines to the C2 system.
- Advanced Courses. Designed for Marines who have already completed the operator level course and desire a more in-depth exposure to the C2 system.
- System administrator courses. Designed for Marines who will be responsible for maintaining a C2 system.
- Leaders Courses. Designed for the unit's staff noncommissioned officers and officers who will be operating in their unit's command operations center.
- Marine Corps Tactical Operations Group IKM Course. This course provides an overview of the IKM tools available to MCTOG personnel and IKM processes and best practices.

Operational Information Knowledge Management Courses

Operational IKM management courses include the following:

- The Afloat Knowledge Management Course. The course objective is to provide an understanding of knowledge management fundamental theory and to give context to KM in the military environment. The course provides an operational knowledge management focus on people, processes, organizations, and technology's supporting role within the constraints of afloat operations. In simple terms, the course aims to provide prospective KMOs the information and skills to run a carrier strike group or amphibious readiness group knowledge management program. The course is also useful for anyone working KM issues whether afloat or ashore. The tactical training group, Pacific teaches the course in San Diego and Virginia Beach annually and exports the course to locations, such as Yokosuka, Japan, and Fifth Fleet in Bahrain. Upon formal request, the Tactical Training Group, Pacific exports the course to other locations.
- Joint Enabling Capabilities Command Knowledge Management Practitioners Course. The course objective is to provide a solid foundation covering the major concepts, techniques, skills, and capabilities associated with knowledge management and the Joint Planning Support Element deliberate approach to knowledge management implementation in support of a joint force headquarters. The course is designed to assist commands in establishing a functionally integrated staff, with mature processes and information flows that support a shared understanding, focused on the commander's decision cycle. Attendees are introduced to the basic concepts and terminology of knowledge management as currently defined in Service and joint doctrine. The class introduces the fundamentals of knowledge management, and the skills used to achieve mission success. It is attended in person at the JECC, or unit placed on the Joint Planning Support Element support calendar following command coordination. Its detailed battle rhythm development and management sessions are its hallmark.
- Army KM Qualification Course. This course is available for Marines to attend. Taught at the graduate level, seminar style, this three-week course is held at the Army's Fort Leavenworth, Kansas location. The course is open to military grades captain to colonel, chief warrant officer 2 to chief warrant officer 5, and staff sergeant to sergeant major.

Civilians (GS-9 through GS-15) must be assigned to a knowledge management position and possess a thorough understanding of the operations process. The course is focused on Army knowledge management doctrine and principles. Students learn how knowledge management effectively enhances a unit's capability and mission command. Also, students learn how proper knowledge management facilitates shared understanding to improve organizational effectiveness. Students must demonstrate an understanding of knowledge management duties and responsibilities while maintaining a grade average of 80 percent or higher to successfully complete the course.

Industry, Academic and Information Knowledge Management-Related Courses

Additional IKM certifications and degrees are available online. Consult the local training section or base education office for course listings.

Chapter 4.
Information and Knowledge Management Processes and Procedures

Information and knowledge management processes and procedures are not solely defined by advanced technology and equipment. They are the integrated use of organizations, people, capabilities, training, doctrine, and network infrastructure to support command and control and decision making. Information and knowledge management processes combine the commander's information needs, the associated products, and C2 systems. These processes contribute to the purposeful, continuous, uninterrupted flow of information throughout the organization. Because of the proliferation of complex C2 systems and the resulting increased volume of data and information, commanders and staffs must process and manage information quite deliberately. Operational processes require staffs to consider the rhythm of the operational action, impact of technology, flow of information, and schedule of personnel involved to facilitate and coordinate command and control.

Command and Control

The alignment of technology, people, and focused processes is a visible C2 enabler. The IKM process considers the following questions:

- What information is critical to the commander and when is it needed?
- What format and style are required by the commanders?
- Who is responsible for obtaining, processing, analyzing, correlating, and disseminating the information?
- How should this information be protected and from whom?
- Does the required information already exist?
- Who else might need the information?
- Who has the need to know?
- Who has authority to release information?
- What is the best way to effectively get the information to other users?

Information and Knowledge Management Principles

Information and management principles frame C2 solutions. The principles discussed in the following sections provide a foundation for shaping and prioritizing IKM activities. They are relevant regardless of the situation or mission.

Define the Information Flow with Prioritized Requirements

Command relationships, force organization, mission, and information requirements influence the flow of information. The following are crucial to ensuring a proper information flow:

- Build process maps to identify and analyze the flow of information.
- Identify and prioritize information requirements.
- Ensure resources are available and tasked to collect and provide the prioritized information to the intended audience.
- Coordinate personnel, equipment, training, procedures, information technology, and communications to ensure information is available to the decision maker when needed.

Seek and Deliver High-Quality Information

Information must be accurate, complete, and relevant to generate or transfer knowledge and understanding. To accomplish this, information requirements should be determined as early as possible in the process. Sufficient resources should be employed to obtain the data and to process, collate, and synthesize the information. As information becomes knowledge and understanding through processing, it can be framed within context, and ready for the commander's use in decision making. As situational awareness is gained and maintained, less repetitive information is required in briefings, freeing time for discussion and collaboration. Based on the commander's information requirements, repetitious information should be set aside but not discarded. Furthermore, care should be taken to retain data that could be relevant to future decision making or analysis.

Use Multiple Sources of Information

Using multiple redundant sources to gather and process data helps validate findings in the battlespace by allowing a venue to compare collected information and identify discrepancies. Ideally, three or more sources might highlight a single, inaccurate data source for rapid exclusion. Too few sources can make it difficult to disregard inaccuracy, potentially bringing good data into question as well. Too few sources can also cripple decision making because one source may discredit another and, without enough corroborating information, the commander could be forced to make a subjective call or delay a decision. If only two sources are available and they conflict, the best choice is to avoid using the information until it can be validated. Best practices include establishing metrics for credibility and noting noncredible information sources.

Deliver Timely and Usable Formats

Information delivered late is of no value to the decision maker. The goal is to deliver timely information when it is needed and, in a form, that is readily understandable to the commander. Known gaps in information should be properly documented and a forecast provided for when more relevant data is expected to be available. A dilemma in decision making occurs when clarity or the availability of information is inadequate, and the commander must assume a risk. Making no decision or delaying a decision increases risk.

Identify and Capture Errors

Procedures must be in place to identify and capture the source of errors. This is accomplished by comparing, validating, or verifying data accuracy throughout the information's lifecycle, particularly when used in mission-critical or safety-of-life processes or applications. This is

especially important when unstructured and nonsecure information exchange mediums are employed. For example, when sending coordinates using electronic correspondence or text messaging, characters can be easily transposed while entering or recording the information (both represent error entry points). In such cases, a process to plot and validate coordinates are essential before their use.

Protect Information Throughout its Lifecycle

Information is at risk from the moment it is collected until it is no longer of any value. The nature of the threat to that information varies throughout the information lifecycle. Potential threats include not only overt actions on the part of external actors, but also failures on the part of data owners to properly implement and manage the information through its lifecycle.

Build Understanding from the Bottom-Up

The nature of recent conflicts has forced a refocus and reconsideration about the value, priority, and effort invested in information. Warfighters must attempt to make sense of the actions of many actors, whether they are the enemy or those operating according to other interests. Actions and intentions might come from external elements, such as political leaders, tribal or local elders, insurgents, and noncombatants. Often, the best information comes from corporals who have boots on the ground. Information management processes must support these contributors and capture their situational awareness to provide understanding at the operational and strategic levels.

Decentralize Information Knowledge Management Execution

To maximize the ability to reliably and rapidly process and disseminate information to the intended audience, IKM activities should be decentralized to the greatest degree possible while maintaining effective control. Though technology by its nature is centralized, centralizing IKM activities creates bottlenecks that restrict information flow. These bottlenecks occur when too much information is delivered solely to a key node (whether people or technology), which results in backlogs for information processing and dissemination.

Reduce Complexity

While complexity cannot be completely avoided, it must be minimized so that people can focus on the information rather than on the tool or devices being used to present it.

Repercussions from complexity might include—

- Higher expenditures for initial and sustainment training.
- Lower proficiency if the training effort is inadequate.
- Higher probability that the data will initially be misinterpreted or unusable by decision makers.

Aligning commander expectations with investment in process development, user training, and system integration focuses technology capabilities for the intended outcome.

Tailor Information for Intended Audience

Information increases in value when formatted or tailored for the audience. Tailoring presentations and visualizations accelerate the process of moving from raw data to decision-maker understanding. On the other hand, general or unformatted information hinders and delays decision making, requiring leaders to translate data into a consumable format to achieve understanding before critical decisions can be made.

Set Conditions for Information Development and Knowledge Sharing

The ultimate goal of IKM is to provide a process that enables the user to leverage C2 systems with relevant skills to understand and shape battlespace and to recognize, collect, and share critical information with decision makers to defeat opponents. Creating conditions for rapid information sharing, and assimilation of knowledge for understanding, requires more than production, transportation, and presentation of data. A force must have a keen understanding of the collaborative and C2 systems that model the battlespace; share, store, and visualize information; and provide context for decision-making. Effective information management—

- Makes users aware of available resources (e.g., C2 systems) that find and retrieve relevant information—the higher the quality and timeliness of delivery, the greater the value.
- Institutes a culture of information and knowledge sharing with a sense of urgency and understanding.
- Ensures every leader, from fire team leader up, is assigned commensurate responsibility for preparing, presenting, and ensuring delivery of high-quality training and information sharing to subordinate Marines.

Enabling Command and Control System Structure

Information and knowledge management is a C2 enabler and must work inside the C2 infrastructure. The technology capability is balanced by information sharing policies and technical limitations. Effective information management—

- Ensures personnel are provided C2 system learning opportunities through high-quality training events. Proactively plan appropriate technical and process resources as required.
- Ensures new information relevant to the unit's mission and training objectives is rapidly incorporated into existing training throughout the training cycle. Information sharing is a continuous action.

The following sections define C2 architectures and nuances in a hierarchical form to allow users to leverage technology capabilities in a military context.

Effective Command and Control Structure. An effective C2 structure provides the benefits of labor and time savings and ease of dissemination and information flow. Command and control capabilities and procedures enable rapid, intensive calculations that otherwise might take several people much longer to complete. Networked C2 structure capabilities allow users to transfer information and knowledge simultaneously to many users even if they are not in the same geographic location. Further, when enabling a C2 structure to enhance the flow of information across warfighting functions (i.e., maneuver, fires, logistics, force protection, intelligence, command and control, and information) and across traditional staff sections, the factors discussed in the following sections should be considered.

Location of Information. The location for specific types of information is often predictable, particularly if the process to support the information requirement is understood. Pre-positioning required information at anticipated points of need speeds up the flow of information, reduces demands on communication networks, and provides required information to those who need it in a timely manner. This consideration is particularly important when units are highly dispersed.

Mobility

Reliable and secure flow of information must be commensurate with the commander's mobility and tempo of operations requirements. Capabilities and procedures that support effective information flow must be flexible enough to immediately adjust to support bandwidth-challenged and highly mobile command posts, as well as the mobility requirements of the subordinate units.

Accessibility

All levels of command must have access to required information to support concurrent and parallel planning, mission execution, and assessment. The IKM structure provides access to information to required user(s) via automated means to reduce time and confusion while increasing efficiency and dissemination of high-quality information (e.g., automated, dynamic visual displays of force).

Information Push Versus Pull

The two basic approaches information management uses to share information is supply push and demand pull. The IKM structure must incorporate the most appropriate approach based on the commander's information requirements. A supply push methodology relies heavily on information being pushed from the source to the user, either as the information becomes available or according to a schedule. The advantage of supply push is that the commander does not need to request high-quality information. High-quality information is delivered to the user in a timely manner, but there is always the danger of information overload because producers of information might not completely understand user information requirements (e.g., daily intelligence summary). In contrast to supply push, a demand pull system requires the user to initiate the flow of information. If the information is readily available (already resident in some database), the requirement can be quickly satisfied. If not, the requirement must move through the chain of command until it reaches the appropriate level. Information can be tailored specifically to support the identified requirement, avoiding overload. The disadvantage to demand pull is the potential added time, because the search for information might not begin until the commander or user has identified the need (e.g., RFI systems).

NETWORKS

Numerous systems or applications are used to support operational requirements. The information generated and personnel using these tools could require different communications networks for information sharing and dissemination.

Sensitive Compartmented Information Networks

Specific classified networks are used to process and disseminate information classified as sensitive compartmented information. These networks include the Joint Worldwide Intelligence Communications System and the National Security Agency Network.

SECRET Internet Protocol Router Network

The SIPRNET is a classified network that is authorized to process and disseminate information classified as SECRET or below.

Nonclassified Internet Protocol Router Network

The NIPRNET is a sensitive but unclassified network that is able to process and disseminate sensitive but unclassified information and below.

Coalition Wide Area Network

There are three aspects of the coalition wide area network: the Releasable Internet Protocol Router Network, the Combined Enterprise Regional Information Exchange System (CENTRIXS), and the All Partners Access Network (APAN). The Releasable Internet Protocol Router Network is a secure coalition network used for joint, Republic of Korea, and United States usage. The CENTRIXS is a combination of global, multilateral, and bilateral, virtually separate networks supporting multinational efforts. These networks form the backbone of what is envisioned to become a global infrastructure that allows the United States to share information rapidly with coalition partners worldwide in support of local, regional, and global combined Operations. The APAN is an unclassified network that provides interoperability and connectivity among partners over a common platform (addresses does not end in .mil). The network fosters information exchange and collaboration between DoD and any external country, organization, agency, or individual that does not have ready access to traditional DoD systems and networks, such as when engaging with Red Cross during a humanitarian aid or disaster relief mission.

Information and Knowledge Management Requirements Determination

The IKMO does not own any processes or procedures; rather, the IKMO improves staff and MAGTF process efficiencies. Timely, high-quality information promotes a commander's situational awareness and enables informed decisions. To define information processes, organizations must first define the information's producers and consumers, the products they produce and consume, the timetable on which consumers need products, and the means by which the product is conveyed and delivered. The combination of producer, consumer, and information products are represented as IERs. Aggregated IERs impact C2 system effectiveness and, thereby, the people who produce and provide the information. Information exchange requirements drive network, system, and application requirements that must be planned and coordinated to achieve effective organizational command and control and collaboration.

Commands can follow a structured approach to IKM planning that identifies the information producers and consumers, considers the information to be exchanged, and determines the necessary resources and exchange requirements. These factors are incorporated into the context of the mission to identify and establish IKM services and correlating processes to satisfy the commander's intent for a specific exercise or operation. The IKM planning checklist provided in Appendix B guides the IKMO in accomplishing the eight critical planning steps as follows:

1. Document the IERs.
2. Create the C2 systems and software baseline.
3. Construct and manage the command battle rhythm.
4. Construct the information management matrix web parts (i.e., feature to create web pages).
5. Coordinate with the G-6/S-6 to deconflict authorities to connect ports, protocols, and firewalls.
6. Construct the IKM annex.
7. Brief and train the staff.
8. Prepare for operations.

Process Flow

The first step in developing information requirements is to identify discrete information exchanges or requirements supporting a particular task or function. A process flow diagram identifies the series of tasks necessary to support a particular task or function. Figure 4-1 is an example of a completed process flow diagram. This example delineates the tasks required to provide the information to support the intelligence collection function. Overlaid on the process flow is a depiction of the organizations within a MAGTF responsible for the appropriate components of the process flow.

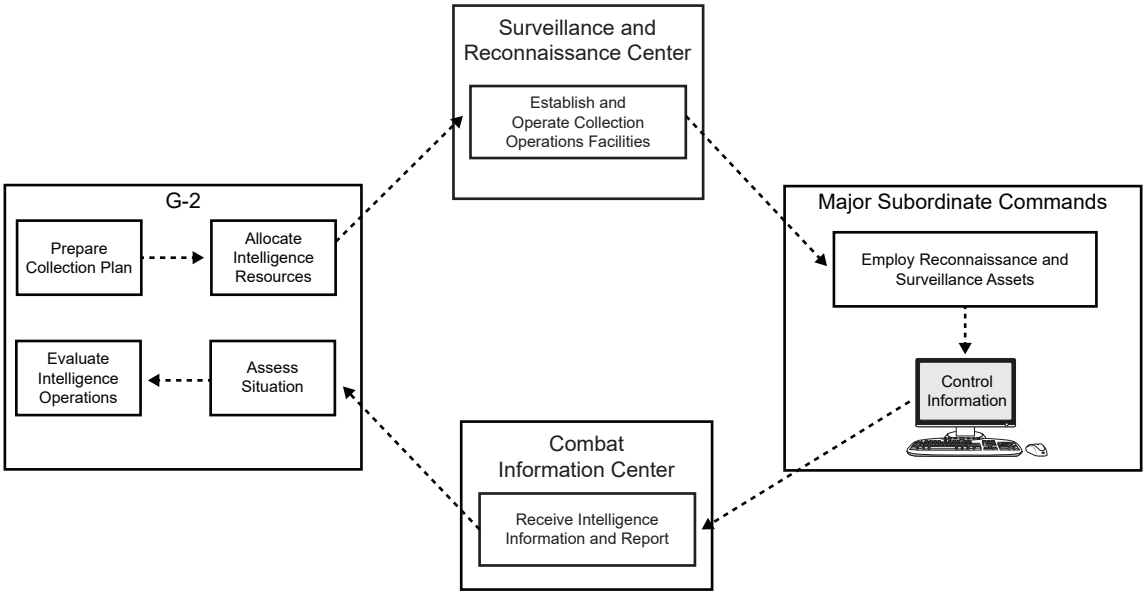


Figure 4-1. Process Flow for Intelligence Collection.

Configuration Flow

Once the process flow diagrams have been created, the next step is to develop a configuration flow diagram. A configuration flow diagram describes the process flow of systems needed to support specific tasks. A configuration flow diagram is established by performing two steps:

determine the system required to perform each task and identify the network infrastructure necessary to disseminate information produced by personnel performing each task. Figure 4-2 depicts a configuration flow diagram to support the process flow described by Figure 4-1. Each system is placed in the appropriate command element organization and linked to a network infrastructure. Current command relationships and task organization of forces are considered to develop the configuration flow diagram. This methodology permits a command to identify system and network shortfalls or potential vulnerabilities.

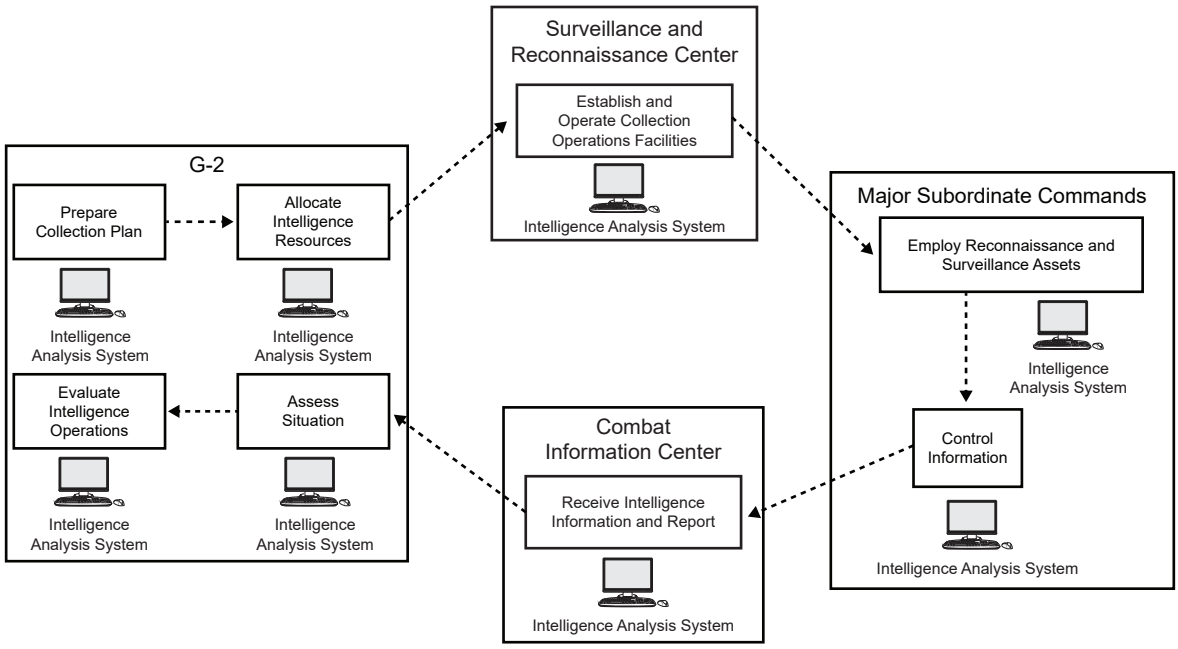


Figure 4-2. Configuration Flow for Intelligence Collection.

Personnel Requirements

During the final step of developing an IKM structure, the command identifies personnel requirements from the configuration flow diagram, which determines the number of personnel, skill sets (training), and procedures necessary to support each warfighting function. These requirements are then measured against what is currently being used by the command. This action enables the command to clearly identify deficiencies and implement corrective action. The result is an efficient flow of information within the command IKM structure and improved decision making. Figure 4-3 demonstrates a personnel requirements diagram to support the configuration flow diagram described by Figure 4-2.

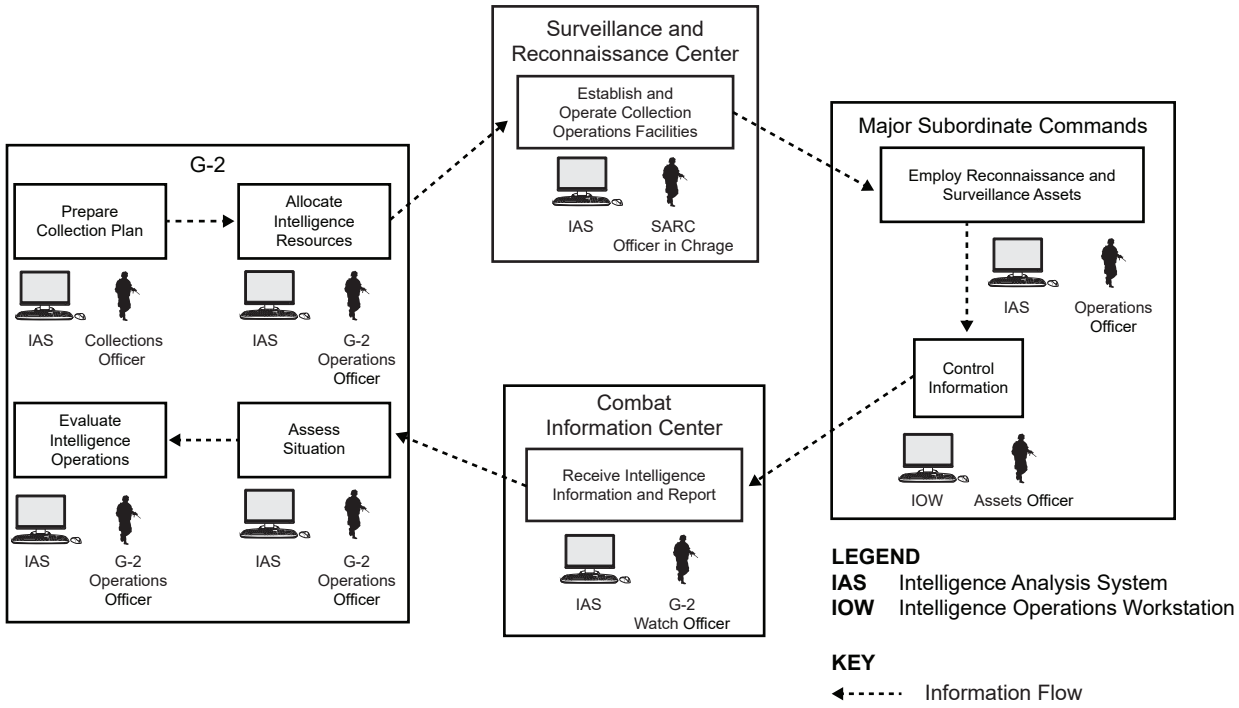


Figure 4-3. Personnel Requirements for Intelligence Collection.

Information Management Documentation, Products, and Tools

Reports Matrix

The reports matrix is a chart of reports provided by subordinate and higher entities to coordinate the flow of information for both routine and immediate notification. There is no doctrinal format for the reports matrix, but it should include the time the report is due, period of time covered, priority, classification, recipient, author, format, means of transmission, and comments, requests, and recommendations. Reports require a coordinated rhythm because senior headquarters collate subordinate information into reports that are delivered to HHQ. As reports move through the command structure, information is confirmed and fused for verification and validation. An effective reports matrix is a powerful planning tool to support execution, verify information, and correct the source of information flow problems. A carefully designed reports matrix significantly enhances the efficiency and effectiveness of staffs and decision makers.

Battle Rhythm

The battle rhythm is a scheduled sequence of daily events (e.g., functional areas and working groups, staff briefings, updates, visits) that involve the commander, staff, and subordinates. The purpose of the battle rhythm is to frame the commander's decision-making cycle; facilitate the proper integration of hierarchical events supporting current operations and future operations and plans; and staff, train, and equip event horizons. The C/S or XO oversees the battle rhythm, but often delegates the responsibility to IKMOs who assemble, publish, manage, and disseminate the battle rhythm. Commanders and staff officers are responsible for identifying events to be placed

on the battle rhythm. The battle rhythm is the backbone of staff and subordinate coordination and decision making. Resources, such as the JECC Knowledge Management Practitioner's Course and MarineNet, provide doctrinal formats for battle rhythm development, analysis, and visualization.

Commander's Critical Information Requirements

A CCIR is an information requirement identified by the commander as being critical to facilitating timely decision making. The two subcategories of CCIRs are priority intelligence requirements and friendly force information requirements. Information requirements represent the commander's determination of critical information requirements during each phase of a campaign. Combined with a DSM, CCIRs can focus an organization for relevant response based on strategic opportunity. Requirements can frame information collection and analysis as well as form the basis of response, shaping the battlespace. The CCIRs are a very important operational framing tool. Instead of reacting to a threat, commanders are able to maintain tempo by controlling the flow of information required to attain the level of understanding they need within the battlespace. Without CCIRs, subordinate units could become overburdened with RFIs; moreover, communication systems and networks could become saturated with requests for nonessential information. As events unfold, the information requirements could change; consequently, new decisions are required and CCIRs must be continuously assessed for relevance to support current and future decisions and situations. The key question is, "what does the commander need to know in a specific situation to make a particular decision in a timely manner?"

The CCIRs serve the following functions:

- Reduce the information gaps generated by uncertainties that the commander might have concerning their force, the adversary, or the environment that are identified as necessary to maintain situational awareness, plan future activities, and facilitate the ability to make timely decisions.
- Focus the staff on the processed data and knowledge the commander needs for making key decisions (particularly during the course of an operation), reduces informational needs and raw data to a manageable set, and ensures that key information requirements are not inadvertently filtered out.
- Define the information required by the commander to better understand the battlespace and to identify risks as well as to make sound, prompt decisions to retain the initiative.

Decision Support Matrix

The DSM identifies key decision points and actions decided upon by the commander during the preceding planning phase. A DSM can be depicted graphically or in table format to frame an action or operation and to time or vary a response. Decision points are annotated throughout the DSM to assist the commander in controlling the effort. A DSM can be used at all levels of a command and is a very helpful tool in the planning phase.

Requests for Information

Requests for information are specific, time-sensitive, ad-hoc requirements for information or products to support an ongoing crisis **or** operation not necessarily related to standing requirements or scheduled intelligence production. The RFIs are generated to answer questions that cannot be resolved with organic assets, and when the information does not exist within internal databases or cannot be satisfied by resident subject matter experts. An example of an RFI process map is shown in Figure 4-4.

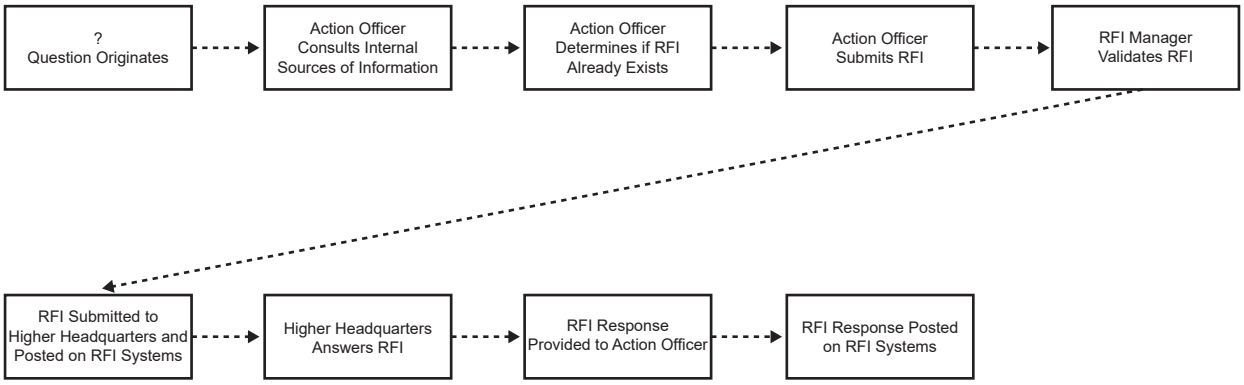


Figure 4-4. Example of a Process Flow Used to Support Request for Information.

Information Management Matrix

The information management matrix, created as a webpart in the collaborative workspace, serves as a single collection of functional area formats and templates used to generate and exchange high-quality information. It provides the primary, alternate, contingency, and emergency (PACE) plan for the exchange of the completed format, as part of the push/pull of information discussed earlier in this chapter. Items required in the matrix include battle rhythm event input and output formats, functional area request forms; report, briefing, and correspondence formats; and other essential templates for generating actionable information.

Journals and Logs

Journals and logs are chronological records of a unit's activity. For units engaged in contingency operations, the importance of accurate journals and logs cannot be overstated. The unit commander should direct that a command journal be maintained in the operations center and that general staff sections maintain their own journals. The value of accurate journals goes beyond historical analysis; it keeps the commander and staff up to date on significant activities and significant events (SIGEVENTs). These products can be used for analyzing operations, extracting lessons learned, and investigating, when requested.

Information and Knowledge Management Plan and IKM Annex (I, M, or U)

The IKMP is the commander's vision for managing and controlling information (see Appendix C). The IKMP details the planned support for all three elements of command and control—information, people, and C2 infrastructure. The IKMP assigns responsibilities and provides instructions for personnel that manage C2 infrastructure. Responsibilities identified by the unit's SOPs do not need to be duplicated in the IKMP. Development of an IKMP is a vital step for enabling a conducive environment for decision makers to receive the required

information, when needed, in an understandable format. Each command must develop an IKMP tailored to manage its information in the context of its mission and current situation or event. An effective IKMP provides guidance to ensure high-quality information is provided in a form users quickly understand. The IKMP should cover C2 filtering tools, unique IKM personnel needs (duties, responsibilities, and skill requirements), C2 structure requirements (processes and procedures), and C2 system protection. The IKMP should include specific guidance for management of the CTP, CCIR, collaborative planning system, and network applications used to share critical and relevant information. Inputs to the IKMP can be accomplished through the use of chat rooms, wikis, blogs, web pages, or other applications. The development and execution of an effective IKMP requires the participation and interaction of all staff sections.

The IKMP is a collaborative document; each staff section must identify its information requirements, warfighting processes, configuration flow diagrams, and personnel requirements for incorporation. Information management policy and procedures are top-down in nature and the IKMP should include considerations for joint and coalition interoperability. Joint task force IKM practices nest within the supported combatant commander's established policies. Likewise, component, MAGTF, and major subordinate commander IKM practices nest within those of the JTF. Commanders and staffs at all levels must have a common understanding of joint IKM policy and procedures.

Detailed examples can be found in Appendix A through D for consideration in developing the IKMP. Appendix D details the development of the Annex U.

Insights and Considerations

The following insights and considerations reflect lessons learned regarding IKM processes and procedures:

- Use CCIRs to prioritize the flow of information. The commander's guidance and CCIRs focus the staff and resources to provide fused information to support decision making. The CCIRs serve as control measures by establishing collecting, processing, analyzing, and disseminating priorities.
- Take charge of knowledge sharing. This is an all-hands responsibility because it is too important to be left to an individual staff section.
- Delineate authority and responsibility for the different aspects of knowledge sharing,
- Information management, and the associated tools and C2 systems.
- The C/S or XO should have the responsibility for information management and knowledge sharing; an operationally focused IKMO should be designated to report to the C/S or XO.
- Clearly define the headquarters' decision-making processes before determining the IKM means and tools. Consider both physical and virtual collaboration means to conduct battle rhythm events, which can be physical meetings, phone calls, or virtual, such as web conferencing, chat rooms, secure video teleconferencing and other collaborative tool suites. Retain the tried and proven use of a scribe to record key information and decisions. Post summaries on a website portal or the collaborative workspace.
- Develop a command climate whereby all personnel are vigilant in protecting sensitive information.

- Identify the communications networks and platforms needed to support the information exchange requirements (e.g., CENTRIXS, SIPRNET, or NIPRNET). Develop processes to share information with interagency and coalition partners not on your communication network.
- Develop an environment that fosters a responsibility to share versus a need-to-know mentality with nontraditional partners (e.g., interorganizational and host-nation partners) to better support decision making while accounting for the risks associated with compromise on the various networks.
- Develop procedures for RFI management and foreign disclosure within the command.
- Develop a sufficient capacity to enable foreign disclosure and information sharing with partners. This includes ensuring there are foreign disclosure officers and trained foreign disclosure representatives on the staff.
- Ensure key information sharing procedures are understood throughout the staff. Carefully select tools that are user friendly. Recognize the impact of personnel turnover and training requirements. An adequate information technology tool, well understood and used by a staff, is much more effective than a perfect, continually changing information technology tool that is too complex to intuitively understand and use.
- Develop and refine IKM processes and procedures through a working group led by the IKMO and composed of staff section representatives. The working group reports to an IKM decision board, which is chaired by the C/S or XO. Task the working group to maintain currency and relevance of the commander's and staff's knowledge and information assets.
- Disseminate approved IKM and knowledge sharing processes through an authoritative IKMP. The IKMP should define the responsibilities of the IKM organization. It should also provide guidance on how to gain and maintain situational awareness; share information; and collaborate with higher, adjacent, and lower organizations throughout the decision cycle. Periodically revise the IKMP to reflect improvements to the command's processes as they are developed over time. Be prepared for change. Do not allow an IKMP to become stagnant. The IKMP must adjust to the individual's decision-making processes.

Appendix A.
Tools, Tactics, Techniques, and Procedures for Information Flow

The commander's guidance frames parameters for information filters used by the battlestaff to develop and refine useful products. Filtering tools, such as commander's intent, commander's guidance, and CCIRs enable personnel to enhance information flow and support decision making.

Tools

Commander's Intent

The commander's intent articulates the purpose of an operation. It might also include how the commander envisions achieving a decision and provides the end state or conditions that would indicate success. The commander's intent establishes the standards by which success is measured and sets the tone and framework for effective information management (IM).

Planning Guidance

The commander's guidance forms the basis for planning. Although not prescriptive in nature, planning guidance helps the staff make initial recommendations on which actions to take. Based on personal experience and judgment, the commander articulates guidance to help staff and subordinate commanders focus on information management efforts.

Commander's Critical Information Requirements

The CCIRs include information about enemy and friendly activities and the environment, as identified by the commander, to maintain situational awareness, plan future activities, and facilitate timely decision making. The CCIRs focus the staff on the information the commander needs for critical decision making and reduces information needs to a manageable set. The CCIRs are continuously assessed for relevance to support current and future decisions and situations. The commander approves CCIRs, but the staff recommends and manages CCIRs to assist the commander.

Information Exchange and Collaboration Tools

To a great extent, the means through which information is exchanged involves technology. Marines not only have grown reliant on information technology to accomplish many objectives, but also have significantly changed TTP as a result. Though the Marine Corps must strive to

maximize the efficiencies that information technology offers, it must, at the same time, preserve the ability to function and to accomplish its mission without it. The following sections discuss some of the tools commonly used.

Electronic Correspondence

As a collaboration tool, electronic correspondence facilitates the dissemination of a large amount of information to large audiences. Although electronic correspondence is an effective means of communication, Marines must remember that the human aspects of communication, such as force of personality and tone of voice, cannot always be conveyed accurately in an electronic correspondence. Electronic correspondence should not be the sole method of conveying critical or important messages.

Computer Networks

The unclassified government computer network that provides connectivity throughout the DoD is the NIPRNET. This network is intended for unclassified official use only and is accessible to all authenticated and authorized users via the internet. The equivalent network operating at the secret level is SIPRNET. The NIPRNET and SIPRNET are mutually exclusive.

Web Services

Another resource supported by both the NIPRNET and SIPRNET is the ability to maintain websites. A website is an excellent tool for disseminating information. Its functionality lends itself to regular use by even the most inexperienced users and it extends to anyone with a network connection.

A command intranet website is a useful means of sharing information and knowledge within a command. It works well in both garrison and tactical environments; although, consideration needs to be given to the lowest unit capable of accessing tactical websites in tactical environments. There are several website portal applications available for use. Some thematic areas that can be addressed on a portal are document libraries and website procedures.

Document libraries are similar to file servers; however, document libraries contain features not available to file servers and use websites. The IKMO needs to consider publishing file naming conventions and file access and upload rules and permissions. To ensure a seamless flow of information, the following procedures and standards for website employment should be considered:

- Document Library. All section documents are maintained in the unit's document library. Folders on the portal are organized around the warfighting functions and traditional staff sections.
- File Naming Conventions. Documents placed on an organization's portal must follow the format developed by the IKMO and approved by the commander.
- Permissions. Assign appropriate permissions. Consider administration, read and write, and read-only permissions. Typical groups for permission assignment include administrators, section administrators, website developers, primary staff, internal and external users.
- Calendar. The operations section maintains the unit calendar. The unit calendar only includes items of interest at the command level. Unit sections maintain their own section's calendars

with information unique to their section's requirements. Information for the unit calendar is inputted by section heads and chiefs or forwarded to the operations chief for inclusion into the calendar.

- News and Discussion Items. Relevant information regarding any of the warfighting functions or unit objectives can be posted here, as well as information and discussion items pertaining to the unit and the Marine Corps.
- Really Simple Syndication Feeds. Really simple syndication (RSS) feeds are a family of web-based feed formats used to publish frequently updated information on websites, such as blog entries, news headlines, messages, and videos. The RSS feed extracts information (XML format) from websites and an RSS reader converts the extracted information into standardized formats (plain text), making it readable by the user. The RSS feeds are viewed using an RSS reader, which can be Web based, desktop based or mobile device based. The user subscribes to a particular feed and the RSS reader provides a user interface to view the content. The RSS reader regularly checks the subscription's content to provide updates at prescribed intervals.
- Document Workspaces. Document workspaces are great areas for organizing and controlling information regarding specific projects. Document workspaces are used for—
  - Coordination with internal and external agencies on specific documents, such as SOP updates and rewrites.
  - Document preparation and approval. Preparation and approvals often use a private network (i.e., extranet).

BEST PRACTICES

Battle Rhythm

Joint Publication 3-33, *Joint Force Headquarters*, states, "effective operations require the synchronization of strategic, operational, and tactical processes, to ensure mission planning, preparation, and execution are coordinated. This process, called battle rhythm, is a routine cycle of command and staff activities intended to synchronize current and future operations [in accordance with] the commander's decision cycle. One of the most critical communication tools on any staff is the ability to conduct an effective battle rhythm described as the sequencing and execution of actions and events within a [MAGTF] to regulate the flow and sharing of information supporting all decision cycles. The battle rhythm provides the structure for managing the most important internal resource, the time of the commander and staff personnel. A stable battle rhythm facilitates effective decision-making, efficient staff actions, and management of information within the [MAGTF] and with higher, supporting, and subordinate HQs."

The battle rhythm is not to be confused with daily schedules or an operations calendar published by the C/S or staff sections. Daily schedules depict specific events and activities such as very important person visits and section activities and are not part of the commander's decision-making cycle. All battle rhythm events require a seven-minute drill, which are forwarded to the

IKMWG for inclusion in the next battle rhythm analysis working group. Battle rhythm activities can be daily, weekly, monthly, quarterly, or on-call requirements. Battle rhythm management considerations include the following:

- Establish a battle rhythm analysis working group or to routinely evaluate the efficacy of the battle rhythm. Changes at HHQ and during the stages of the operation could precipitate the need for modification, event consolidation, or elimination.
- Complete a full battle rhythm analysis, which includes a time synch matrix, staff utilization matrix, and information flow.
- Create hyperlinks on the command landing page to the battle rhythm event website conference rooms, which should be easily located and accessible for participants. Numerous staff move from event to event with little time to transition in some cases.

The MAGTF battle rhythm should be posted to the website as early as possible in an operation or exercise and changes to the should be kept to a minimum. Names for functional areas and working groups should be consistent, and the battle rhythm should reflect synchronization of events across the MAGTF and nested within the headquarters.

Websites

Websites are useful for sharing information with a wide audience. The IKMP must provide guidance to staff sections and subordinate commands on their responsibilities for establishing and maintaining websites throughout the MAGTF. Usually, the IKMO has a webmaster in direct support. The content managers and the IKMO should adhere to the following:

- Cite and release changes to the OPORD and fragmentary orders (FRAGOs) before they are posted to the website, and then notify higher, adjacent, and supporting commands after those products are uploaded. Avoid the tendency to post and forget when adding critical information to the website.
- Have backup plan to transmit OPORD changes and FRAGO(s) in case of website failure.
- Frequently check the MAGTF website for content and accuracy. This action can be delegated to COC team members and rotated among watch standers.
- Frequently check the MAGTF website to guard against public disclosure of personally identifiable information or other sensitive information.
- Ensure critical information, such as FRAGOs, warning orders, CCIRs, or boundary changes, are easily accessed and appropriately flagged for attention on the website. Critical information should be consistently grouped in one area.
- Have a means of reporting website errors to the COC so that corrective action can be taken in a timely manner.
- Ensure FRAGOs are promptly posted on the website with a mechanism that allows the MSC and element to confirm receipt.

The MAGTF website should be simple in design and allow users easy access to critical information. Navigation links should be clearly visible and understandable on the main website page. Main website topics, such as battle rhythm, FRAGOs, or OPORDs, should be prioritized in clearly visible links for rapid access. The MSC website pages should emulate the format of the

MAGTF command element main website page. This facilitates website searches throughout the MAGTF. A good practice is to establish the "three-click rule," which means to design the main website page so that critical information is no more than three mouse clicks from the landing page.

Command Journal

The command journal is a chronological record of events pertaining to a unit or staff section during a given period. All administrative and operational items that have a bearing on the tactics, techniques, operational capabilities, plans, doctrine, and methodology are entered in the command journal. The MAGTF headquarters and each of its MSC headquarters maintains its own command journal.

The SWO must ensure the command journal is being maintained throughout the watch. The journal clerk carries out this task under the immediate supervision of the COC operations chief. The SWO should periodically check journal accuracy and give guidance on the content and timeliness of command journal entries.

The command journal records SIGEVENTs and actions taken by the SWO and the COC team. This enables the later reconstruction of events with minimal friction. The journal also serves as a record for training matters, operational reviews, and historical research. A MAGTF command journal is typically kept (and frequently backed up) electronically and must be available on the website. A backup paper copy should also be kept and updated frequently in case of COC power failure.

The COC should maintain a significant events log near other key COC electronic displays. A significant event could be linked to a CCIR, priority intelligence requirement, friendly force information requirement, or a decision point during current operations. Visitors to the COC can refer to the significant events log rather than request information from the SWO. Place the significant event on the unit website for easy reference.

Combat Operations Center Information Displays

The COC electronic information displays help COC watch standers to stay oriented on the current tactical situation as they perform their duties. There are many displays to keep track of during an operation: they can be on laptop or desktop computers or prominently arrayed around the COC floor on large projection screens. Digital, large-screen displays are particularly useful when the SWO wants to draw the attention of watch standers to key events as they unfold. Also, displays allow the commander and battle staff to visit the COC and get an overall situation update without forcing the SWO to stop current tasking to conduct a formal briefing. Some computer applications can zoom the display from a large-scale map of the area of operations down to a detailed photo of an area of interest. Unmanned aircraft, aided by tactical data link technology, have enabled real time video display of battlefield areas in the COC. Typical displays found in a COC follow:

- Common Tactical Picture. The CTP is a dynamic graphical representation of all active elements the battlespace and all products of those elements within the given area of operations. The CTP is an excellent situational awareness tool for the force commander and thus can be a key element of the commander's decision-making process.

- Mission, Commander's Intent, CCIR(s). A prominent display of this information in the COC reminds COC personnel of how to focus their efforts to keep the commander informed.
- Current Operations Status Boards. The following items are a sample of topics commonly on display in a MAGTF COC, electronically, either on the operation SIPR landing page, or separate large screen monitor, and in hard copy:
  - Current day of the operation (e.g., D+11/Saturday, 11 Feb 20XX). Phase of the operation (e.g., Phase IIIC, Stage II).
  - Mission-oriented protective posture level (e.g., Level II).
  - Air defense warning condition (e.g., red).
  - Weapons control status (e.g., tight).
  - Threat condition (e.g., ALPHA, BRAVO).
  - Ground watch (combat power assessment).
  - Intelligence watch (enemy combat power assessment).
  - Logistics (main supply route status).
  - Communications (system status).
- Command Journal. The COC team should post a SIGEVENTs log (or list) or the actual command journal electronically where the commander and battle staff can review them periodically without interrupting watch standers.
- Control Measures and Targeting Display. A digital electronic display of control and coordination measures serve as a rapid reference in the COC for all watch standers. Advanced Field Artillery Tactical Data System targeting data may also be displayed to track significant targets.
- Unmanned Aircraft System Video Feed. Unmanned aircraft systems enable real time or near-real-time displays of the battlespace and are particularly useful during battle drills where decision making is expedited by personal observation of the situation.

Chat

Many users monitor and use electronic chat rooms during the watch. The best way to manage chat information is to ensure the COC team and subordinate commands adhere to a command chat SOP. This SOP, at a minimum, should offer guidance on the following topics:

- Chat guard chart (e.g., tactical [TAC] 1, fires, air, logistics).
- Rules for entering and exiting chat rooms.
- Language protocol (e.g., brevity codes, acknowledging orders, flagging critical information).
- Information on the number and type of chat rooms authorized in the MAGTF (chat architecture).
- Rules for the use of whisper mode in chat rooms.
- Protocol for date and time stamping entries.
- Rules for setting tools to flag key words, such as troops in contact, mass casualties, weapons of mass destruction, and chemical attack, within the chat software application (not all applications have this capability).
- Rules for "coffee break" events, which is a key term to indicate the watch officer is away from the computer terminal.
- Rules for backing up historical chat records.
- Procedures in the event of chat failure, including alternate means of communication.

Briefing Templates

Preparing and giving briefings consumes a significant portion of the COC team's time. The exact amount of time spent varies with each commander and with how much time the COC team spent preparing briefing templates prior to the operation. Rather than prepare each brief from scratch, a prudent watch officer should prepare briefing shells tailored to each type of brief the briefers are likely to give. Some briefings, common to every operation, include—

- COC shift change.
- Commander's update.
- Operations and intelligence update.
- HHQ update.

When preparing briefs, use maps and map chips to cut and paste into PowerPoint slides. Hide slides that have no change from previous briefs. Limit slide content to three or four key points.

Information Management Matrix

The information management matrix serves as the single collection of functional area formats and templates used to generate and exchange high-quality information. To ensure the matrix is most beneficial include the following:

- Point of contact (POC) using the tactical email address.
- POC's tactical phone number.
- When establishing PACE. options, provide the exact workspace or library URL, organization mailbox address, web-conference room link, location for face-to-face.
- Operational check the format links and confirm the correct formats being used.

Decision Support Matrix and Decision Support Template

The DSM and decision support template can be displayed individually or together. The DSM identifies key decision points and actions decided upon by the commander during the planning phase. The decision support template is a graphic depiction of the DSM information in the command and control personal computer. The electronic display of both tools in the COC gives each COC team member a common reference for situational awareness.

Digital Rules of Protocol

Video Teleconferencing. Video teleconferencing is a communication technology that allows collaboration between users at two or more different locations by creating a face-to-face meeting environment. The primary briefer for the session uploads the slides to be presented into the auditorium file cabinet. The first slide shows the file address in the auditorium file cabinet. The alternate briefer is responsible for answering posted questions (this allows the primary briefer to continue) and announces where the briefing and minutes will be posted. The systems administrator provides technical assistance as required and the note taker keeps track of taskings, recommendations, and questions, copying questions posted into the minutes at the conclusion of the session and posting the minutes as directed.

Audience members should log in at least 10 minutes prior to the start time and check in (voice and chat) with the deputy. If a member attends as a generic sign on (e.g., Planner 22), then a specific identification should be immediately placed in the chat. As audience members enter the chat, they should—

- Choose a seat in a row to facilitate chat in an interest group.
- Change rows to coordinate with other groups.
- Ask questions that focus on meeting issues.
- Use private chats to increase collaboration.

Ad Hoc Meetings via Chat

The active users function provides a listing of all users logged into the virtual collaboration environment and current room location. Users may contact one another without leaving their respective rooms. The following are functions within a chat that users might choose:

- Invite. Invites addressee to join the room.
- Join. Transports user to the room of the person selected.
- Send Note. Sends a text message.
- Chat. Opens a private chat window.
- E-mail. Sends an electronic correspondence through the mail system.

Document File Naming Convention

Consistent document naming is essential to proper workings of the collaboration tool. All files (e.g., documents, presentations, spreadsheets) must conform to the following naming conventions:

- Arabic numerals only (no Roman numerals).
- No spaces. Use an underscore in lieu of a space.
- All documents use military date (yyyymmdd), then an underscore, then the document's name, and then an underscore and the version number (e.g., 20090122_ReportsMatrix_v1.doc).

File Management and Information Storage

Fundamental to the process of information management is the implementation of an information storage system and procedures that provide the ability to store information in a searchable database. The following technologies provide a solid foundation for any command's information management scheme.

The IKMO, in conjunction with the G-6, determines and publishes the rules for file and folder naming conventions. Folders can be created along warfighting functions, staff sections and departments, or command lines.

Website portals, both private network (extranet) and intranet, should be used as a knowledge repository. Information must be kept current and relevant. Public folders can be shared with members outside of the command as long as they have a common access card or public key infrastructure access.

File Management and Information Storage Recommendations

Files should be saved to the designated drive of a computer or an approved file server or device. Nothing is to be saved to the designated primary drive; rather, to an approved government issued laptop or drive until shared publicly. All file naming conventions should be followed as published by the IKMO and the file name of a document should not be changed after it has been published to the user community.

Briefing Slide Show

File production and management formal briefing slides should follow a consistent format. The IKMO should make a blank presentation template available for everyone to use. The following is an example of formatting standards:

- Keep text slides basic, removing logos and only using pictures when required. If graphics are necessary, the image concerned must be grouped and then saved as a .gif [graphics interchange format] or .jpg [Joint Photographic Experts Group] file and then placed on a blank slide.
- Keep briefs short (fewer than 15 slides is ideal). If a longer brief is required, break it into sections with question and clarification breaks.
- Use Arial font for the text. The title should be 36-point type (32 point if two lines), subtitle 28-point, first level 28-point, second level 24-point, third level 20-point, and footers 14-point.
- Make text emphasis bold, underline, and italic, limit the use of colors, and only use colors that stand out well.
- Keep text spacing (tool bar, format, line spacing) minimums—lines 0.90, returns 0.25.
- Organize the footer as follows:
  - Lower right: slide number.
  - Lower left: date-time group of briefing and version.
  - Bottom center: point of contact information and JTF portal posting location.

Calendar Operations

Calendar functions are used to conduct numerous operations in the scheduling and management of collaborations. The common use calendar is maintained for the purpose of coordinating all staff collaborations. Groups, such as plans, operations, or intelligence, may maintain their own calendars for the specific purpose of their own groups' management. When calendars are used, they are linked to the main calendar, such that the main calendar shows all entries. All boards, and centers are scheduled on the calendar, specifically inviting the required and optional members with the meeting reminder enabled. In addition, the invitations have the location and the fallback procedure and location in case of system failure. The agenda of the event is posted in the text area of the invitation. The recurring event feature is recommended for standing meetings. If this is used, the meeting owner should review the invitation list and agenda daily.

Guidelines for Electronic Correspondence

Electronic correspondence should not be used for sensitive or emotionally charged issues. Personnel, personal, or work-related issues that have certain sensitivities are best handled with either a face-to-face meeting or telephone call.

Electronic correspondence should not be used to disparage others. It is an effective medium for conveying information; however, it is totally inappropriate to use e-mail to disparage or incite others. Be aware that electronic correspondence is not private. Keep in mind that all correspondence sent to others becomes official record. Do not send electronic correspondence to individuals unless you wouldn't mind it being seen by either the JTF commander or public media.

Electronic correspondence should be limited to what is essential to the mission. Jokes, stories, and nonessential audio, video, interleave or image files may temporarily improve morale; however, they tend to clutter the local communication infrastructure.

Appendix B.
Information and Knowledge Management Planning Process

Information and Knowledge Management Planning Process Checklist

Commands follow a structured approach to IKM planning that identifies the information producers and consumers, considers the information to be exchanged, and determines the necessary resources and exchange requirements. These factors are incorporated into the context of the mission to identify and establish IKM services and correlating processes to satisfy the commander's intent for a specific exercise or operation. The following provides a high-level overview of the IKM planning process. Although no particular person is assigned to provide IER, this requirement falls to each section within a command who has a need to share information with users. The following requirements are what should be considered when developing IER's:

- Document the Information Exchange Requirements:
  - Identify the MAGTF's command relationships and paths and nodes to exchange information.
  - Determine the info needed to perform applicable staff and command functions.
  - Identify the networks being used.
  - Identify the right people, right information, right time, right format, right
  - classification.
  - Determine if the IER distills large quantities of data into relevant, high-quality information.
  - Complete the IER table worksheet, Figure B-1.
- Create the C2 Systems and Software Baseline (Figure B-2):
  - For each IER, determine the correct network, application, and software version across the MAGTF area of operations.
  - Ensure linkages to higher, adjacent, subordinate, joint and coalition partners, and non-government or government organizations.
  - Identify all means and methods for collecting, processing, and distributing information.
  - Provide the C2 systems and software baseline to the G-6/S-6 network operations center.
  - Coordinate with G-6/S-6 cyberspace on all approved software versions, ensuring all MAGTF elements and mission partners have compatible information management capabilities.
  - The G-6 network operations center coordinates software validation and retrieval.

- Lock the C2 systems and software baseline and adhere to a formal process approved by C/S or XO to add, or drop systems, and applications.
- Coordinate with the G-6 network operations center to establish the command software image for use across the MAGTF and mission partners.

- Construct and Manage the Command Battle Rhythm
  - The KMO coordinates with HHQ based on the community relations to nest the command battle rhythm into the HHQ battle rhythm.
  - Primary and special staff prepare 7-minute drills using appropriate format, with a seating chart for a face-to-face event and where applicable. Figure B-3 explains format and steps for completing a 7-minute drill.
  - The C/S or XO reviews all staff submissions and approves events for the IKMO to construct the battle rhythm.
  - Ensure battle rhythm information flow of functional areas addresses event horizons: current operations, future operations and plans, staff, train, and equip to include event feeds, inputs and outputs, and portal exploitation, as depicted in Figure B-4.
  - Prepare a complete initial battle rhythm analysis to include the staff utilization matrix, time-space matrix, 7-minute drill roll up, battle rhythm info flow, and a consolidated 7-minute drill file. This saves time as changes occur later.
  - The G-6/S-6 enables communication pathways by providing secure video teleconferencing or other capabilities per the PACE plan for the inclusion of the 7-minute drill.

The functional areas and working groups follow a critical path from product production to act and plan, and the commander's touchpoints, and are nested within HHQ battle rhythm.

Information Exchange Requirements

HHQ	JTF Elements						Ad/Subordinate			Information Exchange Requirements	Network				Potential Application	Office of Primary Responsibility	Comment
	JTF Name Here						Coalition										
	USMC	JTF-PO	CFLOC	C/JACCE	C/JMCC	HMS Vessel	FAR	RMAF	FRN		APAN	NIPRNET	CENTRIXS	SPIRNET			
										Chat (XMPP)					Transverse Chat		
										Chat (IRC)					MAKO Chat		
										(Joint) (COP) Battle Field Geometry/Fire Support Coordination/Targeting/Reporting					JADOCS		
										(Joint) Artillerly/Fires Planning, Execution, and Deconfliction/Targeting Reporting					AFATDS		
										(Joint/Combined) Air Tasking Order (ATO)/Airspace Control Order (ACO) Execution and Status Update Tool							
										(Joint/Combined) Air Tasking Order (ATO)/Airspace Control Order (ACO) Planning, Development, and Execution Program					TBMCS		
										Simulation Server Monitoring (IF RC is USMC)					MTWS		
										Marine Corps INTEL & INFO Data Base					MARINELINK		
										Imagery Interpretation System					DTAMS-LITE		
										Imagery Interpretation System					TEG	J-2	
										Fires					STRIKELINK		
										Fires					PSS-OF		
										Logistics-Movement Control					BCS3		
										Logistics					TCPT		
										Logistics					CLC2S		
										(USMC) C2 System Intel Tracking System					JSTARS		
										(USN) What is the Requirement?					Turbulent Wave		

Figure B-1. Information Exchange Requirement Table Worksheet.

C2 Systems/Software Baseline (Example)

	System, App, SW Version, URL	Confirmed by IER workbook inputs			
POR?	Application	Network(s)	Software Version	OPR	Comments/Changes
	CISCO Jabber		X.X.X.X.X	G-6	
	Openfire 4.5.1		X.X.X.X.X	IKMO	
	TSOA		X.X.X.X.X	IKMO	
	J-Chat		X.X.X.X.X	IKMO	
	MS VOIP		X.X.X.X.X	G-6	
	Radio		X.X.X.X.X	G-6/AAOG	
	LOGFAS		X.X.X.X.X	G-4	
	SharePoint		X.X.X.X.X	IMO	
	Outlook		X.X.X.X.X	G-6	
	Office		X.X.X.X.X	G-6	
	Teams		X.X.X.X.X	IKMO	
	GVS		X.X.X.X.X	IKMO	
	C2PC		X.X.X.X.X	IKMO	
	TCS		X.X.X.X.X	IMO/ EXCON/MTWSS	
	MCCIS		X.X.X.X.X	G-2	
	MCCASA		X.X.X.X.X	G-2	
	CGSA		X.X.X.X.X	G-2	
	MCCIW		X.X.X.X.X	G-2	
	CGW		X.X.X.X.X	G-2	
	NITES		X.X.X.X.X	G-2	
	TCAC-G		X.X.X.X.X	G-2	
	VEW		X.X.X.X.X	G-2	
Website Requirements (Example)					
	MOL	NIPR	https://sso.tfs.usmc.mil/sso/DoDConsent.do	G-1,G-2	
	MYPAY	NIPR	https://mypay.dfas.mil/	G-1	

Figure B-2. The C2 Systems and Software Baseline Worksheet.

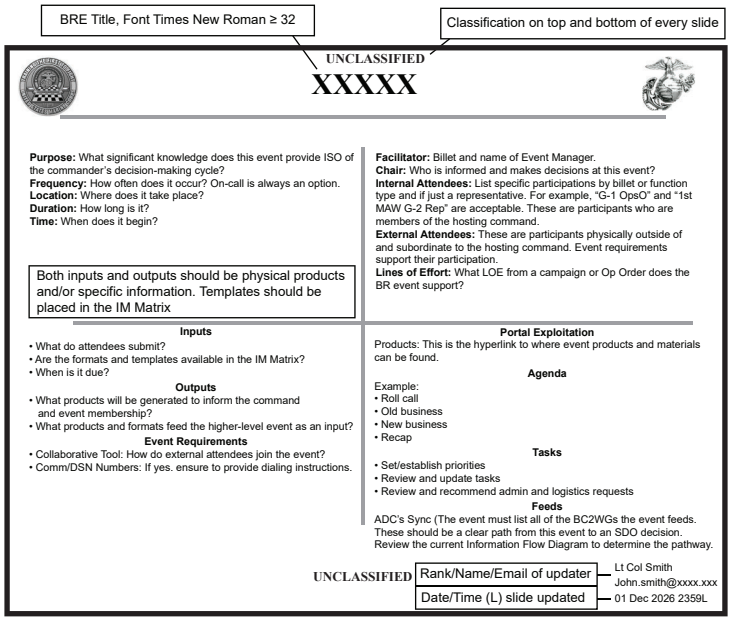


Figure B-3. Seven-Minute Drill Format Explained.

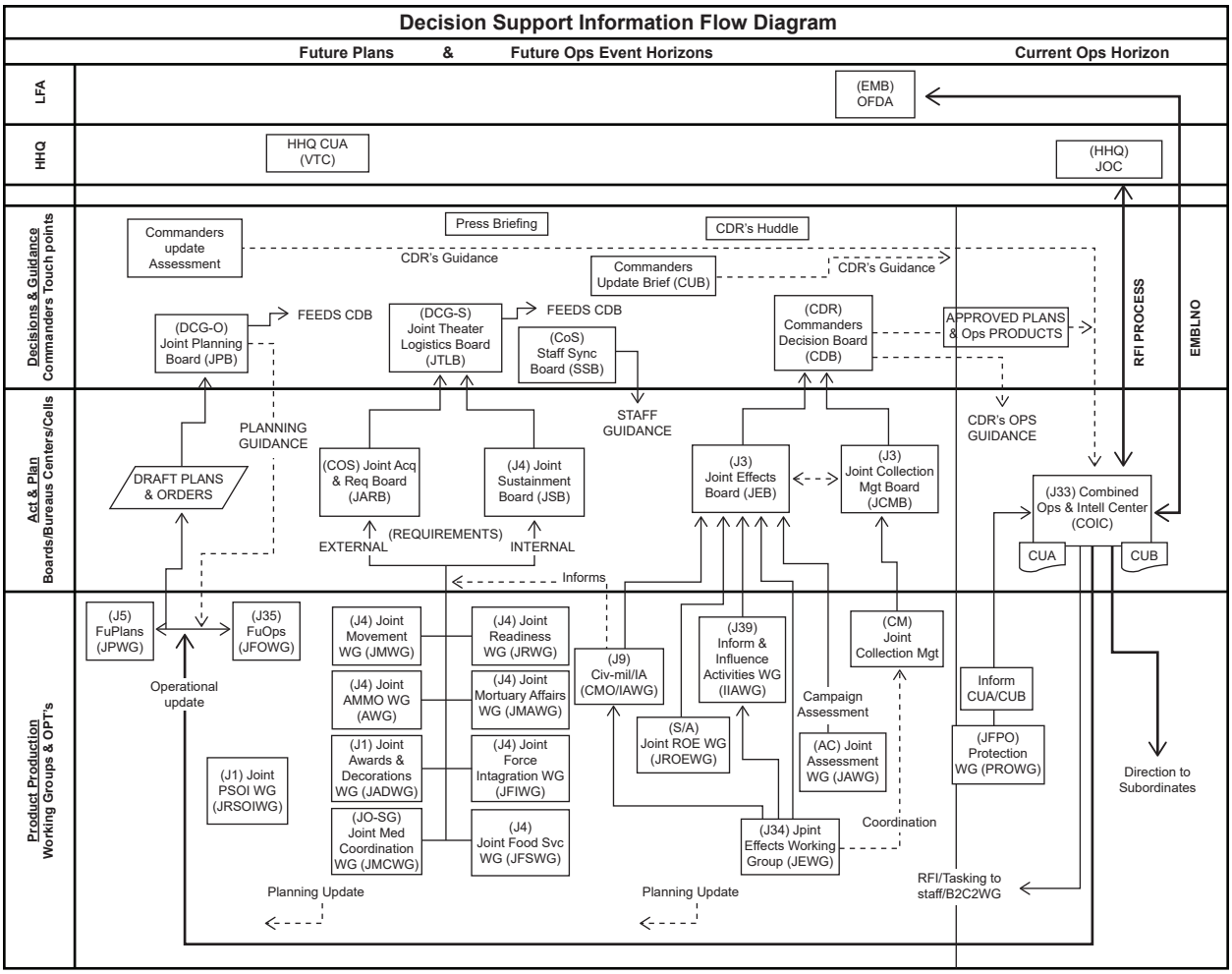


Figure B-4. The Battle Rhythm Information Flow Diagram.

- Construct the Information Management Matrix Web Part:
  - Supervises collection of the functional area input/output formats and other required functional templates for organizing data into high-quality information (methods).
  - Identifies PACE systems, applications or services used to move the information (means).
  - Places hyperlinks to input/output formats in a spreadsheet or web part.
  - This serves as the one stop reference for exchanging the MAGTF's information, to include report formats.
- Coordinate with the G/S-6 to Deconflict Authorities to Connect, Ports, Protocols, and Firewalls:
  - Ensures all warfighting and staff function systems are identified for inclusion in G/S-6 planning cyber documents.
  - Relies on the handoff of the C2 systems and software baseline.
  - The IKMO provides MAGTF-related ports and protocols to the G-6.
  - The G-6 coordinates with HHQ, adjacent, and supporting units that require opening of ports, protocols, and firewalls to enable communication pathways.

- Construct the Information and Knowledge Management Annex (Annex U):
  - Defines the IKM infrastructure.
  - Provides relevant information to users specific to the operation and for technicians to install, operate and maintain IKM and C2 services.
  - Articulates the business rules of protocols, shared situational awareness, collaboration services, and process solutions routine or unique to the mission.

Brief and Train the Staff

Completion of these actions is critical to mission success:

- Provides the details unique to the knowledge architecture and guides staffs in how to operate within it.
- The IKM and G-6/S-6 brief to the staff - network and C2 and software terrain.
- Review battle rhythm events, key tools and process automations being employed and how they work.
- Identify critical events in the IMLC, along with where and how information and knowledge is managed during key phases of the operation/exercise.
- Explain the IKM service request process.

Prepare for Operations

- Systems and services are technically ready at the communications rehearsal exercise.
- The IKMO requests group policy object pushes for both browser re-direction and the IKMO smart pack also known as a SmartPak. A SmartPak is a pamphlet which contains point of contact information, answers to frequently asked questions, common procedures, and important information about a command, unit, section etc.
- Figure B-5 is example of a IKMO SmartPak (it is spelled this way to differentiate it from other functional area smart packs) it provides users essential IKM information to connect to various IKM C2 applications or relevant locations.
- Confirm functional area IKM exchange takes place between higher adjacent and subordinate commands at information flow exercises (also known as INFOFLOEX), as applicable.
- Establish the IKM watch team, dets and support to subordinate commands.
- Transition to battle rhythm management and IKM infrastructure oversight.
- Capture IKM performance metrics.

UNCLASSIFIED

Online Conference Rooms

Root URL:
Add The Conference Room to the Root URL
Conference Rooms
– Ops & Intel Brief:
– Planners Update:
– Logistics Coordination Working Group:
– Information Operations Working Group:
– ROE & Authorities Working Group:
– Collections Management:
– G3 MSC Sync:
– C4I Coordination Working Group:
– Planner's Working Group:
– Comm Strat CCS Working Group:
– Cyber Working Group:
– Engineering Working Group:
– Targeting Working Group:
– Targeting & Effects Board:
– Targeting Cell:
– Aviation Coordination Working Group:
– Electromagnetic Spectrum Operations:
– Surgeon's Sync:
– FOPSCOP Cell:
– Force Protection Working Group:
– IMKM Working Group:
– Transportation Working Group:
– Assessment Working Group:
– Assessment Board:
– Manpower Working Group:
– Material Readiness Working Group:
– G2 MSC Synch:
– DOT Working Group:

AMERICAN SITE

All instructions for IM Service access are the same as those described in the interior of this trifold with the following exceptions:

– SharePoint
Enter SharePoint simply by using the following URL LINK.

– Tactical Chat: Using MAKO Client
Use Fwd/Main Tactical Chat Guide.

– C2PC
Set time with UB Host Timebase (XX X XX XX) to ensure Track and Overlay transfer.
- Select time.
- Select Options → Protocol → SNTP.
- Enter XX X XX XX → OK.
- Click "Query Timebase" & Correct System Clock.
- The system time will sync with the TCS to allow passage of tracks and overlays.

– C2PC Web
Open browser and enter the following:
- https://xx xx xx xxxx/C2PC web.
- Enter the username and password you received from the CPSA.
- WEBCOP will be view only and is accessible from any SIPR TIE workstation.
- Contact the CPSA on the COC floor for access information.

– II MEF Fwd IM SERVICE DESK (IMSD) INFO
Service Desk personnel will be located in the G-6 tent and can be reached via chat at **#MEF_IMO**.

To submit a service request, select the "**IMO Service Desk**" link on the TIE SIPR SharePoint portal.

IM Service	P	A	C	E
CWS	SP	E	P	J
Chat (C)	MAK	P	E	FtoF
COP (WebCOP)	TIE S	P	NA	NA
Web Conf	SP	P	NA	NA
INFORMATION EXCHANGE MEANS				
SP-SharePoint, J-MAKO COP-Common Operational Picture (WebCOP), E-Email, P-Phone, FtoF-Face to Face				
P-Primary, **A**-Alternate, **C**-Contingency, **E**-Emergency				

UNCLASSIFIED

Figure B-5. Information Knowledge Management SmartPak Example.

Appendix C.
Information and Knowledge Management Plan

An IKMP is developed to augment a tactical SOP and command staff regulations and govern IKM planning within a command. It describes the purpose and objectives of IKM, identifies all major participants, identifies the framework, and assigns tasks associated with the execution of the IKMP. The following example shows one format of an IKMP that can be configured for use by any specified size of command.

UNIT HEADING

IN REPLY REFER TO:

SSIC

IKMO

10 Nov XX

UNIT ORDER XXXX.XXX

From: Commanding Officer

To: Distribution

Subj: UNIT INFORMATION AND KNOWLEDGE MANAGEMENT PLAN

Ref: (a) Directive 5010.42, DoD Wide Continuous Process Improvement.

(b) CJCSI 3151.01, Global Command and Control (C2) System Common Operational. Picture (COP) Reporting Requirements.

(c) CJCSI 5870.01, Joint KM Program.

(d) Insights and Best Practices Focus Paper – Chief of Staff Functions at a Joint Headquarters.

(e) JP 3-33, Joint Force Headquarters (2022).

(f) JP 6-0, Doctrine for C4 Systems Support to Joint Operations.

(g) JP 6-02, Joint Doctrine for Employment of Operational/Tactical C4 Systems.

(h) Department of the Navy Knowledge Management Strategy.

(i) NAVMC 3500.54F, Command and Control Training and Readiness Manual.

(j) MARFORCOM Order 5224.1B, Continuous Process Improvement Program.

(k) Marine Corps Information Knowledge Management Strategic Guidance, dtd 1 Oct 2024.

(l) MCDP 6, Command and Control.

(m) MCDP 8, Information.

(n) MCTP 3-30B, Information Management.

(o) MCRP 3-40.2B, Multi-Service Tactics, Techniques, and Procedures (MTTP) for Internet Tactical Chat in Support of Operations.

(p) MCWP 3-30, Marine Air-Ground Task Force Command and Control.

Encl: (1) Staff Section Mission-Essential Tasks.

(2) Staff Section Information Requirement.

(3) Plan of Action and Milestones.

(4) Systems Usage and Training Requirements.

1. Purpose. This order provides planning guidance and direction to all staff sections with regard to execution of the IKMP. Per the references, the unit will develop and execute an IKMP that captures how the command manages and controls information.

2. Scope. This order constitutes the primary planning document for the IKMP. It describes the purpose and objectives of the IKMP, identifies all major participants, identifies the IKMP framework, assigns tasks associated with the execution of the IKMP, and provides general information regarding the execution of the IMP.

3. Mission. The unit IKM office establishes and maintains required IKM procedures to facilitate the sharing of information and knowledge throughout the command as cited in the IKM office's METs.

a. Provide command information process support.

b. Create executive decision support tools, when directed.

c. Establish and maintain access to C2 systems.

d. Establish and maintain a common operational picture or common tactical picture.

e. Provide for staff information exchange.

f. Establish and maintain a collaborative services environment.

4. Execution

a. Commander's Intent

(1) Purpose. Unit XX will use the IKMP to aide in identifying functional essential tasks, processes, and required systems training necessary to maintain a common IE during routine operations and during predeployment, deployment, redeployment, and post-deployment periods. The deploying unit will be governed by reference (p) and specifically the exercise or operation order, of which Annex U is an essential part.

(2) Method. Unit XX will increase the speed of the commander's decision-making cycle by creating an IE that links operational and administrative information using standardized formats and optimized processes, enabled by existing systems and applications. Unit XX IKMOs and KMR will—

(a) Develop an operational information architecture.

(b) Facilitate internal and external information exchange requirements.

(c) Resolve IKM training shortfalls to provide timely, analyzed, and relevant information to the commander, optimizing this cycle. This method will support the following IKM objectives:

1 Create a culture that establishes IKM as a matter of practice.

2 Support command and functional area IER.

3 Simplify information flow by developing and refining processes and procedures.

4 Generate high-quality information through the use of standardized input and output formats and templates housed within Unit XX's information management matrix.

(3) End State. The end state is to meet the commanding officer's IKM requirement for an agile decision-making cycle and optimized operational performance.

b. Concept of Operations. Staff sections shall ensure that they follow the steps detailed herein to determine their mission-essential tasks (METs) in support of Marine Corps tasks. Results of this activity are used to assist in determining IKM systems requirements. The process is similar to the IKM planning process described in Appendix B; however, Appendix B is intended for operational planning after completing the sequence of actions listed here:.

(1) Identify METs. The identification of functional METs allows a staff to readily identify critical events necessary to successfully accomplish the functional area's mission while identifying, evaluating, and analyzing the information requirements essential to accomplish each MET.

(2) Identify Supporting Information Requirements. Section information requirements are derived by performing mission analysis of a section's METs and answering the question, "what information requirements are required to achieve this MET?" An information requirement can be addressed either by a process or a system that identifies the piece or pieces of information, the entities the information exchanges between, and the means by which that information travels. Once all information requirements have been identified, staff sections validate and prioritize current processes in descending order as critical, essential or enhancing as it relates to a MET's accomplishment.

(3) Define the Information Requirements Process. The process refers to the inputs, actions, and outputs to complete an identified information requirement. Furthermore, assess processes to determine whether improvements may be applied to save time or eliminate waste. Improvements can be in the form of a process modification, training solution, personnel augmentation, or use of a system or technology.

(4) Identify Enabling Systems and Applications. To facilitate the collation, coordination, dissemination, and retrieval of information requirement inputs and outputs, identify the system(s), application(s) and collaborative service(s) used for each information requirement.

(5) Identify Training Requirements. Based on action (4), proper use of systems and applications across functional staffs must include a sufficient number of qualified operators. The information requirements identified are the basis of the IKMP training table found in enclosure (2). The IKMWG will also evaluate the commercial sector for innovative training opportunities, when required.

(6) Identify IKM Gaps. To identify IKM gaps, the staff must review METs and information requirements and identify which information requirements have not been resolved. Once an IKM gap is identified and forwarded to the IKMWG, the IKMWG will determine if the gap can be filled with resources internal to the command. If the gap cannot be addressed internally, then the IKMO will coordinate with outside agencies to assess alternatives.

(7) Train. Training remains a continuing action to ensure sufficient number of qualified personnel are in place as IKMOs, C2 systems operators, and file-sharing site managers to provide and perform functional IKM related tasks.

5. Tasks

a. Chief of Staff/Executive Officer

(1) Ensure effective mechanisms are in place to transition raw data into actionable knowledge in support of the commander.

(2) Act as reporting senior for the command IKMO.

(3) Chair the IKM Board.

(4) Own the command battle rhythm.

(5) Direct staff compliance with the IKMP.

b. Information Knowledge Management Officer

(1) Publish the IKMP.

(2) Coordinate training scheduling with S-3, Marine Corps resources, required civilian organizations, and sections.

(3) Schedule and chair the IKMWG comprised of staff KM representatives, major subordinate command IKMOs, and mission partner IKMOs.

(4) Schedule and facilitate IKM boards for the XO, to discuss progress of predeployment IKMP.

(5) Track progress of IKMP development and execution.

c. S-3 Officer (Operations)

(1) Provide a staff noncommissioned officer to serve as IKM chief.

(2) Serve as the co-chair of the IKM board.

(3) Have the section KMR participate in the IKMWG.

(4) Ensure IKM training events are added to the training, exercise, and evaluation plan.

d. S-4 Officer (Logistics)

(1) Coordinate fiscal requirements in relation to civilian IKM training requirements.

(2) Have the section KMR participate in the IKMWG.

(3) Ensure IKM training events are added to the training, exercise, and evaluation plan.

e. S-6 Officer (Communications System)

(1) Serve as the assistant IKMO and co-chair of the IKMWG.

(2) Coordinate with the IKMO in the establishment of an IKMP.

(3) Have the section KMR participate in the IKMWG.

(4) Provide communication estimates of supportability for IKM requirements identified by the IKM board.

f. Information Management Chief

(1) Serve as collaborative service manager.

(2) Coordinate website external support.

(3) Verify tactical chatrooms comply with the chat plan.

(4) Confirm battle rhythm website conference rooms remain functional.

(5) Assist the IKMO and assistant IKMO.

(6) Supervise the IKM augments and contractors in the execution of their duties.

g. All Staff Sections and Special Staff

(1) Develop section IERs.

(2) Provide an officer or staff noncommissioned officer to serve as KMR.

(3) Identify in writing a section information support coordinator.

(4) Identify system and process training requirements.

(5) Identify specific training requirements for section-specific information requirements.

(6) Coordinate specific training for sections with the appropriate training resource.

6. Coordinating Instructions

a. Ensure that appropriate personnel attend required training.

b. Have the staff primary or deputy attend the IKM board.

c. Coordinate with functional system representatives to identify support requirements and resource availability.

d. Make maximum use of the collaborative workspace (portal).

(1) Document libraries

(2) Calendars

(3) Lists

(4) Linked lists

(5) Static content.

e. Leverage website conferencing, which includes integrated chat, application sharing and screen casting, voice and audio communication, and presence and awareness.

7. Administration and Logistics. Omitted.

8. Command and Signal. Omitted.

IM N. CHARGE

Staff Section Mission-Essential Tasks

The MET areas in Table C-1 are examples of staff responsibilities when producing and managing information products related to their functional areas.

Table C-1. Example Mission-Essential Task Checklist.

Section	Mission-Essential Task
S-1 (Administration)	Provide personnel accountability. Conduct personnel administration. Manage the command's personnel casualty report.
S-2 (Intelligence)	Provide intelligence updates as required to reduce uncertainty and provide for force protection. Track and manage security clearances and isolated personnel reports. Track, manage, and maintain updated intelligence-specific classified documents and geospatial information and services holdings. Provide timely intelligence support for all mission types.

Table C-1. Example Mission-Essential Task Checklist (Continued).

Section	Mission-Essential Task
S-3 (Operations)	Plan, coordinate, and execute all operations and exercises. Plan, coordinate, and document command element training. Manage and execute the rapid response planning process and deliberate planning process. Conduct coordination, planning, training, and execution of all fires. Conduct planning and coordination of aviation in support of exercises and operations. Provide and maintain and operations center capable of planning, executing, and coordinating with higher, adjacent, and subordinate units. Conduct training and develop, maintain, and disseminate a COP. Provide operational support to the forward command element. Provide COMMSTRAT assets for documentation of training and operations. Compile and disseminate operational reporting and commander's brief Provide a MAGTF assessment and consequence management set Provide detection, identification, and decontamination package. Provide accurate readiness status report. Develop, coordinate, and manage time-phased force deployment data. Develop, coordinate, and manage the ammunition allocation plan. Manage and maintain the unit historian program. Manage and maintain a safety awareness program. Provide, develop, and implement a force protection plan.
S-4 (Logistics)	Plan and coordinate internal and external combat service support. Prepare logistic and combat service support plans, orders, and letters of instruction. Provide contracting support. Manage budget. Manage supply warehouse. Manage hazardous waste and hazardous materials program. Provide armory support to command element. Provide precision weapons armorer support. Prepare load plans. Identify and validate lift requirements. Manage ammunition account. Manage ground equipment readiness.
S-6 (Communications)	Conduct communications planning, engineering, and supervision for assigned Marine Corps and other Service communications elements. Plan, install, and operate wideband data and voice services. Plan, install, and operate single-channel radio circuits. Develop communication plans and orders. Coordinate support to higher, adjacent, and subordinate command communications system requirements. Support communication requirement to C2 nodes. Exercise management of the tactical network. Publish communication electronic operating instructions. Provide communication support to the forward command element. Provide secure data and voice capability for liaison elements. Provide Global Broadcast Service. Provide electronic management key system support. Protect information systems.

Table C-1. Example Mission-Essential Task Checklist (Continued).

Section	Mission-Essential Task
Staff Judge Advocate	Provide command legal advice to the commander regarding international law, military justice, and fiscal law. Advise commander and staff on legal issues related to release of information. Assist command with conduct, processing, and storage of investigations. Advise commander on the law of war and rules of engagement. Train personnel on the law of war and rules of engagement. Investigate and process foreign claims. Provide legal assistance to eligible personnel.
Medical	Provide force health protection. Provide health service support. Support casualty evacuation.
COMMSTRAT	Provide visual information support to military information support operations (also known as MISO). Provide visual information support to military operations in the information environment. Conduct communication strategy and operations actions: • Conduct research. • Provide counsel. • Plan. • Conduct engagement. • Create products. • Disseminate products. • Assess and evaluate efforts. Conduct issue management. Conduct crisis communication.
Chaplain	Coordinate religious ministry services. Manage American Red Cross message handling. Coordinate and manage special programs. Affect suicide prevention. Act as advisor for family readiness.
IKMO	Establish and maintain a functional IKM program. Implement and complete the formal IKM planning process. Coordinate the scheduling of IKM training as required. Provide information process support. Develop executive decision support and performance support solutions. Establish and maintain command shared situational awareness. Provide for the staff's information exchange. Establish and maintain a command collaborative environment. Assist subordinate unit IKMOs with IKM requirements.

Staff Section Information Requirements Table

Staff section information requirements are derived by performing mission analysis of a section's METs and are recorded in the staff section information requirements table as shown in Table C-2. Table C-3 is an example of a systems usage and training requirements matrix.

Table C-2. Staff Section Information Requirements Table.

STAFF SECTION NAME HERE			
Assigned Mission-Essential Tasks			
List the department's assigned mission-essential tasks here			
Information Requirement	**Action Officer**	**Process, Inputs and Outputs**	**Supporting System or Application**
List all IRs in order of priority (mission critical, mission essential, or mission enhancing) to accomplish, achieve, and meet the MET.	Who identifies and completes the IR? List by billet title.	What are the actions required to obtain and achieve IRs? What information templates or forms are used for providing inputs or receiving outputs to this process? Where or to whom is the product delivered?	List all program of record systems or web based applications used in acquiring, collating and transmitting the IR data. List application name and network (AFATDS-SIPR)
Legend IR information requirement			

Table C-3. Example System Usage and Training Requirements Matrix.

LEGEND 1 - Training Required 2 - Training within Unit 3 - Training outside Unit	S-1	S-2	S-3	S-4	S-6	IKM	Com Strat	HSS	SJA	Chap	FRO
DCIPS	1										
MOL	2	2	2	2	2	2	2	2	2	2	2
MCTFS	1										
DMM	1										
IDMS	1										
MCMPS	1										
TFMS 2.0	1										
ETMS2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1,2
IAPS	2	2	2	2	2	2	2	2	2	2	2
DFAS/MY PAY	2	2	2	2	2	2	2	2	2	2	2
MROWS	1										
DTMS	1										
MARINE NET	2	2	2	2	2	2	2	2	2	2	2
CMS-ID	1										
TOPS	1										
NDAWS	1										
Navy SWANK LMS	1										
CLA	1										
DAI	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1,2	1,2
DCPS	1										
DCPS REMEDY	1										
DCPDS	1										

Appendix D.
Annex U (Information and Knowledge Management)

Annex U is focused on supporting a MEF-level MAGTF, but the same principles are applicable for all commands. A unit's IKMP serves as the basis for developing and building an Annex U in support of operations and exercises. Various components of an Annex U might not be indicated because they are referenced in the unit's IKMP or tactical SOP (TACSOP), while others are inserted from the IKMP or TACSOP and configured for the specific mission.

CLASSIFICATION

Copy no. of copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

ANNEX U TO XX MARINE EXPEDITIONARY FORCEOPERATION ORDER 10-01 (U)
(U) INFORMATION MANAGEMENT

(U) REFERENCES:

(a) XX MEF Tactical Portal: http://www.xxmef.usmc.smil.mil
(b) TACSOP, current operations, XX MEF (Annex C)

(1) Time Zone:

1.(U) Situation

a. (U) General. This annex provides guidance on processes and procedures for information management in support of XX MEF. It promulgates concepts, assigns responsibilities, and provides planning guidance for all XX MEF forces and joint or coalition forces operational or tactical control to XX MEF. All IKM planning and execution will be in accordance with references (a) and (b) except as noted in this annex.

CLASSIFICATION

b. (U) Enemy

(1) (U) See Annex B (Intelligence).

(2) (U) Forces and nations in the XX MEF area of operations have the capability to:

(a) (U) Employ collection systems and means to record and analyze clear-voice coalition force communications.

(b) (U) Collect, aggregate, analyze, and disseminate information from publicly accessible websites, compromised NIPRNET websites, and compromised publicly accessible mail servers. The threat to coalition networks continues to be determined in theater by the G-6.

c. (U) Friendly. See Annex A (Task Organization).

(1)(U) Command Relationships. See Annex J (Command Relationships).

(2)(U) Attachments and Detachments. See Annex A (Task Organization).

2.(U) Mission. See base order.

3.(U) Execution

a. (U) Concept of Information Management. The purpose of information management is to provide the commander and staff accurate, relevant, and timely information to effectively command and control forces to accomplish the assigned mission. Many information processes are specific to a warfighting function, but there are many others that are shared across the staffs. In both cases XX MEF will use common IM processes to maximize the information pipeline for increased accuracy, timeliness, and relevancy of information to include coalition partners. This includes the specific processes and systems governed by IKM personnel.

(1) (U) In general, tasks of the IKM architectures, tools, and processes for (MISSION NAME) will continue to provide essential IERs for ongoing operations. These tasks, while decentralized in execution, must be closely coordinated with higher, adjacent, and subordinate units already in place. Additionally, XX MEF will be prepared to geographically transition current bases and forward operating base locations and command, control, communications, and computers system support within the area of operations when directed.

CLASSIFICATION

(2) (U) Geographic Transition. Any realignment of forces requiring the transition of existing C2 architectures and systems will require planning, coordination, and preparation with XX MEF. Units will exercise the principles of redundancy and the tenets of passing control when geographic transitions are directed and can accept, as directed by HHQ, to ensure uninterrupted C2 architecture is maintained at all times.

b. (U) General Guidance

(1) (U) Tactical Data Networks. Four tactical data networks will be the primary internet protocol wide-area networks employed during this campaign: SIPRNET, NIPRNET, CSD [Common SIPRNET Domain], and other coalition networks.

(a) (U) SIPRNET. Provides classified connectivity to the SIPRNET down to end users.

(b) (U) NIPRNET. Provides connectivity to NIPRNET and the Internet.

(c) (U) CSD. Provides filtered connectivity via SIPRNET to Secret//Rel USA, AUS, CAN, GBR/.

(d) (U) Other coalition networks as required by the CCDR, which provide connectivity among coalition forces in the theater, including virtually all coalition forces.

(2) (U) Common Operating Picture Management. XX MEF will maintain appropriate command and control nodes for the COP. For information on the COP, see Appendix 3.

(3) (U) XX MEF Portal. XX MEF internal and external portals will be integrated, maintained, and managed by the IKMO in concert with XX MEF staff section content managers. A separate site will be used for segregating NOFORN [Not Releasable to Foreign Nationals/Governments/Non-US Citizens] material. See Appendix 4.

(4) (U) Collaborative Systems. These collaborative systems will be managed by the IKMO. See Appendix 4.

(5) (U) Software Versioning. XX MEF Tactical Systems Software has been baselined with HHQ and service chains. Changes to the XX MEF baseline are not authorized unless coordinated through the XX MEF IKMO. Tactical software includes software fielded with all systems of record as well as critical commercial off-the-shelf software. Software that is currently authorized for limited user evaluations may not be distributed beyond those users without coordination with the XX MEF IKMO or authorization from HHQ. New applications will be vetted through the Information Management Working Group and approved by the Information Management Board prior to deployment in XX MEF networks to limit the tasks associated with maintaining additional applications that are not part of a program of record. See Appendix 5 for a detailed list of software and versions.

CLASSIFICATION

(6) (U) Coalition Information Sharing. In the event a coalition unit is assigned operational and tactical control to XX MEF, the following guidance applies: enabling command and control of a subordinate unit from a different nation (higher to lower) is a bilateral responsibility; subordinate units should coordinate through an assigned liaison officer for all efforts to enable C2 information sharing.

(a)(U) Responsibilities from a command to an adjacent unit from a different nation is the responsibility of both units. Both commands are responsible for terminating their communications circuits at the other command. Where liaison teams are required, both commands will provide liaison team personnel and appropriate communications systems.

(b)(U) The foreign disclosure officer will approve disclosure or release of applicable information.

(7) (U) Properly Classifying Information, Information Security, and Operational Security.

(a)(U) The baseline classification for classified information is SECRET// REL _ _ _//FOR VIEW BY (coalition partners). Whenever appropriate, using this level of classification provides the widest dissemination to forces within the area of operations. All units must be familiar with changes to the proper classifications of classified material to ensure effective information flow among (coalition partners) personnel. Specifically, units should understand the distinction between SECRET; SECRET//REL USA, AUS, CAN, GBR/; and SECRET//REL _ _ _//FOR VIEW BY (coalition partners).

(b)(U) Maximum use will be made of information security and operational security policies and procedures detailed in Annexes K and Y to prevent disclosure of vital information to opposing forces. Message classification software is used by XX MEF to assign appropriate level information classification for email traffic. All units must ensure incident response and reporting capability is established to comply with XX MEF G-6 cyber security policies.

(8) (U) Common Systems and Processes. XX MEF units will maintain commonality of IKM processes and systems to the greatest extent possible, balanced by the information requirements throughout all phases of operations. See Appendix 5.

c. (U) Tasks and Responsibilities

(1) (U) XX MEF Staff Directorates.

(a) (U) Ensure IKMO is assigned (primary or collateral duty) and that the IKMO reports the following to the XX MEF IKMO: contact information, unique requirements for IKM or C2 system technical support for the section, and staff organization. Ensure the IKMO coordinates IKM-related plans, SOPs, and orders.

(b) (U) Coordinate any external emerging website or C2 system support requirements with the Science and Technologies section and the IKMO.

CLASSIFICATION

(2) (U) XX MEF IKMO

(a) (U) Develop and publish guidance on IKM and staff action processes for the operations and maintenance of the XX MEF COP architecture, XX MEF portal, command journal, and other web-based tools in accordance with reference (b) and as directed by the Commanding General, XX MEF. See Appendix 5.

(b) (U) Provide directive guidance on C2 systems within XX MEF to ensure synchronization and integration for staff and MSCs. See Appendix 5.

(c) (U) Provide guidance on the best methods to exchange data between systems using multiple networks to include SIPRNET, NIPRNET, Common SIPRNET Domain, and other coalition networks.

(d) (U) Provide technical support personnel, including deployed contractors, to support C2 systems and information systems as required.

(e) (U) Establish a website development section to support XX MEF headquarters and all XX MEF units that require web-based support services.

(f) (U) Provide XX MEF portals as required.

(g) (U) Review all subordinate supporting IKM annexes developed in support of this order.

(h) (U) Conduct Information Working Groups with the MSC IKMOs, and MEF Staff KMRs.

(3) (U) General Tasks for XX MEF Subordinate Commands. These tasks are directed to ensure rapid integration and continuing interoperability of XX MEF forces.

(a) (U) Install, operate, and maintain C2 systems in accordance with the information presented in this annex.

(b) (U) Assign a unit IKMO (as a primary duty for regiment-sized elements or collateral duty for battalions). The unit IKMO will report to the XX MEF IKMO with contact information; unique requirements for IKM or C2 system technical support; unit task organization; and IKM plans, SOPs, and orders.

(c) (U) Participate in the IKMWG and other scheduled or on-call events Public shed by XX MEF IKMO.

CLASSIFICATION

(d) (U) Act as functional area manager for C2 and information systems communities of interest identified in Appendix 5.

(e) (U) Establish and maintain a tactical portal or coordinate for the use of a supported/supporting unit portal per Appendix 5.

(f) (U) Maintain an online web-based command journal or coordinate for the use of a supported/supporting unit command journal. A command journal will be displayed on each MSC's primary tactical portal or supported/supporting unit portal.

(4) (U) Specified Tasks

(a) (U) Aviation Combat Element

1 (U) Act as alternate command post.

2 (U) In addition to standard C2 architecture, establish and maintain a mid-tier server capability for C2 systems as required.

3 (U) Be prepared to conduct and support C2 system software and hardware upgrades to include units within the task organization.

(b) (U) Logistics Combat Element

1 (U)Serve as an intermediate-level node for IKM flow and C2 systems architecture.

2 (U)In addition to standard C2 architecture, establish and maintain a mid-tier server capability for C2 systems as required.

3 (U)Be prepared to conduct and support C2 system software upgrades to include units within the task organization.

(c) (U) Ground Combat Element

1 (U)Identify and coordinate any Service-specific requirements necessary to integrate Army Battle Command Systems as required.

2 (U)In addition to standard C2 architecture, establish and maintain a mid-tier server capability for C2 systems as required.

3 (U)Be prepared to conduct and support C2 system software and hardware upgrades to include unit within your task organization.

CLASSIFICATION

(d) (U) Additional MSCs and MSEs

1 (U) In addition to standard C2 architecture, establish and maintain a mid-tier server capability for C2 systems as required.

2 (U) Be prepared to conduct and support C2 system software and hardware upgrades to include units within the task organization.

d. (U) Coordinating Instructions

(1) (U) The Information Management Working Group, which consists of all XX MEF unit IKMOs and/or information managers, will convene bi-monthly. Additional sessions may be scheduled as required and will be published via e-mail and in the XX MEF Daily Battle Rhythm. See Ref (b) TACSOP.

4.(U) Administration and Logistics. Refer to Annexes E and D, respectively.

5.(U) Command and Signal. Units assigned as alternate command posts or in the succession of the chain of command shall maintain the ability to provide C2 system support and information resources to the extent required to carry out succession of command or activation of an alternate command post. Each MSC is responsible for providing its own Continuity of Operations Plan and data recovery capability.

ACKNOWLEDGE RECEIPT

I. A. MARINE
Lieutenant General, USMC
Commanding

APPENDICES:
1—Information Management Lifecycle
2—Battle Rhythm Management
3—Common Operational Picture (COP)
4—Command and Control (C2) Systems
5—Collaborative Systems Services
6—Digital Business Rules
7—Process Automation Tools
8—Information Knowledge Management Service Desk (IKMSD)

OFFICIAL:
s/
U. R. MARINE
Colonel, USMC
Chief of Staff

Page Number
CLASSIFICATION

CLASSIFICATION

Copy no. of copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

APPENDIX 1 TO ANNEX U TO OPERATION ORDER XXX-XX
INFORMATION MANAGEMENT LIFECYCLE (U)

1. (U) Purpose. To more effectively meet information needs, XX MEF and its MSCs must recognize that information management (IM) requirements will vary cross functionally as the operation unfolds. A lifecycle approach to information and knowledge management during this exercise has several advantages. First, it permits information managers to recognize and effectively focus critical IM tasks in each phase of the exercise lifecycle, as well as anticipate key information needs of the next phase. Secondly, it allows IKMOs to identify and analyze information exchange requirements throughout the various phases of the lifecycle to better focus and manage information flow through the proper processes, use of correct formats found in the IM matrix and ensuring information sharing of events takes place by routing through the appropriate collaborative services.

2. (U) Phases. The phases for OPERATION X and the IMLC are located in Annex C.

TABS:

A—IMLC Table
B—IMLC Tasks and Information Requirements, by Phase.

Page Number
CLASSIFICATION

CLASSIFICATION

Copy no. of copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

TAB A TO APPENDIX 1 TO ANNEX U TO OPERATION ORDER XXX-XX (U)
INFORMATION MANAGEMENT LIFECYCLE (U)

1. (U) Purpose. To provide a guide to key IKM events during the conduct of OPERATION X requiring IKMO coordination and visibility to ensure successful information exchange and collaboration to complete the specified task(s), while recording and reporting its completion.

2. (U) IMLC Table. The following table describes IMLC events.

Information Mangagement Lifecycle.

Planning	Pre-deploy	Deploy	Employ	Transition	Redeploy
Appoint IKMO	Activate IM Board	Ensure in transit visibility of resources	Execute Annex U		Ensure in transit visibility of resources
Conduct IKM Planning Process	Activate IKM Working Group (IKMWG)	Run IKMWG	Run IKMWG	Complete final backup of all data files	
Prepare Collaborative Workspace and C2 Systems	Coordinate IKM Training for ALCON	Conduct Battle Rhythm Rehearsal	Oversight of Battle Rhythm and IMLC Mods and Execution	Finalize File and Record X-fer Plan	Execute File and Record X-fer Plan
Establish RFI tracking tool	Establish Electronic CMD Journal	Tool for managing CCIRs	Coordinate for File and Record X-fer	Place AAR tool online	
Meet with All Site Managers	Coordinate with S-3, S-6				
Oversee CTP development	Develop Annex U	Complete/Issue Annex U	Manage IKM Service Requests	Preserve and Secure all POR and app files	

CLASSIFICATION

Copy no. of copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

TAB B TO APPENDIX 1 TO ANNEX U TO OPERATION ORDER XXX-XX (U)

INFORMATION MANAGEMENT LIFECYCLE TASKS AND INFORMATION REQUIREMENTS BY STAGE (U)

1. (U) Purpose. To identify specific information exchange requirements to be used during each phase of OPERATION X to focus and manage information flow to ensure MAGTF-wide visibility, based on need to know, to complete the specified task(s), while recording and reporting phase completion.

2. (U) IMLC Table. Key IKM events by phase for OPERATION X are provided in the following table.

Key Tasks and Information Requirements by Stage.

Stage A	Stage B	Stage C	State D	Redeploy	Reconstitute
Info Exchange (IE) for onload via DTCS radio and TAK	Conduct IE with ESG to synch on amphib action via CAS and ESG TAC chat	ICW ESG, NLT X, establish an AOA IVO XXX, via ESG TAC chat, CAS, SPO	Validate IERs for JISR and Joint targeting ISO TF Jagged Edge	Complete backup of SIPR, Coalition CS	Report full recovery and accountability of IKM sensitive items via #MEF_ C2SYS_SPT
Validate info exchange w/ deploying elements	Conduct IE to manage MEF Deep Area via TAK and #MEFTAC chat	Report aggression and incursion via #MEF_COC chat	Exercise PACE btwn ESG and MAW IOT to prep for DATF		Confirm Staffs posted and can locate/access key files
Establish CTP links with ESG and AAOG	Establish IE to coordinate ISR and support targeting via SCR		Coordinate plan for orderly shutdown of C2 and CS services		Ensure IAPS is accessible
Coordinate w/G-3, G-6					
Confirm CMD journal fully operational				Ensure AAR tool is operational	
Ensure in transit visibility of resources via LOG and TPFFD				Ensure in transit visibility of resources via LOG and TPFFD	

CLASSIFICATION

Copy no. of copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

APPENDIX 2 TO ANNEX U TO OPERATION ORDER XXX-XX (U)
BATTLE RHYTHM MANAGEMENT (U)

1. (U) Purpose. This appendix provides the MEF staff a daily sequence of events necessary to support the Commander's monitor, assess, planning, and decision, and execution cycle.

2. (U) General. While the MEF daily battle rhythm is the responsibility of the MEF Chief of Staff (C/S), the Information Knowledge Management Officer (IKMO) or his delegate provides daily oversight of daily battle rhythm execution and adjustments, when required. The current daily battle rhythm can be viewed on the SIPR collaborative workspace (CWS). See the IKMO SmartPak for the location of the CWS.

a. (U) The battle rhythm is not to be confused with daily schedules published by the C/S or staff sections. Daily schedules depict specific events and activities such as VIP visits and section activities.

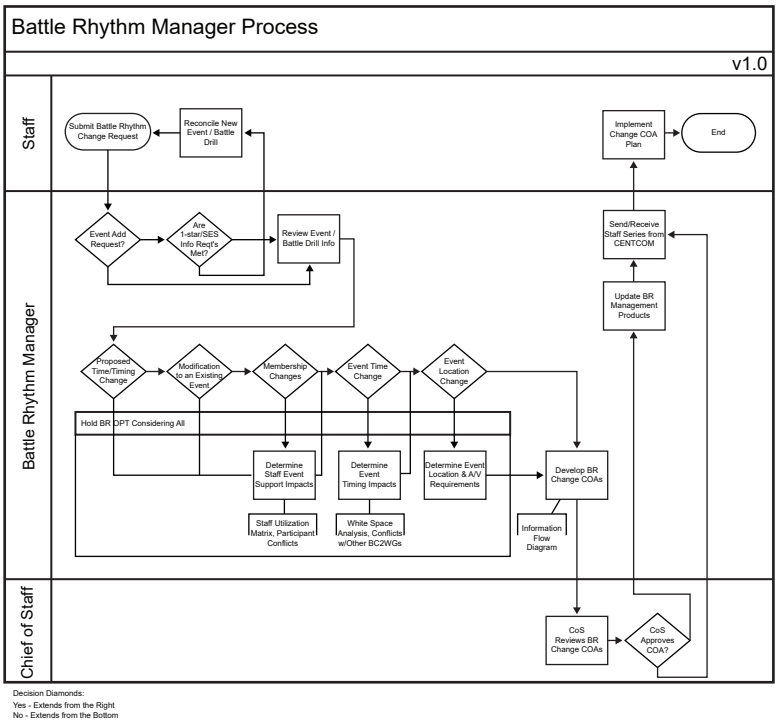
b. (U) The battle rhythm will be closely coordinated across the staff and serve as the foundation for BC2WGs.

3. (U) Procedures

a. (U) The MEF OPERATION XXX battle rhythm is approved by the C/S and posted to the MEF SIPRNET homepage and maintained by the X MEF IKMO. Staff section KMRs who require updates to the battle rhythm must submit their request and updated 7-minute drill to the IKMO via the Information Knowledge Management Working Group (IKMWG).

b. (U) Staff sections will participate in various BC2WGs as indicated in the daily battle rhythm. Each staff section is responsible to ensure their key information products are posted and maintained on the MEF homepage in accordance with the daily battle rhythm.

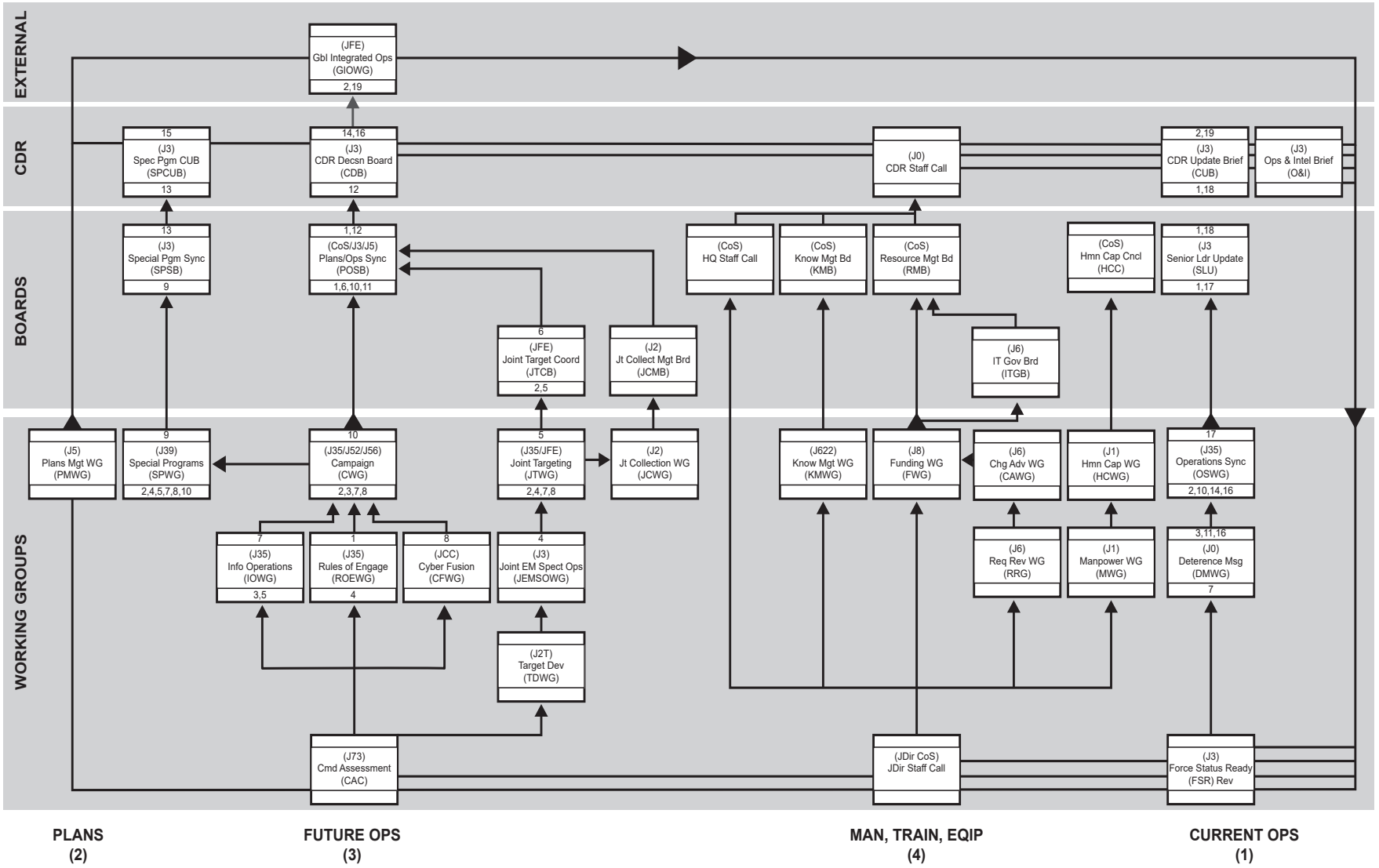
4. (U) Battle rhythm change management. The C/S is the approval authority for permanent changes to the daily battle rhythm. Daily modifications (e.g. one-time delay of an event to accommodate an unscheduled event) will be distributed via email. Refer to the Battle Rhythm Change Process for details on the MEF OPERATION XXX battle rhythm change process.



Battle Rhythm Change Management Process.

Battle Rhythm Time Synch Matrix.

Time	HHQ	MEF
0600	ATO Executed	
0700		
0800		
0900		
1000		
1100		
1200		
1300		
1400		
1500		
1600		
1700		
1800		
1900		
2000		



Battle Rhythm Information Flow Diagram. (Click to Enlarge.)

OPERATION XXX BATTLE RHYTHM STAFF UTILIZATION MATRIX																									
7-Min Drill	Assessment Board	Assessment WG	Aviation Coordination WG	C4I Coordination WG	CG's LNO Sync	CG's Planners Update Brief	Chief of Staff Huddle	Collections Management WG	COMMSRAT Communication Sync WG (CCCS)	Cyber WG	DOT WG	EMSO	Engineer WG	FOPS/COPS Cell	Force Protection WG	G2/MSC G2 Sync	G3/MSC G3 Sync	IKMWG	IO WG	Log Coordination	Manpower WG	Material Readiness WG	Ops and Intel Brief	Planners WG	ROE & Authorities WG
Chair:	CG/CoS	MEF G3	MEF G3	AC/S G6	MEF Commander	MEF Commander	CoS	G2	MEF CoS	G39 Information Operations Officer	II MEF Force Deployment Officer	G39 Space Operations Officer	II MEF Engineer	FOPSO	AT Officer	G2 Ops	G3	IMO	G39 Information Operations Chief	MEF AC/S G4	AC/S G1	MEF G4 Material Readiness Officer	MEF Commander	G3/OPSO	MEF Commander/CoS
Facilitator (OPR0: (Name)	G3 Plans Officer	G3 Plans Officer	MEF Air O	G6 Ops O	SSEC/DCG	G3 Plans Officer	SSEC	G2 Collections Manager	MEF COMMSTRAT	G39 Defensive Cyberspace Operations Officer	II MEF Force Development Officer	G39 Space Operations Officer	II MEF Force Development Officer	FOPSO	AT Officer	G2	G3	IMO	G39 Information Operations Chief	MEF G4 Operations or Material Readiness Officer	Operations Officer	MRB OIC	G-33	FOPSO	SJA
CG	X				X	X	X																X		X
DCG					X		X																X		
SgtMaj							X		X														X		
CMDCM							X																X		
CoS	X					X	X		X														X		X
G1	X	X				X	X				X				X			X			X		X	X	
G2	X	X	X			X	X	X	X	X					X	X		X	X				X	X	X
G2 Targeting Officer								X								X									
G2 Collections																X									
G3	X	X	X			X	X			X	X	X	X		X		X	X	X				X	X	X
G3 Targeting Officer												X													
Air Officer			X					X									X							X	X
COPSO							X	X	X					X			X						X		
FOPSO						X	X	X	X					X			X						X	X	
CMO Planners																									
FECC	X	X					X					X		X			X						X	X	X
G4	X	X	X			X	X				X		X		X			X		X		X	X	X	
G5						X	X								X			X					X		
G6	X	X		X		X	X			X					X			X					X	X	
G8						X	X								X			X					X	X	
G10						X	X								X			X					X		
IKMO				X		X	X								X			X					X	X	
COMMSTRAT	X					X	X								X			X	X				X	X	X
SJA	X					X	X		X						X			X	X				X		X
HSS						X	X								X			X					X	X	X
Assessments						X	X		X						X			X					X		
SSEC					X	X	X		X						X			X					X		X
Security						X	X								X			X					X		
Chaplain						X	X		X						X			X					X		

Battle Rhythm Staff Utilization Matrix. (Click to Enlarge.)

CLASSIFICATION

Copy no. of copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

APPENDIX 3 TO ANNEX U TO OPERATION ORDER XXX-XX (U)
COMMON OPERATIONAL PICTURE ANDCOMMON TACTICAL PICTURE (U)

1. (U) Purpose. This appendix provides a basic description of the COP and CTP services that will be used during OPERATION XXX.

2. (U) General. The COP and CTP models the battle space and provides the commander and staff relevant, reliable, and available battlespace information. It is the primary tool for orienting the MEF battle staff on the single battle. It is a digital integration of many efforts and products across staff lines. Overall, the AC/S G- 2 develops procedures for Threat Track Management, and the AC/S G-3 develops procedures for Friendly Track Management. A Tactical COP Server (TCS) sits atop the entire MEF COP architecture, acting as a single point to higher and adjacent commands for sending and receiving COP data designed to include units maneuvering ashore, afloat and in the air. This platform is commonly referred to as the MEF TOP COP. Extraneous connections between servers within or outside of the MEF COP architecture are not authorized without the approval of the II MEF IKMO.

3. (U) COP and CTP Internal to MEF

a. (U) MEF TOP COP server. The TOP COP server is a TCS employed at the MEF Command Element to host and manage all track data.

(1) (U) Command and Control Personal Computer (C2PC). C2PC is a windows-based application that is loaded on the Joint Tactical COP Workstation and allows users to interact with the COP. The software allows users to manipulate track data, create overlays and other digital products, and produce CTP views. The C2PC is widely used throughout the MEF at every level down to platoons. It extends CTP viewing and editing capabilities to a large number of users. The C2PC requires the establishment of a C2PC gateway at the local command. The C2PC gateway manages track data from the next higher-level gateway.

(2) (U) TCS Server. A diagram of the core C2 TCS architecture employed by MEF to build, maintain, distribute, and receive the COP in support of OPERATION XXX is provided in Tab B of Appendix 3.

Page Number
CLASSIFICATION

CLASSIFICATION

b. (U) Track Management Procedures. Track Management Procedures, to include Track Naming Conventions, are provided in Tab C of Appendix 3.

c. (U) Major Subordinate Commands and Major Subordinate Elements. MSCs and MSEs are responsible for track manipulation and management for units at the battalion level and below.

d. (U) Overlay Naming Conventions. Overlay Naming Conventions are provided in Tab D of Appendix 3.

4. (U) COP External to MEF

a. (U) Tab A of Appendix 3 is the OPERATION XXX COP diagram depicting the GCCS-J topology at the MEF. The MEF will act as the U.S. Forces TOP COP for OPERATION XXX. The MEF TCS will distribute the COP and CTP to all MEF subordinate TCSs participating in OPERATION XXX.

b. (U) TAB B of Appendix 3 shows the location of all TCSs and C2PC gateways in use for OPERATION XXX.

TABS:

A—Common Operational Picture HHQ Architecture
B—Common Operational Picture MEF Architecture
C—Track Management and Naming Convention Procedures
D—Overlay Naming Convention

Glossary

Section I. Acronyms

C/S	chief of staff
C2	command and control
CCIR	commander's critical information requirement
CENTRIXS	Combined Enterprise Regional Information Exchange System
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COC	combat operations center
COP	common operational picture
CTP	common tactical picture
CWS	collaborative workspace
DSM	decision support matrix
FRAGO	fragmentary order
G-1	assistant chief of staff, personnel
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-4	assistant chief of staff, logistics
G-6	assistant chief of staff, communications
HHQ	higher headquarters
IER	information exchange requirement
IM	information management
IMLC	information management lifecycle
JECC	Joint Enabling Capabilities Command
JTF	joint task force
KM	knowledge management
KMO	knowledge management officers
KMR	knowledge management representative
MAGTF	Marine air-ground task force
MCDP	Marine Corps doctrinal publication
MCTOG	Marine Corps Tactical Operations Group
MEF	Marine expeditionary force
MET	mission essential task
MISTC	MAGTF Information Systems Training Center
MSC	major subordinate command
NIPRNET	Non-classified Internet Protocol Router Network

OODA	observe, orient, decide, act
OPORD	operation order
PACE	primary, alternate, contingency, emergency
POC	point of contact
RFI	request for information
RSS	really simple syndication
S-1	personnel officer
S-2	intelligence officer
S-3	operations officer
S-4	logistics officer
S-6	communications system officer
SIGEVENT	significant event
SIPRNET	SECRET Internet Protocol Router Network
SOP	standing operating procedure
SWO	senior watch officer
TTP	tactics, techniques, and procedures
URL	uniform resource locator
VAULTIS	visible, accessible, understandable, linked, trustworthy, interoperable, secure
XO	executive officer

The following acronyms are applicable specifically to this publication.

IKM	information and knowledge management
IKMO	information and knowledge management officer
IKMP	information knowledge management plan
IKMWG	information and knowledge management working group
TCS	tactical common operational picture server

Section II. Definitions

commander's critical information requirement
Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decision-making. The two subcategories are priority intelligence requirements and friendly force information requirements. Also called **CCIR**. (USMC Dictionary)

common operational picture
A single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called **COP**. (DoD Dictionary)

common tactical picture
An accurate and complete display of relevant tactical data that integrates tactical information from the multi- tactical data link network, ground network, intelligence network, and sensor networks. Also called **CTP**. (DoD Dictionary)

information management
The function of managing an organization's information resources for the handling of data and information acquired by one or many different systems, individuals and organizations. (DoD Dictionary)

information requirements
Those items of information regarding the relevant aspects of the operational environment that need to be collected and processed to meet the intelligence requirements of a commander. (DoD Dictionary)

knowledge management
A discipline that integrates people and processes to create shared understanding, increased organizational performance, and improved decision-making. Also called **KM**. (DoD Dictionary)

request for information
Any specific, time-sensitive, ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. (DoD Dictionary)

situational awareness
Knowledge and understanding of the current situation that promotes timely, relevant, and accurate assessment of friendly, enemy, and other operations within the battlespace to facilitate decision-making. An informational perspective and skill that fosters an ability to determine quickly the context and relevance of events that are unfolding. (USMC Dictionary)

The following pertain to this publication:

information filter
A filter used to assess the value of information and discard what is not pertinent or important.

information flow
The movement of information.

References and Related Publications

Federal Publications

United States Code, Title 44, Public Printing and Documents, chapter 21, National Archives and Records Administration

United States Code, Title 44, Public Printing and Documents, Administration, chapter 33, Disposal of Records

Chairman of the Joint Chiefs of Staff Instruction (CJCSI)

3151.01_ Global Command and Control System Common Operational Picture Reporting Requirements

Joint Issuances

Joint Publications (JPs)

3-0 Joint Operations

3-33 Joint Force Headquarters

6-0 Joint Communications

Miscellaneous

Department of Defense Dictionary of Military and Associated Terms

Navy Issuances

Miscellaneous

Department of the Navy Knowledge Management Strategy

Marine Corps Issuances

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
1-0	Marine Corps Operations
3	Expeditionary Operations
5	Planning
6	Command and Control
8	Information

Marine Corps Warfighting Publication (MCWP)

5-1	Marine Corps Planning Process

Marine Corps Orders (MCOs)

5210.11F	Marine Corps Records Management Program
5400.52	Department of the Navy Deputy Chief Information Officer Marine Corps Roles and Responsibilities

Miscellaneous

Marine Corps Supplement to the Department of Defense Dictionary of Military Associated Terms

Marine Corps Information Enterprise (MCIENT) Strategy Neilson, Robert E, (2001). Information Resources Management College, National Defense University. Knowledge Management and the Role of the CKO, in Knowledge Management: Catalyst for Electronic Government, Vienna, Virginia.