Office of the Army Chief Information Officer/G-6

U.S. Army Enterprise Service Management (AESM) Reference Architecture (RA)

20 May 2015

Version 1.0

CIO/G-6

ENABLING SUCCESS For Today and Tomorrow

U.S. ARMY

CIOG6.ARMY.MIL

DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

DISPOSITION INSTRUCTIONS

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.

Army Enterprise Service Management Reference Architecture Executive Summary

The LandWarNet 2020 and Beyond vision highlights the need to serve and support an Army trained to deploy on little notice - anytime and anywhere - with the ability to conduct successful unified land operations. To ensure the Army has the capability to deliver the required information technology (IT) enterprise services across the full range of military operations, the Army has established an Army Enterprise Service Management Framework (AESMF). In alignment with the Defense Enterprise Service Management Framework (DESMF), the AESMF is a holistic and integrated approach that relies on people, processes, functions, and technology to deliver effective IT services within a well-defined governance structure. The AESMF will enable Army users to meet strategic and operational mission requirements through the implementation, management, and continual improvement of standard IT Service Management (ITSM) processes across the Army enterprise.

In support of the AESMF and the Army Network Campaign Plan (ANCP), this Army Enterprise Service Management (AESM) Reference Architecture (RA) complements and guides the Army's existing service management practices and capabilities by providing principles, rules, technical positions, and implementation patterns.

In coordination with the ITSM community across the Department of Defense (DoD), this RA aligns with Army ITSM policies as well as Army, DoD, Joint, and Service Component ITSM operational documents, implementation frameworks, and best practices.

The RA supports the DoD IT Enterprise Strategy and Roadmap and the Secretary of the Army's IT Management Reform Implementation Plan to publish IT architecture guidance. The RA is a key part of the Army Chief Information Officer (CIO)/G-6 Rules-Based Architecture and ensures alignment with DoD Information Enterprise Architecture and the Joint Information Environment (JIE). It also ensures Army implementations are integrated with and postured to leverage JIE capabilities.

BLOHM.GARY.W.1228949589

Digitally signed by BLOHM.GARY.W.1228949589
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=BLOHM.GARY.W.1228949589
Date: 2015.05.20 15:26:47 -04'00'

GARY W. BLOHM

Director, Army Enterprise Architecture

Table of Contents

Table of Figures

Table of Tables

Chapter 1
Introduction

1-1. Architecture Introduction

a. The Army Information Enterprise Architecture (IEA) is a high level representation of the LandWarNet (LWN) architecture, as it supports the Army's Enterprise Information Environment, Warfighting, Business, and Defense Intelligence Mission Areas. The IEA is sub-divided into the LWN 2020 and Beyond Enterprise Architecture (EA), and a set of Enterprise Reference Architectures (RAs), all of which the Chief Information Officer (CIO)/G-6 develops.

b. The hierarchy of the IEA, and the context in which it fits, is shown in Figure 1.

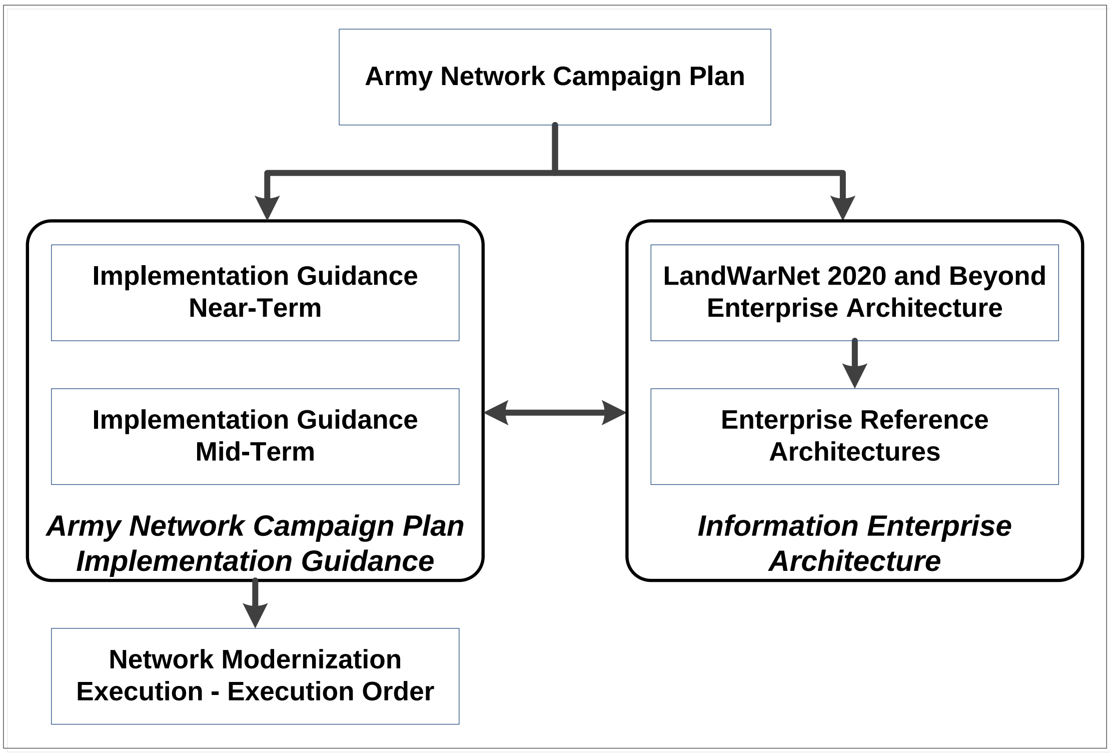

Army Network Campaign Plan
Implementation Guidance Near-Term
Implementation Guidance Mid-Term
Army Network Campaign Plan Implementation Guidance
LandWarNet 2020 and Beyond Enterprise Architecture
Enterprise Reference Architectures
Information Enterprise Architecture
Network Modernization Execution - Execution Order

Figure 1. Hierarchy and Context of the IEA Documents

c. The overall objective of the documents shown in Figure 1 is to provide the architecture guidance and direction for LWN to achieve the vision in the Army Network Campaign Plan (ANCP). This includes policy, principles and rules, constraints, technical guidance, standards and forecasts, implementation conventions, and criteria. Each of these documents has a unique role in the IEA by providing specific architecture-related information, as described below.

(1) LWN 2020 and Beyond EA – Captures CIO/G-6 architecture guidance and direction at the level of detail needed to support the evaluation of potential Information Technology (IT) investments and architecture options for their alignment with the ANCP.

(2) Enterprise RAs – Aid in the resolution of specific recurring problems and explain context, goals, purpose, and the problems being solved.

d. The IEA documents can be found at http://ciog6.army.mil/Architecture/tabid/146/Default.aspx. Those with a Common

Access Card (CAC) may also visit the Army Capability Architecture Development and Integration Environment (ArCADIE) site at: https://cadie.tradoc.army.mil/CIO-G6_20Architecture/SitePages/Home.aspx.[1]

e. The AESM RA is a specific instance of an Enterprise RA. It provides overarching guidance to support Army efforts to achieve Federal and DoD mandates to transition to a holistic and integrated approach for managing IT services. Successful delivery of the capabilities described herein is coupled with successful delivery of capabilities discussed in the other enterprise reference architectures.

1-2. Background

a. The Army has been managing its enterprise IT services from concept to solution and retirement since 2003, but it lacked a holistic and integrated approach. This lack of standard processes and inconsistent use of AESM throughout the Army inhibits its ability to deploy, sustain, and make sound strategic and investment decisions to achieve ANCP objectives and vision for the LWN 2020 & Beyond EA.

b. On 17 November 2014, the CIO/G-6 signed the Army Information Technology Service Management (ITSM) Policy establishing and directing implementation of the Army Enterprise Service Management Framework (AESMF) for managing Army IT enterprise services. The AESMF is the Army's implementation of the DoD Enterprise Service Management Framework (DESMF), which originated from industry best practices such as Information Technology Infrastructure Library (ITIL), COBIT,[2] and ITSM. The Army has adopted and adapted many of the concepts and methodologies from these sources as well as elements of the DESMF and from the Navy Process Reference Model (NPRM).

c. The AESMF is the Army's overarching guidance for conducting integrated AESM. As shown in a high level illustration in Figure 2, it establishes a foundation for the development and implementation of principles and rules based on the concepts and methodologies derived from industry best practices.

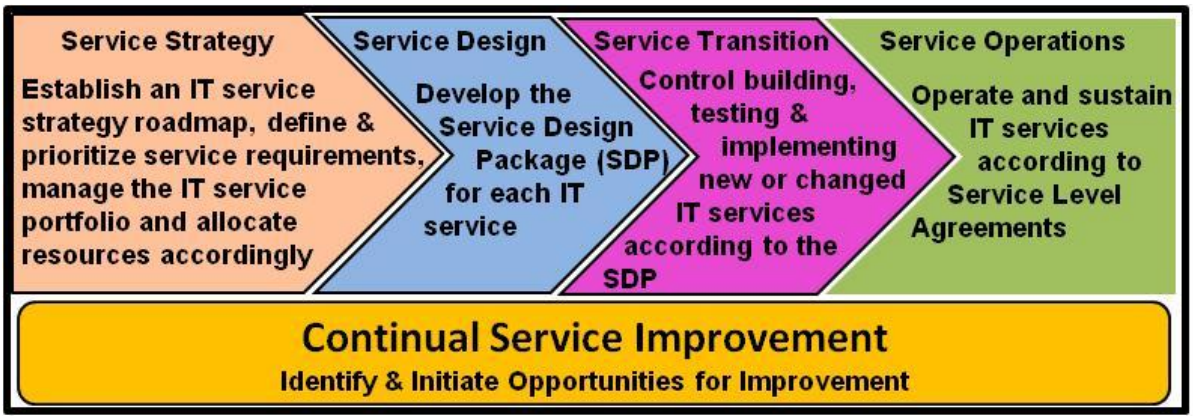

Service Strategy
Establish an IT service strategy roadmap, define & prioritize service requirements, manage the IT service portfolio and allocate resources accordingly
Service Design
Develop the Service Design Package (SDP) for each IT service
Service Transition
Control building, testing & implementing new or changed IT services according to the SDP
Service Operations
Operate and sustain IT services according to Service Level Agreements
Continual Service Improvement
Identify & Initiate Opportunities for Improvement

Figure 2. AESM Framework Life-cycle Stages

[1] First time users may have to request access.

[2] COBIT was originally an acronym for Control Objectives for Information and related Technology. It now is used in short form to identify the name of the framework (Information Systems Audit and Control Association, COBIT v5, 2014).

d. In coordination with the development of other associated guiding AESM documents, this AESM RA provides the guidelines for supporting and facilitating AESMF establishment and implementation.

1-3. Intended Audience

a. The intended audience primarily includes Army AESM participants: Process Owners, Process Managers, Service Providers, Service Owners, and Service Managers. The audience also extends to DoD organizations (e.g., Service Components, Agencies, other Army units) with executive managers, mission area (Warfighting, Business, and Enterprise Information Environment) leads, portfolio leads, architects, and engineers involved in the planning, development, implementation, operation, and maintenance of AESM IT services.

1-4. Purpose

a. The AESM RA is a foundational document providing a common set of principles, rules, and terms aligned with the AESMF to support the implementation of IT service management. The specific purpose of this RA is as follows:

(1) Implement Army ITSM Policy and support associated documents.

(2) Inform the audience of the intent to establish an AESMF.

(3) Guide implementation through principles, rules, technical positions, and implementation patterns.

b. Figure 3 below, the AESM RA relationship to other documents diagram, shows where the AESM RA falls in line with other key document related to the overall management and security of IT services.

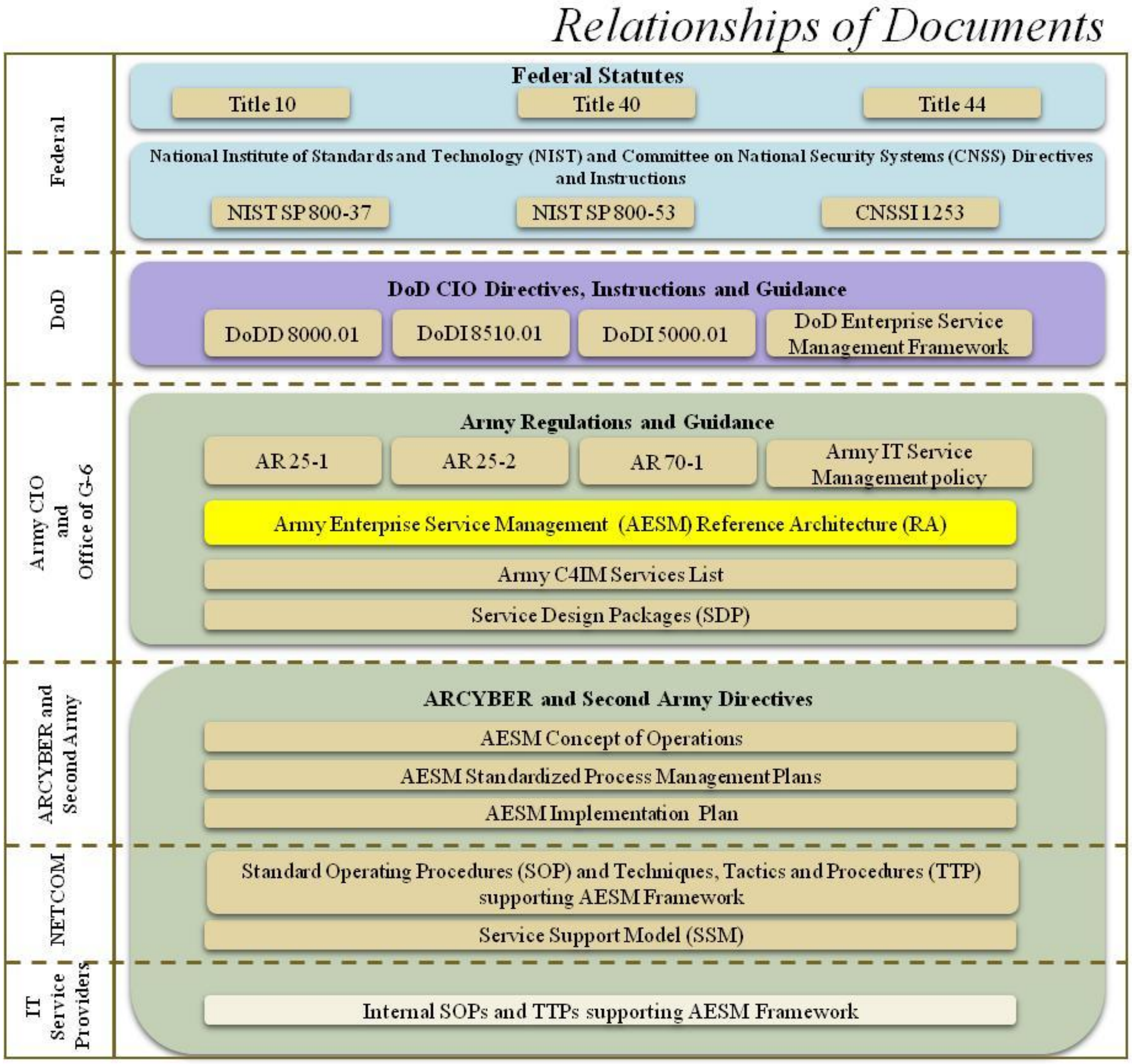

Relationships of Documents
Federal
DoD
Army CIO and Office of G-6
ARCYBER and Second Army
NETCOM
IT Service Providers
Federal Statutes
Title 10
Title 40
Title 44
National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) Directives and Instructions
NIST SP 800-37
NIST SP 800-53
CNSSI 1253
DoD CIO Directives, Instructions and Guidance
DoDD 8000.01
DoDI 8510.01
DoDI 5000.01
DoD Enterprise Service Management Framework
Army Regulations and Guidance
AR 25-1
AR 25-2
AR 70-1
Army IT Service Management policy
Army Enterprise Service Management (AESM) Reference Architecture (RA)
Army C4IM Services List
Service Design Packages (SDP)
ARCYBER and Second Army Directives
AESM Concept of Operations
AESM Standardized Process Management Plans
AESM Implementation Plan
Standard Operating Procedures (SOP) and Techniques, Tactics and Procedures (TTP) supporting AESM Framework
Service Support Model (SSM)
Internal SOPs and TTPs supporting AESM Framework

Figure 3. AESM RA Relationship to Other Documents

1-5. Scope

a. This version of the RA primarily supports the establishment and transition of AESMF by providing the following:

(1) Codification of AESMF and Vision.

(2) Guiding Principles and Rules (with AESMF alignments).

(3) Initial Technical Positions (Standards) and Implementation Patterns.

(4) Initial Integrated Dictionary.

b. This RA also supports acquisition efforts to improve operational effectiveness, security, interoperability, IT efficiency, and information sharing with standardized enterprise service management practices, tools, and services. Applicable IT services are in the Army Command, Control, Communications, Computers, and Information Management (C4IM) Services List.[3]

c. This RA is an authoritative source that guides AESM efforts by also showing the implementation of industry ITSM best practices. This is evidenced by the identification of processes and functions in each of the AESMF Life-cycle Stages (described in Chapter 2) as well as the establishment of technical positions and implementation patterns (described in Chapter 4).

d. The ANCP – Implementation Guidance, Near-Term 2015-2016 and ANCP – Implementation Guidance, Mid-Term 2017-2021 documents identify key enterprise activities and priorities across the three AEN Domains. These guidance documents are living documents developed on an annual basis to reflect the realities of Army missions, acquisition planning, and resourcing. Although ANCP covers time periods, this RA supports enterprise service management activities (e.g., IT Asset Management, Service Desk, Enterprise Service Management System, Joint Management System, Optimized Network Functions and Resource) identified in both documents.

e. As AESM documents (e.g., AESM Concept of Operations [CONOPS], Implementation Plans, Service Design Packages) become available and mature, the next version of the AESM RA will be updated accordingly to support continuing implementation efforts.

1-6. Alignment with Department of Defense (DoD) and Army Enterprise Network (AEN) Portfolio

a. This RA describes AESM and its alignment with the DESMF, DoD IEA (and Joint Information Environment [JIE]) and the AEN Portfolio Domains.

b. DoD Enterprise Service Management Framework (DESMF). The AESMF is aligned with the DESMF in the following areas:

(1) Purpose and Goals.

(2) Guiding Principles.

(3) Life-cycle Stages (Structure).

(a) Five Stages (Strategy, Design, Transition, Operations, and Continuous Service Component [CSI]).

(b) Standard Processes and Functions (Twenty-seven processes and five functions under the five Life-cycle Stages).

(4) Roles and Responsibilities (Provider, Owners, and Managers).

(5) Standards (International Standards).

c. DoD Information Enterprise Architecture (IEA) and AEN Portfolio. The JIE is envisioned as a secure environment comprising shared information technology

[3] The C4IM Services List is the foundation for the LandWarNet Services Catalog, which is the customer-facing document that identifies standards for delivery of services based on funding constraints. It can be accessed from here: http://ciog6.army.mil/Leadership/LeaderBlog/tabid/108/EntryId/18/Update-to-LandWarNet-LWN-Services-Catalog.aspx.

infrastructure, enterprise services, and cybersecurity architecture to achieve full spectrum superiority, improved mission effectiveness, increased security, and the realization of IT efficiencies. Operation and management of JIE is in accordance with the Unified Command Plan using enforceable standards; specifications; and common tactics, techniques, and procedures described in DoD IEA v2.0. The DoD IEA describes a vision of required information enterprise capabilities, as follows:

(1) End User Capabilities: Connect, Access, Share.

(2) Enable Capabilities: Operate, Defend.

(3) Users & Operations Requirements (Govern): Processes, Policy, Compliance.

d. The Army's framework for managing network modernization is the Army AEN portfolio, which manages the Communications and Computers Joint Capability Area (JCA 6.0). The portfolio comprises three AEN Domains: Network Capacity, Enterprise Services, and Network Operations & Security. Each domain is further divided into capabilities as follows:

(1) <u>Network Capacity Domain (NCD).</u> The NCD portfolio includes the physical infrastructure necessary for all services and information based activities to traverse the network. The portfolio encompasses the foundational infrastructure upon which the Enterprise Services and Network Operations & Security solutions reside. Capabilities within this domain include Information Transport and Computing Services.

(2) <u>Enterprise Services Domain (ESD).</u> This portfolio oversees delivery of an easy-to-use, integrated suite of globally available, adaptable solutions that seamlessly support the Total Force while working with Unified Action Partners (UAPs). These services, both user-facing and enabling, provide the Total Force awareness of and access to information. Capabilities within this domain include: Core Enterprise Services and Position, Navigation & Timing.

(3) <u>Network Operations & Security Domain (NSD).</u> The NSD is responsible for providing a secure, seamless, and continuous network environment with protected critical data and information for the Total Force and UAPs. To meet this objective, NSD will provide capabilities that will improve the Army's ability to protect, detect, respond, restore, and manage information and systems. NSD will also pursue capabilities that support the management of underlying physical assets that provide end user services for a continuous network environment. Capabilities within this domain include Net Management and Cybersecurity.

e. The alignment between DoD IEA and AEN Domains is depicted in a Capability Viewpoint (CV-2a). As noted in Figure 4, this is a first-level mapping to identify the capabilities associated with AESM. It is provided to support the crosswalk from delivered capabilities back to the DoD IEA capabilities.

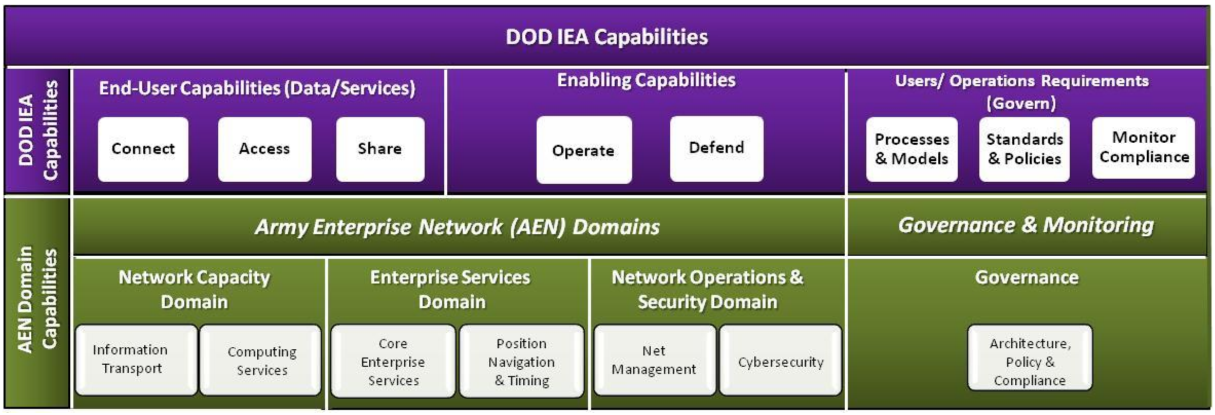


Figure 4. Capability Taxonomy (CV-2a): AEN Mapping to the DoD IEA Capabilities

f. The second level of mapping, as depicted in Figure 5, pertains to the AESM-specific capability aligned with the AEN Domains (as described in the ANCP). As shown, the capability of AESM relates to the six JCAs in the AEN Domains.

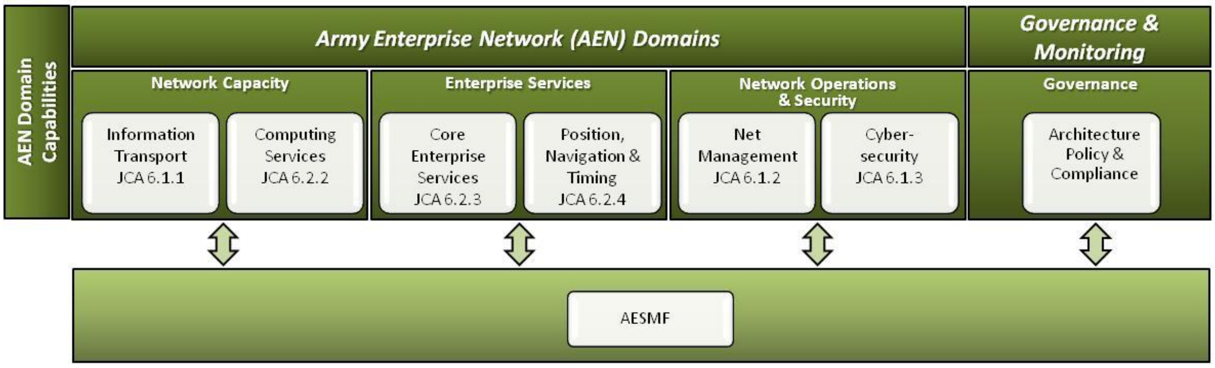

AEN Domain Capabilities
Army Enterprise Network (AEN) Domains
Governance & Monitoring
Network Capacity
Information Transport JCA 6.1.1
Computing Services JCA 6.2.2
Enterprise Services
Core Enterprise Services JCA 6.2.3
Position, Navigation & Timing JCA 6.2.4
Network Operations & Security
Net Management JCA 6.1.2
Cyber-security JCA 6.1.3
Governance
Architecture Policy & Compliance
AESMF

Figure 5. Capability Taxonomy (CV-2b): AESMF Mapping to AEN Domains

1-7. Assumptions and Constraints

a. AESM is enabled through the synchronization, integration, and interoperability of a number of other Army IT capabilities (e.g., Unified Capabilities, Network Security). Accordingly, several high-level assumptions are as follows:

(1) The AESM end-state will be achieved through implementation and operation of other DoD and Army IT capabilities (e.g., DoD Enterprise Email, Unified Capabilities, Army Network Security) as well as the maturation of AESM via AESM CONOPS, AESM RA, Process Management Plans (PMP), Service Design Packages (SDPs) and Service Management Plans (SMPs).

(2) The AESM RA will be used to inform, guide, and support AESM processes and implementation plans across the Army.

(3) Intended organizations will use this RA as enterprise guidance for standardizing methods, benchmarking, architecture, and developing Critical Success Factors (CSF) with supporting Key Performance Indicators (KPI) and related metrics.

Chapter 2
Army Enterprise Service Management (AESM)

2-1. Overview

a. AESM is the Army’s approach to managing IT enterprise services. It ensures Army investments in services meet user needs by standardizing a holistic and integrated approach to delivering IT services. This approach implements the AESMF in a way that continually increases effectiveness, improves security, and gains efficiencies in Army IT services by standardizing the service delivery process. The AESMF has adopted and adapted the DESMF, which is based on best business practices and the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 20000 standards.[4]

b. A key characteristic of Army IT services is that they must be developed based on the standards specified by the LWN 2020 and Beyond EA, Appendix C to Annex A. Army Standards Profile Guidance In Support of Common Operating Environment (COE) v3. Services will leverage shared IT capacity, security, and commodity service, and they need to be easy to use, globally available, adaptable, and user-facing to provide the Army with the awareness of and access to information on any trusted device anywhere in the world. Developed and provided as an integrated suite of tools, these services will be designed to seamlessly support the Total Force. Services range from a core set of services provided and funded by CIO/G-6 to mission-funded services spanning war-fighter and business functions.

c. As shown below in Table 1, AESM is depicted in a framework of five Life-cycle Stages. Each stage includes a number of best practice processes or functions. A process is a structured set of activities designed to accomplish a specific objective. Each IT life-cycle stage contains several processes and each process contains several activities. The Life-cycle Stages enable the Army’s IT support organizations to leverage capabilities in the most effective and efficient manner. The Life-cycle Stages provide structure, stability, and strength to IT service management capabilities with durable principles, methods, and tools. This serves to protect IT investments and provide the necessary basis for measurement, learning, and improvement.

d. A function is a team, organizational unit, or group of people that specializes to perform certain activities or types of work. They typically have the similar skill sets and resources to carry out their duties to achieve specific outcomes. The function is responsible for defining the standards and procedures to be followed when operating within the function. The AESM CONOPS describes each process and function in more detail. Chapter 3 of this RA provides the CSFs and KPIs for each process and function.

[4] An international standard that promotes the adoption of an integrated process approach to effectively deliver managed services to meet business and mission partner requirements; ISO/IEC 20000 is well recognized as the world-wide standard for IT service management.

Table 1. AESMF Life-cycle Stages

AESMF Life-cycle Stages	Processes and Functions
Service Strategy (SS)	Strategy Generation Management (SGM)
	Business Relationship Management (BRM)
	Demand Management (DM)
	Financial Management for IT Services (FM)
	Service Portfolio Management (SPM)
	Service Catalog Management (SCM)
Service Design (SD)	Design Coordination (DC)
	Availability Management (AvM)
	Capacity Management (CapM)
	Information Security Management (ISM)
	IT Service Continuity Management (ITSCM)
	Service Level Management (SLM)
	Supplier Management (SUP)
	Engineering (Function) (ENGF)
Service Transition (ST)	Transition Planning and Support (TPS)
	Asset Management (AM)
	Change Management (ChM)
	Change Evaluation (EVAL)
	Configuration Management (CfM)
	IT Services Knowledge Management (ITSKM)
	Release and Deployment Management (RDM)
	Service Validation and Testing (SVT)
Service Operations (SO)	Access Management (AcM)
	Event Management (EM)
	Incident Management (IM)
	Problem Management (PRM)
	Request Fulfillment (RF)
	Service Desk (Function) (SDF)
	Application Management (Function) (AMF)
	IT Operations Management (Function) (ITOMF)
	Technical Management (Function) (TMF)
Continual Service Improvement (CSI)	7 Step Improvement Process

e. Service Strategy. SS aligns the needs of Army's Warfighting, Business, and Defense Intelligence Mission Areas with those of the Enterprise Information Environment Mission Area along with Army mission partners and the objectives of Army IT support organizations. It postures decision-makers to understand and manage the costs and risks associated with the IT service portfolio. It also provides the foundation for operational IT effectiveness as well as provides guidance to ensure IT services are well understood during the Service Design life-cycle stage. A service strategy plan will be created from over-arching Army and Army IT strategy documents and the culture of the organization that the service provider supports.

f. Service Design. SD is the blueprint for designing appropriate IT services, processes, policies, and documentation to meet current and future agreed-upon requirements. It begins with a new or changed service requirement and ends with the development of an IT service solution designed to meet the needs of customers.

g. Service Transition. ST uses the blueprints provided by SD to build, test, and deploy the solution to service operations. It encompasses the project side that is a temporary endeavor designed to produce a unique product or service for operational use. Successful service transition rests on effective understanding and use of change management, quality assurance, and risk management as well as effective program and project management.

h. Service Operations. SO delivers agreed service levels to all users and strives to ensure uninterrupted services by monitoring events and resolving incidences, issues, and problems. SO coordinates and executes activities needed to deliver and manage IT services and supporting applications as well as the technologies and infrastructure needed to observe performance, collect operational data, make assessments, and report on prescribed service metrics.

i. Continual Service Improvement. CSI is concerned with maintaining value through the continual evaluation and improvement of service quality. CSI monitoring focuses on the effectiveness of services, tools, and processes. It identifies where improvements can be made to the existing level of service and IT performance. The 7 Step Improvement Process is as follows:[5]

(1) Define what to measure.

(2) Define the areas that you can measure.

(3) Collect the data.

(4) Process the data.

(5) Analyze the data.

(6) Make data usable and present the data.

(7) Implement change.

2-2. AESM End-State Vision

a. The end-state vision of AESM, as illustrated in Figure 6, High Level Operational Concept (Operational Viewpoint [OV]-1), is to establish a standardized management framework to ensure services efficiently and effectively meet customer needs. Ultimately, this will provide Army Service Component Commands (ASCCs), Army Commands (ACOMs), Army Staff (ARSTAF), Direct Reporting Units and supported Combatant Commanders efficient management and process improvement of enterprise IT services. In addition, AESM vision will ensure the availability of resources to detect and respond to global threats while supporting regional and functional commands.

b. To achieve this vision, the Army will leverage applicable ITSM best practices as guided by DESMF and AESMF. The Army will develop documents such as the AESM RA, AESM CONOPS, Service Design Package, and Process Management Plan to continuously improve service management processes for improving mission effectiveness while strengthening cybersecurity and gaining efficiencies across the Army.

[5] Details of the 7 steps are located at: http://itilcontinualserviceimprovement.blogspot.com/2008/09/itil-csi-7-step-improvement-process.html.

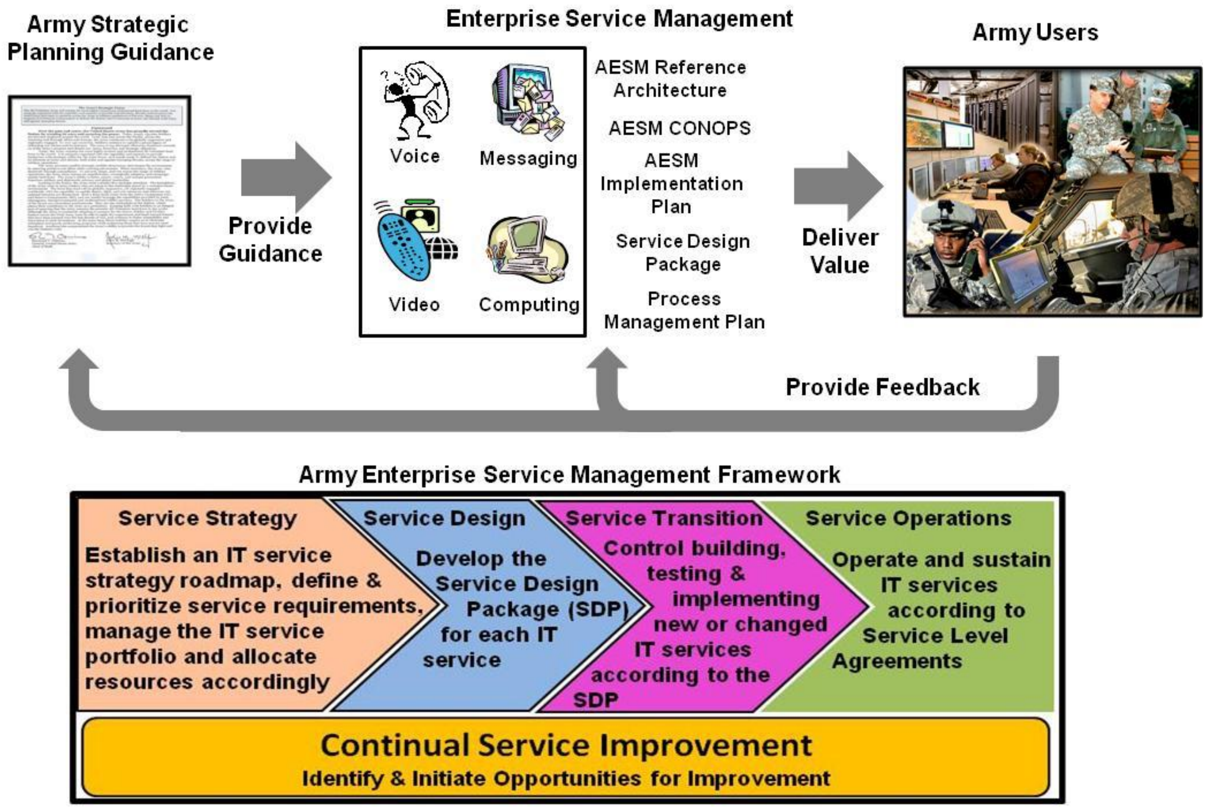

Army Strategic Planning Guidance
Provide Guidance
Enterprise Service Management
Voice
Messaging
Video
Computing
AESM Reference Architecture
AESM CONOPS
AESM Implementation Plan
Service Design Package
Process Management Plan
Deliver Value
Army Users
Provide Feedback
Army Enterprise Service Management Framework
Service Strategy
Establish an IT service strategy roadmap, define & prioritize service requirements, manage the IT service portfolio and allocate resources accordingly
Service Design
Develop the Service Design Package (SDP) for each IT service
Service Transition
Control building, testing & implementing new or changed IT services according to the SDP
Service Operations
Operate and sustain IT services according to Service Level Agreements
Continual Service Improvement
Identify & Initiate Opportunities for Improvement

Figure 6. High Level Operational Concept (OV-1)

2-3. Army Enterprise Service Management Framework (AESMF) Summary

a. The AESMF is largely a structure of processes and functions that provide the necessary support for efficient and effective delivery and management of IT services for the Army. As adopted and adapted from the DESMF, it is a five-stage IT service life-cycle approach designed to monitor, manage, and improve services throughout the LWN, the Army's component of the DoD Information Network (DoDIN). The Life-cycle Stages and key processes/functions are depicted in Table 1 followed by an overview of each life-cycle stage. All Army IT enterprise service development, fielding, and retirement will follow this life-cycle.

Chapter 3
Guiding Principles and Rules

3-1. Introduction

a. Guiding principles and rules represent the highest level of guidance for IT planning and decision making. They are high-level statements that apply to specific warfighting and business requirements, and they are intended to serve as enduring guidelines that describe how AESM enables the Army to accomplish its mission. They express the intent of capabilities and fundamental values to be applied within AESM. Principles strengthen and support the Army's strategic goals as outlined in the ANCP and the LWN 2020 & Beyond EA. Rules are definitive statements that provide design tenets while constraining and guiding implementation efforts.

b. The following sub-chapters show the principles, rules, gaps, outcomes, risks, and mitigations collectively in five tables. These tables correspond one-to-one with the AESMF Life-cycle Stages.

c. Following each table is a second coordinating table, a listing of CSFs and KPIs.[6] The CSFs and KPIs were developed in coordination with AESM/ITSM stakeholders. CSFs are specific goals (or thresholds) that must be achieved if an IT service is to be deemed successful. KPIs are measures that characterize the performance of activities and services necessary to produce the outcomes. CSFs and KPIs are key factors used in Continuous Process Improvement. In addition, there is a listing of processes and functions (e.g., SGM, BRM) to show corresponding applicability of CSFs and KPIs.

d. A generic template and a more detailed description of the tables with principles, operational rules, gaps, risks and mitigations can be found in Appendix E.

[6] In the context of this RA, the term "performance" will be used to generally refer to both CSFs and KPIs (not to be confused with referring to only KPIs).

3-2. AESM Service Strategy Rules

Table 2. Service Strategy Principles and Rules

<table>
<tr><th colspan="2">Guiding Principle</th></tr>
<tr><td colspan="2">DoD IEA Guiding Principle (GP) 01 - DoD CIO-governed resources are conceived, designed, operated, and managed to address the mission needs of the Department.

<b>AESM 1.1, Under the Service Strategy life-cycle stage, the Army will:</b>
1. Document the AESM Strategy.
2. Establish clear definitions of IT services for the customer.
3. Define criteria for measuring the value of IT Services.
4. Institute and enforce a governance framework.</td></tr>
<tr><th>DoD IEA/JIE Capability</th><th>AEN Capability</th></tr>
<tr><td>Enabling Capabilities
Users/Operations Requirements (Govern)</td><td>Network Capacity
Enterprise Services
Network Operations and Security
Governance</td></tr>
<tr><th colspan="2">JCA [or Army] Capability Gap(s)</th></tr>
<tr><td colspan="2">JCA 6.2.3 Core Enterprise Services:
1. The Army lacks a holistic and integrated approach (e.g., IT governance, processes, monitoring) for developing and managing its enterprise IT service strategy from concept to solution and retirement.</td></tr>
<tr><th>Architectural or Business Rule(s) that Mitigate Gaps</th><th>Desired Outcome(s)</th></tr>
<tr><td>AESM 1.1.1 - Establish, implement, and manage AESMF efforts to ensure a holistic and integrated approach in IT service management.
AESM 1.1.2 - Establish strategic objectives for Army Enterprise Service Management.
AESM 1.1.3 - Define governance required to address emerging and sustaining capabilities and associated services for baseline and operational support.
AESM 1.1.4 - Identify standardization for projections and validation of existing and new services; ensure services are aligned with the C4IM Services List.
AESM 1.1.5 - Define business models for Enterprise Services (e.g., Defense Security Service, Baseline, Mission Funded).
AESM 1.1.6 - Ensure applicable Business Case Analysis is used in the selection of AESM services and solutions.
AESM 1.1.7 - Develop mechanisms to ensure all processes in the service life-cycle are integrated; ensure common definitions and terms across all processes in the AESMF Life-cycle Stages.</td><td>Strategic direction for IT Services is being followed via key activities and/or documents including the following: AESM Strategy, Portfolio Management, AESM RA, and AESM CONOPS.

See Table 3, Service Strategy Measurements, for additional information.</td></tr>
<tr><th colspan="2">Known Risk(s) with Mitigation</th></tr>
<tr><td colspan="2">Risk:
1. As the development of service management progresses in an iterative manner, there is the potential for misalignment due to improper coordination.</td></tr>
</table>

Mitigation:

1. Development and continued refinement of detailed implementation guidance and plans.
2. Educate key stakeholders on the benefit of a standardized, Army-wide approach to IT service management.

Table 3. Service Strategy Measurements

SS CSF	SS KPI	Process/Function Applicability
SS-CSF 1: The Service Strategy is clear, has concrete short term goals that are derived from, and are traceable back to, specific long-term plans.	SS-KPI 1.1: Services are prioritized and resourced in accordance with the IT Strategy.	SGM
SS-CSF 2: Corrective actions are taken and implemented based on the Business Relationship data collected.	SS-KPI 2.1: Customer satisfaction goals are met or exceeded.	BRM
SS-CSF 3: Service Owner proactively understands the customer's workload (demand) with the available resources (supply) through analysis, trending, and forecasting.	SS-KPI 3.1: The number of Capacity issues identified is not due to poor demand management procedures.	DM
SS-CSF 4: Effective Stewardship of IT Finances will be provided.	SS-KPI 4.1: Financial Management Process Maturity - execute financial management to a high level of process maturity. Evaluated as a COBIT capability level.	FM
SS-CSF 5: Effective IT service offerings will be provided.	SS-KPI 5.1: Percentage customer satisfaction with current IT service offerings (survey results)	SPM
SS-CSF 6: An accurate service catalog will be maintained.	SS-KPI 6.1: Service Catalog accuracy and completeness.	SCM

3-3. AESM Service Design Rules

Table 4. Service Design Principles and Rules

<table>
<tr><th colspan="2">Guiding Principle</th></tr>
<tr><td colspan="2">DoD IEA GP 03 - Data assets, services, and applications on the Global Information Grid (GIG) shall be visible, accessible, understandable, and trusted to authorized (including unanticipated) users.[7]
DoD IEA GP 04 - DoD CIO services shall advertise service level agreements (SLAs) that document their performance, and shall be operated to meet that agreement.
DoD IEA Secured Availability Principles (SAP) 02 - The globalization of information technology, particularly the international nature of hardware and software (including supply chain) development and the rise of global providers of Information Technology (IT) and communications services presents a very new and unique security challenge. GIG resources must be designed, managed, protected, and defended to meet this challenge.
DoD IEA Shared Infrastructure Business Rules (SIR) 02 - GIG infrastructure capabilities shall be designed, acquired, deployed, operated, and managed in a manner which enables continuity of operations and disaster recovery in the presence of attacks, failures, accidents, and natural or man-made disaster to support customer SLAs.
<b>AESM 1.2, Under the Service Design life-cycle stage, the Army will:</b>
1. Design effective IT Services, and ensure incremental improvements as required during the life-cycle.
2. Ensure Service solutions and designs provided are effective (quality).
3. Recognize shifting trends in the environment.</td></tr>
<tr><th>DoD IEA/JIE Capability</th><th>AEN Capability</th></tr>
<tr><td>Enabling Capabilities
Users/Operations Requirements (Govern)</td><td>Network Capacity
Enterprise Services
Network Operations and Security
Governance</td></tr>
<tr><th colspan="2">JCA [or Army] Capability Gap(s)</th></tr>
<tr><td colspan="2">JCA 6.2.2 Computing Services:
1. Lack of standardized processes to ensure effective access to hosted information and data centers across the enterprise.
JCA 6.2.3 Core Enterprise Services:
1. Lack of clarity or specificity of the set of Enterprise Services to design to.
2. Lack of metrics and processes to accurately depict the effectiveness and efficiency of LWN.
JCA 6.1.2 Net Management:
1. Lack of ability to monitor end-to-end IT services.</td></tr>
<tr><th>Architectural or Business Rule(s) that Mitigate Gaps</th><th>Desired Outcome(s)</th></tr>
<tr><td>AESM 1.2.1 - Develop design documents that ensure</td><td>All IT Services have</td></tr>
</table>

[7] Although usage of the term “Global Information Grid” has been replaced by “DoD Information Network (DoDIN),” the term will be used in the principles and rules cited in this RA because they are stated verbatim from DoD IEA V2.0, Jul 2012.

services are interoperable, accessible, discoverable, available, sharable and protected. AESM 1.2.2 - Develop design documents and SLAs to ensure customer needs are met and metrics support CSI. AESM 1.2.3 - Ensure design document address end-to-end IT services, project availability and capacity planning; ensure security services (e.g., monitoring) protect the information with security controls defined in NIST SP 800-53, Revision 4. AESM 1.2.4 - Develop implementation plans to ensure service federation, regional transition, and system/application termination. AESM 1.2.5 - Ensure design document definitions/terms are consistent; ensure architecture (e.g., services, capabilities, activities, processes) is integrated.	accurate SDPs. See Table 5, Service Design Measurements, for additional information.
Known Risk(s) with Mitigation	
Risk: 1. CSFs are not met. 2. A coordinated interface is not provided between IT planners and business planners. Mitigation: 1. Understanding service strategy requirements and priorities and ensuring they are included when designing service package.	

Table 5. Service Design Measurements

SD CSF	SD KPI	Process/Function Applicability
SD-CSF 1: Maintain an accurate Service Design Package.	SD-KPI 1.1: Service Design Package accuracy and completeness.	DC
SD-CSF 2: Availability and reliability of IT services are managed.	SD-KPI 2.1: Percent of time IT Service meets or exceeds its availability and reliability SLAs.	AvM
SD-CSF 3: Availability and reliability of accurate business forecasts.	SD-KPI 3.1: Accuracy of the forecasted capacity based on business trends.	CapM
SD-CSF 4: Service Designers will be able to identify and manage risks so that they can be avoided or mitigated.	SD-KPI 4.1: Average time lag between identification of enterprise risks and mitigation action(s).	ISM
SD-CSF 5: Continuity test results and associated changes based on the testing are available.	SD-KPI 5.1: Number of open issues and risks since last test.	ITSCM
SD-CSF 6: Availability and reliability of IT services.	SD-KPI 6.1: Percent of time IT Service meets or exceeds its availability and reliability	SLM

	SLAs.	
SD-CSF 7: Ability to monitor and manage supplier service activities.	SD-KPI 7.1: Time between a requisition for a Supplier and a successful negotiation with the researched and selected Supplier.	SUP
SD-CSF 8: Ability to monitor and manage engineering support requests.	SD-KPI 8.1: Time between a requisition for an engineering activity and the response from the appropriate engineering tier.	ENGF

3-4. AESM Service Transition Rules

Table 6. Service Transition Principles and Rules

<table>
<tr><th colspan="2">Guiding Principles</th></tr>
<tr><td colspan="2">DoD IEA Operational Reference Architecture (ORA) - Derived Operational Rules (OPR) 26 - Develop a common set of functional policies so that all components of each IE program or system are developed, tested, certified, and deployed with an emphasis on end-to-end enterprise commonality.
<b>AESM 1.3, Under the Service Transition life-cycle stage, the Army will:</b>
1. Plan and manage the changes in the Service effectively and efficiently.
2. Manage risks that are related to new, changed, or retired Services.
3. Deploy the release of the Service into the production environment successfully.</td></tr>
<tr><th>DoD IEA/JIE Capability</th><th>AEN Capability</th></tr>
<tr><td>Enabling Capabilities
Users/Operations Requirements (Govern)</td><td>Network Capacity
Enterprise Services
Network Operations and Security</td></tr>
<tr><th colspan="2">JCA [or Army] Capability Gap(s)</th></tr>
<tr><td colspan="2">JCA 6.2.3 Core Enterprise Services:
1. Lack of definition of service and associated metrics to ensure measurable outcomes.
JCA 6.1.2 Net Management:
1. Lack of a management plan to ensure available resources to support the service employment.
2. Inadequate implementation of change process to ensure tracking and monitoring of service changes.
3. Incomplete configuration management and audit plans to ensure successful transition.</td></tr>
<tr><th>Architectural or Business Rule(s) that Mitigate Gaps</th><th>Desired Outcome(s)</th></tr>
<tr><td>AESM 1.3.1 - Develop governance and control processes (IT governance and/or standard processes [configuration control] for the build, test, and acceptance when transitioning into the operational environment) that ensure services are effectively transitioned; ensure the transition results in services being visible,</td><td><i>Services or changes to a service are controlled via a standard process for ensuring successful transitioning into the operational environment.</i></td></tr>
</table>

accessible, understandable, and trusted. AESM 1.3.2 - Ensure updates of portfolios and assets within designated portfolio/asset management systems (e.g., Army Portfolio Management Solution or other AESM platform); ensure information from these management systems is reviewed during the planning and execution of the termination and retirement of applicable systems and applications. AESM 1.3.3 - As identified in the ANCP - Implementation Guidance, Near-Term 2015-2016, ensure IT Asset Management addresses strategy, process, and repository to provide visibility of IT assets across the network. AESM 1.3.4 - Ensure plans addressing the termination of systems and applications are in place and appropriately implemented as new enterprise services are transitioned.	*See Table 7, Service Transition Measurements, for additional information.*
Known Risk(s) with Mitigation	
Risk: 1. Transitions occur without the guidance of a mature configuration, change management plans, and transition processes. 2. Fiscal constraints impacting ability to transition in a timely manner. 3. Transition efforts fail to terminate and retire redundant or obsolete systems and application in a timely manner. Mitigation: 1. Ensure service transition is governed by an agreed upon and coordinated management plan; ensure plan identifies resources and is designed to meet complex and changing requirements.	

Table 7. Service Transition Measurements

ST CSF	**ST KPI**	**Process/Function Applicability**
ST-CSF 1: Effective planning to properly prepare users, environment, and support teams for scheduled Deployments.	ST-KPI 1.1: Increased client and end-user satisfaction regarding plans and communications.	TPS
ST-CSF 2: An accurate and complete asset management system is established and maintained.	ST-KPI 2.1: Increased quality and accuracy of asset information.	AM
ST-CSF 3: Changes are made efficiently and effectively.	ST-KPI 3.1: Change success rate – how effectively is change managed.	ChM
ST-CSF 4: Major changes are routed through the proper command and control channels.	ST-KPI 4.1: Percent of unsuccessful changes that were not properly evaluated by the appropriate command and control channels.	EVAL

ST-CSF 5: Maintain a complete and comprehensive Configuration Management Plan.	ST-KPI 5.1: Percent of managed Configuration Items (CIs) to known unmanaged CIs.	CfM
ST-CSF 6: High rate of search results delivering usable solutions.	ST-KPI 6.1: Percentage increase in first contact resolution incidents.	ITSKM
ST-CSF 7: The new or changed service has been tested against the Service Design.	ST-KPI 7.1: Number of incidents attributed to deployment.	RDM
ST-CSF 8: Design Validation.	ST-KPI 8.1: Percentage of designs rejected by Customer.	SVT

3-5. AESM Service Operations Rules

Table 8. Service Operations Principles and Rules

<table>
<tr><th colspan="2">Guiding Principles

DoD IEA GP 04 - DoD CIO services shall advertise SLAs that document their performance, and shall be operated to meet that agreement.
DoD IEA SIR 02 - GIG infrastructure capabilities shall be designed, acquired, deployed, operated, and managed in a manner which enables continuity of operations and disaster recovery in the presence of attacks, failures, accidents, and natural or man-made disaster to support customer SLAs.

AESM 1.4, Under the Service Operations life-cycle stage, the Army will:
1. Ensure that IT services are delivered effectively and efficiently.
2. Include fulfilling end-user requests, service failure resolution, fixing problems, and performing routine operational tasks.</th></tr>
<tr><th>DoD IEA/JIE Capability</th><th>AEN Capability</th></tr>
<tr><td>Enabling Capabilities
Users/Operations Requirements (Govern)</td><td>Network Capacity
Enterprise Services
Network Operations & Security
Governance</td></tr>
<tr><th colspan="2">JCA [or Army] Capability Gap(s)</th></tr>
<tr><td colspan="2">JCA 6.2.3 Core Enterprise Services:
1. Lack of collaborative tools, policies, and procedures across the DoD and Federal enterprise.
JCA 6.1.2 Net Management:
1. The lack of end-to-end visibility hinders the effective delivery, management, protection, and oversight of IT services.</td></tr>
<tr><th>Architectural or Business Rule(s) that Mitigate Gaps</th><th>Desired Outcome(s)</th></tr>
<tr><td>AESM 1.4.1 - Ensure SLAs are consistent with SDPs, SMPs, and AESM CONOPS.
AESM 1.4.2 - Ensure SLAs include metrics to support mission effectiveness and continuous process improvement.
AESM 1.4.3 - Develop tools that integrate with and</td><td>Services are in the operational environment with the applicable measures in place to ensure customer needs are being met.</td></tr>
</table>

support processes under the Life-cycle Stages.	See Table 9, Service Operations Measurements, for additional information.
Known Risk(s) with Mitigation	
Risk: 1. Potential network changes and related risks will not be adequately assessed before changes are transitioned or provisioned. 2. Security breaches from incidents or events. 3. DoD and Federal Agencies will be unable to communicate across a common, standards based, collaborative IT environment. Mitigation: 1. Network changes should be verified in applicable development environment before provisioning. 2. Service Operations will have a capability to report security risks to system and service developers.	

Table 9. Service Operations Measurements

SO CSF	SO KPI	Process/Function Applicability
SO - CSF 1: Ability to verify the identity of a user.	SO-KPI 1.1: Number of users logging in with an authoritative credential (e.g., CAC).	AcM
SO-CSF 2: Use appropriate tools for Event and Alert Monitoring supporting automated monitoring of systems and services.	SO-KPI 2.1: Number of events that resulted in Incidents and Problems.	EM
SO-CSF 3: Resolve incidents quickly.	SO-KPI 3.1: Percentage of incidents resolved by first call to 1st Line Support.	IM
SO-CSF 4: Minimize the impact of problems.	SO-KPI 4.1: Percentage of repeat incidents.	PRM
SO-CSF 5: Define standard fulfillment procedures and models.	SO-KPI 5.1: Total number of service requests (as a control measure).	RF
SO-CSF 6: Satisfied customers.	SO-KPI 6.1: Percentage of satisfied customers.	SDF
SO-CSF 7: Successfully resolve Level 2 incidents.	SO-KPI 7.1: Percentage of incidents assigned to Application Management `for resolution.	AMF
SO-CSF 8: Minimize impact of major incidents.	SO-KPI 8.1: Percentage of major incidents resolved within specified time.	ITOMF
SO-CSF 9: Successfully resolve Level 2 incidents.	SO-KPI 9.1: Percentage of incidents assigned to TMF for resolution.	TMF

3-6. AESM Continuous Service Improvement (CSI) Rules

Table 10. Continual Service Improvement Principles and Rules

<table>
<tr><th colspan="2">Guiding Principle

DoD IEA GP 01 - DoD CIO-governed resources are conceived, designed, operated, and managed to address the mission needs of the Department.
DoD IEA GP 02 - Interoperability of solutions across the Department is a strategic goal. All parts of the DoDIN must work together to achieve this goal. Information is made interoperable by following the rules for net-centric sharing of data and services across the enterprise. The DoD achieves infrastructure interoperability through definition and enforcement of standards and interface profiles and implementation guidance.

<b>AESM 1.5, Under the CSI life-cycle stage, the Army will:</b>
Continually align IT services to changing Army mission needs.
Identify and implement improvements throughout the service life-cycle.
Determine what to measure, why to measure it, and define successful outcomes.
Implement processes with clearly defined goals, objectives, and measures.
Review service level achievement results.
Ensure quality management methods are used.</th></tr>
<tr><td>DoD IEA/JIE Capability</td><td>AEN Capability</td></tr>
<tr><td>Enabling Capabilities
Users/Operations Requirements (Govern)</td><td>Network Capacity
Enterprise Services
Network Operations & Security
Governance</td></tr>
<tr><td colspan="2">JCA [or Army] Capability Gap(s)</td></tr>
<tr><td colspan="2">JCA 6.2.3 Core Enterprise Services; Architecture, Policy and Compliance:
1. Lack of implementation of processes, procedure, and change with clearly defined goals, objectives, and measures.</td></tr>
<tr><td>Architectural or Business Rule(s) that Mitigate Gaps</td><td>Desired Outcome(s)</td></tr>
<tr><td>AESM 1.5.1 - Implement the 7 Step Improvement Process: Opportunities for improvement throughout the IT Service life-cycle will be identified via the implementation of the seven step process.</td><td>IT services are continually and efficiently managed for improvement to ensure mission security and effectiveness.
See Table 11, Continual Service Improvement Measurements, for additional information.</td></tr>
<tr><td colspan="2">Known Risk(s) with Mitigation</td></tr>
<tr><td colspan="2">Risk:
1. Costs of enterprise service improvements exceed planned budgets.
Mitigation:
1. Ensuring the Army’s path to continual service improvement is aligned with the 7 Step Improvement Process.
2. Service improvements designed to ensure they meet desired service requirements.
3. Service improvements flexible enough to absorb non-critical problems without</td></tr>
</table>

impacting service levels.

Table 11. Continual Service Improvement Measurements

CSI CSF	CSI KPI	Process/Function Applicability
CSI-CSF 1: Identify improvement opportunities.	CSI-KPI 1.1: Number of improvement opportunities logged in the CSI register.	7 Step Improvement Process

Chapter 4
Implementation Patterns

a. Implementation patterns are a collection of perspectives, descriptions, models (e.g., DoDAF), and views that guide and support activities for transition and implementation. It is anticipated that these patterns will be used for such activities as follows:

(1) Development of life-cycle stage/processes (e.g., event sequencing).

(2) Establishment of governance (e.g., roles and responsibilities).

(3) Definition and integration of architecture.

(4) Development of solution architecture (e.g., System of Systems RA, Common Operation Environment RA).

(5) Management of service maturity.

b. For this version of the RA, two patterns are provided:

(1) The Activity Pattern (using DoDAF models) applies to all Life-cycle Stages and is provided to support overall architecture integration.

(2) The Service Desk pattern is a result of the application of principles and rules identified under the Service Operations life-cycle stage; it is provided to guide the development and implementation of Service Desk processes.

c. As other patterns are identified and developed during the establishment and implementation of AESMF efforts, they will be documented in updated AESM RAs as applicable.

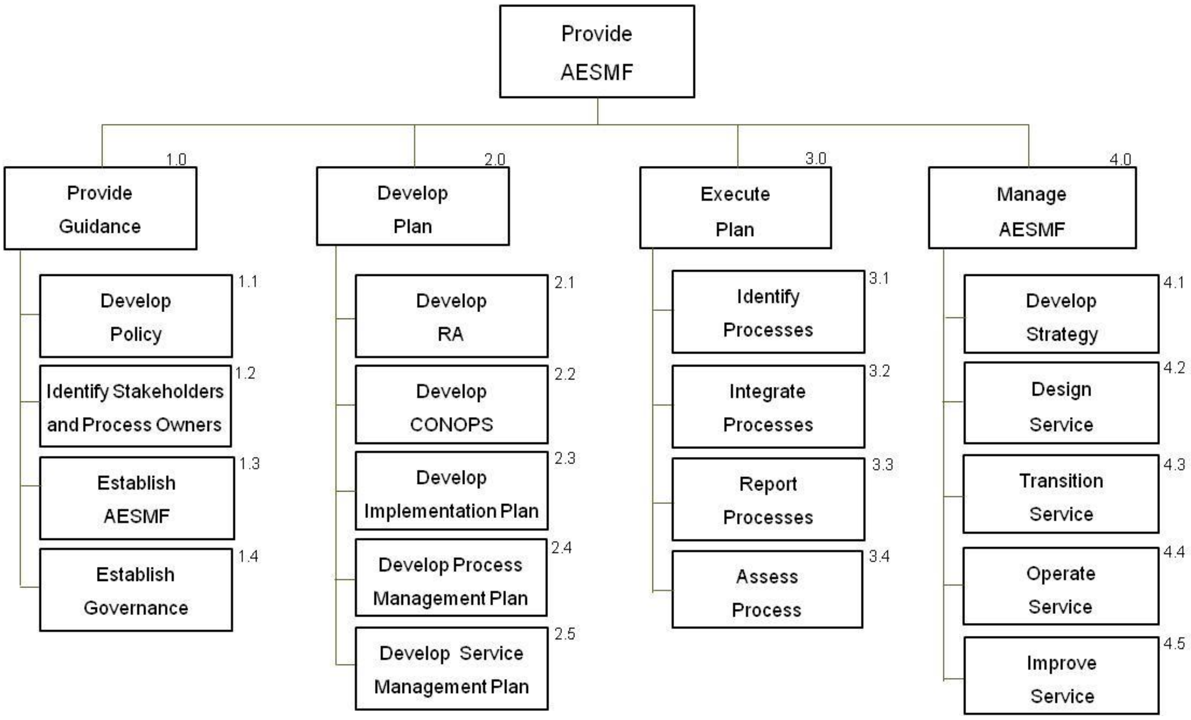
4-1. Activity Pattern

a. Figure 7 below shows the four main first-level activities involved in the establishment of the framework as well as the execution of processes under AESMF. The activities are numbered (1.0, 2.0, etc.) and are not necessarily sequential in this diagram.[8] The five second-level activities under Manage AESMF are also shown, and they are aligned with the five AESMF Life-cycle Stages described in Table 1.[9]

[8] Actual sequencing of activities can be shown in a different DoDAF model.

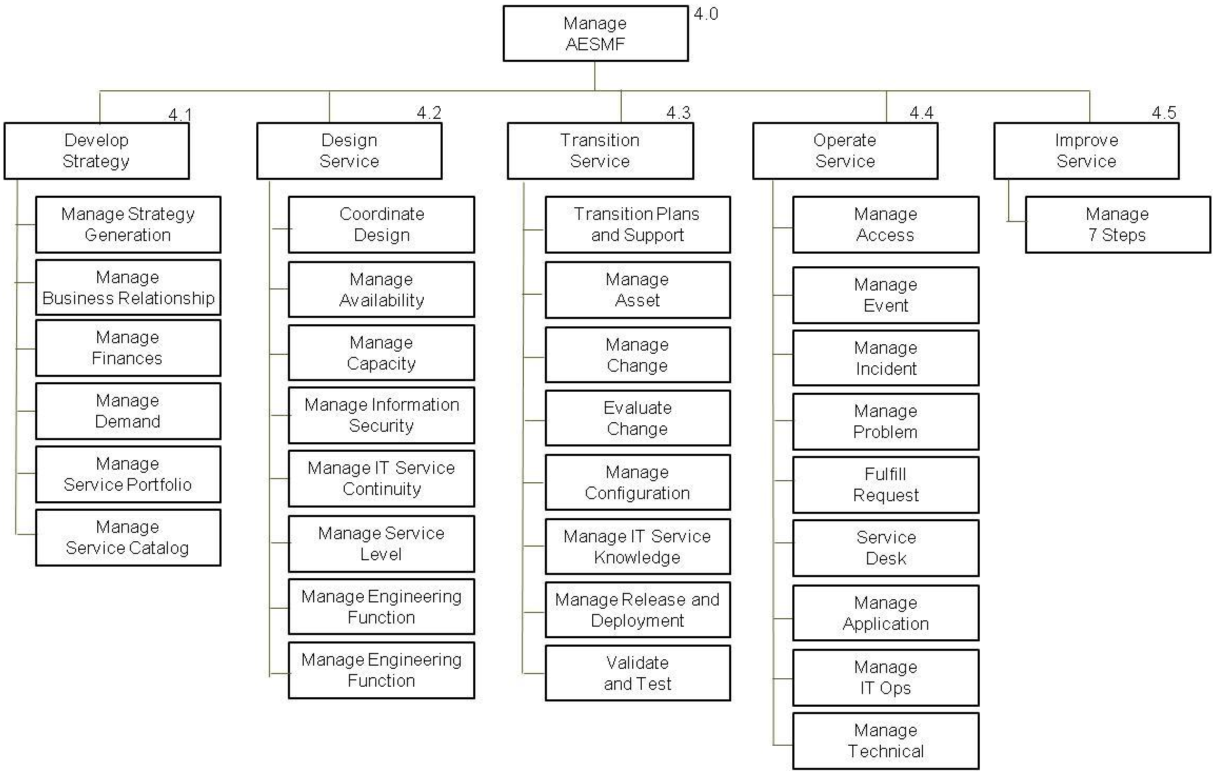
[9] An “activity” in the OV-5a corresponds to a “stage” in the AESMF Life-cycle Stages table. The processes identified under each stage can be considered a collection of activities.

Figure 7. Operational Activity Decomposition Tree for Provide AESMF (OV-5a)



b. Under Manage AESMF, the second-level activities are further decomposed into third-level activities (e.g., Manage Strategy Generation and Manage Business Relationship are two particular decompositions under the Develop Strategy activity). Figure 8 below details the third-level decompositions of each of the five second-level activities.

Figure 8. Operational Activity Decomposition Tree for Manage AESMF (OV-5a)



c. Figure 9 depicts how resources (e.g., data) will flow between the four first-level activities (Provide Guidance, Develop Plan, Execute Plan and Manage AESMF). Also, for illustrative purposes, only a few data flows are shown (e.g., AESM CONOPS, KPI/CSF) between activities.

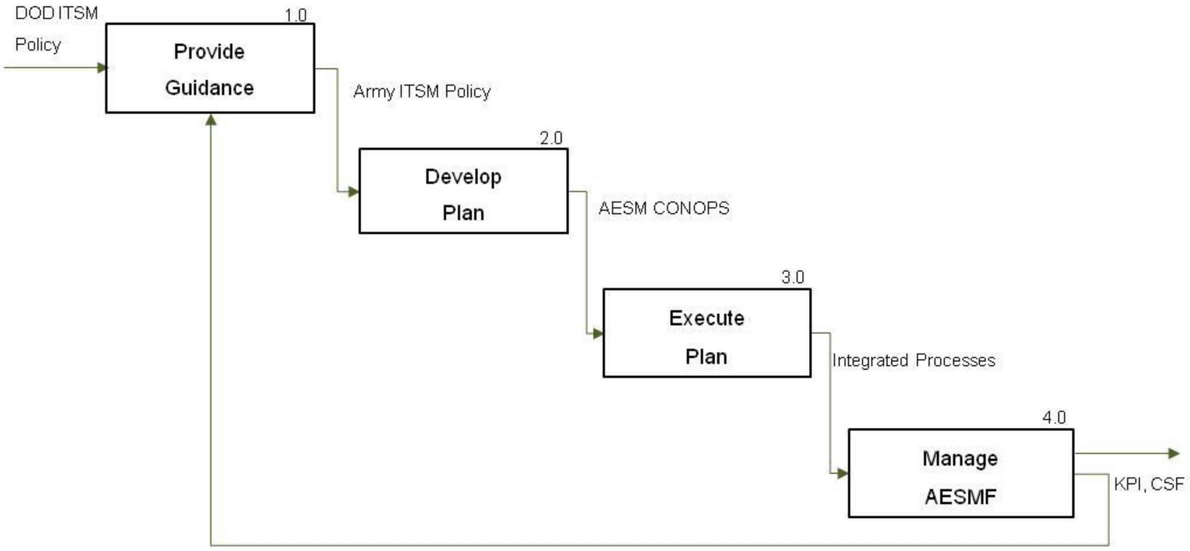


Figure 9. Operational Activity Model for Provide AESMF (OV-5b)

4-2. Service Desk Pattern

a. The Service Desk function is identified under the Operate Service life-cycle stage. Figure 10 below depicts the Army Enterprise Service Desk (AESD) model adapted for the Army based upon the JIE Enterprise Service Desk Model found in the JIE Operations CONOPS v2.0. The AESD model depicts a unified construct to provide a single point of contact (SPOC) to all Army users for incidents, service requests, and other service management activities across a Tier 0 through Tier 3 support model for Army and DoD Enterprise services. Each tier is defined as follows:

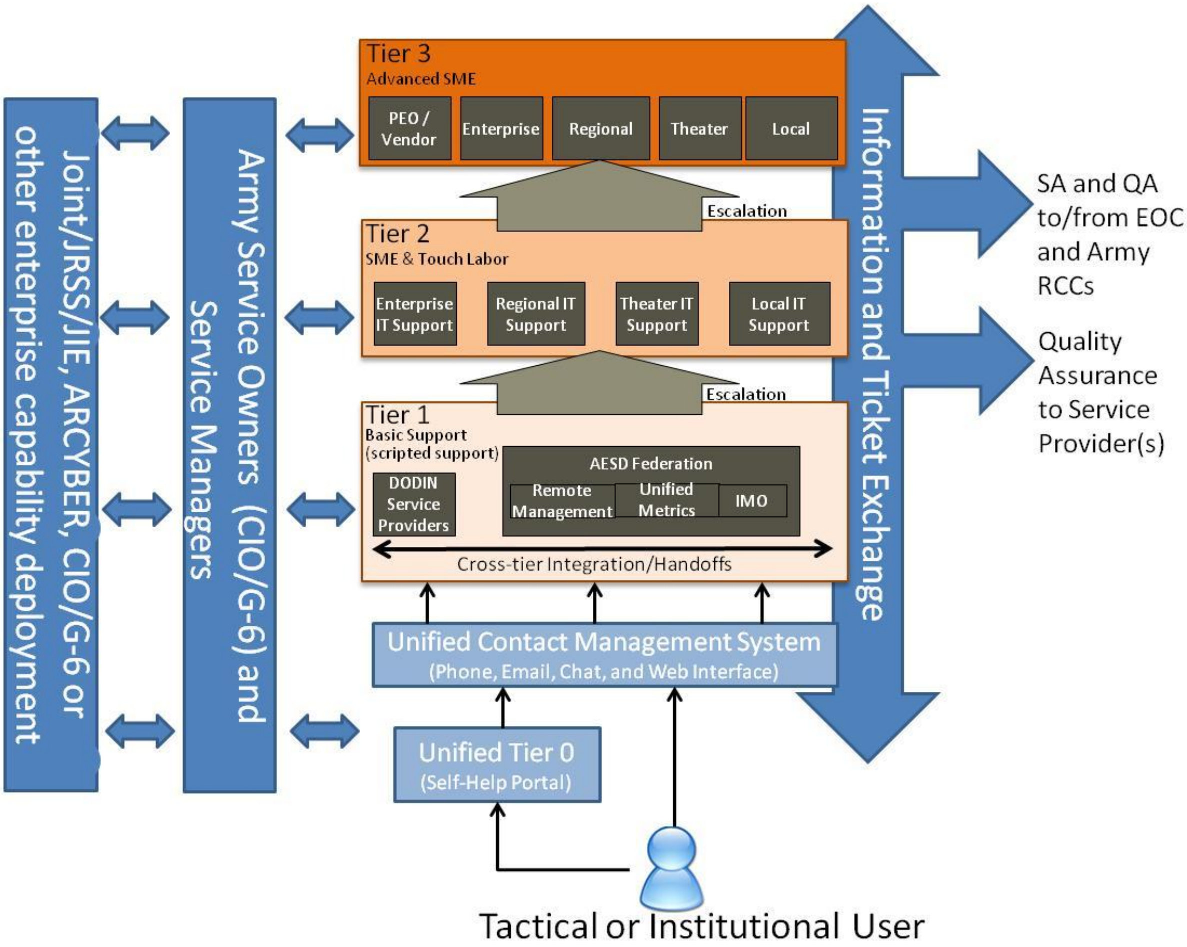
(1) **Tier 0, Self-Help.** Provides automated service desk functions and a user-facing knowledge base for common issues with the use of a portal. Tier 0 aims to minimize a user's need to interact directly with service desk personnel by providing an efficient self-help service via interactive phone, chat, email, and web functions for the most common reasons.

(2) **Tier 1, Basic Support.** Provides a unified construct consisting of components from the AESD Federation or DoDIN Service Providers (Commercial or Government) that provide IT services to Army organizations. Tier 1 IT Support can provide basic service for restoral and fulfillment. This basic support is limited to support that has been pre-scripted by the service provider and/or operational community. Tier 1 also manages all user interactions to the service desk from beginning to end, including coordinating Tier 2 and 3 responses. Tier 1 is a distinct operational entity within the AESM concept dedicated to performing service desk support functions.

(3) **Tier 2, Touch Labor and Subject Matter Expertise.** Provides two major subcomponents: touch labor and subject matter expertise (SME). Both roles handle requests beyond the scope of Tier 1 basic and scripted support across enterprise, regional, theater, and local IT support organizations. These organizations include the Enterprise Operations Centers (EOC), Regional Cyber Centers (RCC), Theater Network Operations Support Centers (TNOSC), Network Enterprise Centers (NEC) and local Army IT support organizations; they fulfill the two roles in coordination with the service provider.

(4) **Tier 3, Advanced Subject Matter Expertise.** Tier 3 consists of engineers who resolve user requests or issues that are beyond the expertise of Tier 2 personnel. This includes investigating root causes and interfacing with vendors and developers. Tier 3 personnel are provided by the service provider and align operationally to the lead enterprise, regional or theater IT support organization for the respective Army and DoDIN enterprise service. Tier 3 personnel support Tier 1 personnel until the user's request or issue is resolved.

Figure 10. Army Enterprise Service Desk Model


Tier 3
Advanced SME
PEO / Vendor
Enterprise
Regional
Theater
Local
Escalation
Tier 2
SME & Touch Labor
Enterprise IT Support
Regional IT Support
Theater IT Support
Local IT Support
Escalation
Tier 1
Basic Support (scripted support)
DODIN Service Providers
AESD Federation
Remote Management
Unified Metrics
IMO
Cross-tier Integration/Handoffs
Unified Contact Management System
(Phone, Email, Chat, and Web Interface)
Unified Tier 0
(Self-Help Portal)
Tactical or Institutional User
Joint/JRSS/JIE, ARCYBER, CIO/G-6 or other enterprise capability deployment
Army Service Owners (CIO/G-6) and Service Managers
Information and Ticket Exchange
SA and QA to/from EOC and Army RCCs
Quality Assurance to Service Provider(s)

b. In addition to the service desk tiers, Figure 10 depicts the primary supporting technical capabilities necessary for a unified service desk. The AESD model requires the three technical capabilities described as follows:

(1) Unified Contact Management System (UCMS). All forms of interaction between the user and the Tier 1 service desk will be managed through a UCMS.

(2) Information and Ticket Exchange. Information and Ticket Exchange integrates processes and the flow of information across Tier 1, 2, and 3 entities and the UCMS provides seamless transitions between service desk elements and an enhanced end-user experience. The unified ticketing workflow will also provide quality assurance metrics and situational awareness to the service providers, RCCs, and EOCs.

(3) Knowledge sharing between Tiers, Service Owners, and Managers. The service desk will share scripted tactics, techniques, and procedures (TTP), frequently asked questions, known errors, and other knowledge between all service desk components in order to improve effectiveness of the service desk function and Army Enterprise Services. This will move knowledge from higher tiers down to lower tiers, including providing the base knowledge for the Tier 0 self-help, to support user requests more efficiently.

c. In support of higher level AESM principles and rules, Table 12 below lists specific rules to support the development of the Service Desk function.

Table 12. Implementation Rules for the Service Desk Process

ID #	Implementation Rule	Desired Outcome
AESD 1.3.1	Adopt common DoD and Army standards to automate information exchanges between UCMS, Tiers (1, 2, 3), and IT operational entities.	Enhanced end-user experience Increased cyber situational awareness and security Reduce costs of multiple ESM processes and platforms.
AESD 1.3.2	The UCMS must support all service contact channels: - Communication technology such as computer telephony integration or Voice over Internet Protocol - Interactive voice response systems - Email, fax servers (fax via email or the Internet), forwarding calls to pagers, mobile phones, laptop and palmtop computers - Web-based, self-service platforms	Rapid response, resolution and/or restoration of enterprise services.
AESD 1.3.3	AESM platforms must enable a unified ticketing workflow to ensure data exchange that support coordination and defense of the DoDIN and Army IT Services across all Tiers.	Enhanced end-user experience Army-coordinated response to emergent cyber threats and network outages.
AESD 1.3.4	AESM platforms allow the AESD federation to provide Tier 1 support for Army enterprise services: - Army Knowledge Online - DoD Enterprise Email - Enterprise Content Management and Collaboration Services - Mobile Devices on the Mobile Device Manager	Standardized Service management platforms to reduce costs and increase security.

Chapter 5
Summary

a. The Army has used industry ITSM best practices in varying degrees since 2003. However, the lack of a holistic and integrated approach and standardized processes across all Army IT service providers has inhibited the Army’s ability to manage its enterprise IT services effectively or to make sound strategic and investment decisions to achieve the ANCP objectives and vision for the LWN 2020 & Beyond EA. This AESM RA, in support of DESMF and AESMF, provides the principles, rules, and guidance that will standardize ITSM in support of the Army’s continuing efforts to manage services efficiently and effectively while achieving greater security and mission effectiveness.

Appendix A References

A-1. U.S. Army References

1. AR 25-1, Army Information Technology, 25 June 2013; http://www.apd.army.mil/pdffiles/r25_1.pdf
2. AR 25-2, Information Assurance, 23 March 2009; http://armypubs.army.mil/epubs/pdf/r25_2.pdf
3. DA PAM, 25-1-1, Army Information technology Implementation Instructions, 26 September 2014; http://www.apd.army.mil/pdffiles/p25_1_1.pdf
4. Army Network Campaign Plan 2020 and Beyond; ANCP-Implementation Guidance, Near-Term 2015-2016; ANCP-Implementation Guidance, Mid-Term 2017-2021; http://ciog6.army.mil/AboutCIO/Mission/ANCP/tabid/237/Default.aspx
5. Army Cyber Command (ARCYBER) & Second Army, Army Enterprise Service Management (AESM) Concept of Operations (CONOPS), Version 1.0, 18 December 2014; https://army.deps.mil/army/cmds/hqda_ciog6/PR/PRU/HQDA-ITSM/Shared%20Documents/Forms/AllItems.aspx
6. Army IT Reform Implementation Plan with 2015 Directive, 20 February 2013; http://ciog6.army.mil/Portals/1/Policy/2012/Information%20Technology%20Management%20Reform%20Implementation%20Plan_20Feb13.pdf
7. Army CIO/G-6 Memorandum, Army Information Technology Service Management (ITSM) Policy, 17 November 2014; http://ciog6.army.mil/Portals/1/Policy/2015/Army%20ITSM%20Policy_17Nov2014.pdf
8. LandWarNet 2020 and Beyond Enterprise Architecture, Version 2.0, 30 July 2014; http://ciog6.army.mil/Architecture/tabid/146/Default.aspx

A-2. DoD/JIE References

9. DoD Enterprise Service Management Framework Edition II, 8 November 2013;
10. https://community.apan.org/esmf_consortium_working_groups/m/desmf_edition_iii/default.aspx or https://www.milsuite.mil/book/docs/DOC-198729?sr=stream&ru=448259
11. DoD CIO memo: DoD CIO Executive Board Charter (Architecture Management and EIEMA domain oversight), 7 July 2005; http://DoDcio.defense.gov/Portals/0/Documents/DoD_CIO_ExecutiveBoardCharter.pdf
12. DoD Information Enterprise Architecture, Version 2.0, July 2012; http://DoDcio.defense.gov/Home/Initiatives/DIEA.aspx
13. DoD IT Standards Registry, under Global Information Grid Technical Profiles (GTP); https://gtg.csd.disa.mil/disr/dashboard.html
14. DoDD 8115.01, Information Technology Portfolio Management, 10 October 2005;

15. http://DoDcio.defense.gov/Portals/0/Documents/DIEA/811501p.pdf
16. DoDI 8410.02, NetOps for the Global Information Grid, 19 December 2008; http://www.dtic.mil/whs/directives/corres/pdf/841002p.pdf
17. DoDI 8410.03, Network Management, 29 August 2012; http://www.dtic.mil/whs/directives/corres/pdf/841003p.pdf
18. DoD Memorandum, DoD CIO, ITSM in the DoD, 15 May 2013; https://army.deps.mil/army/cmds/hqda_ciog6_Project/UC/ETM/Demo/TAB_C_DoD_CIO_Memo_15_May_2013.pdf
19. Joint Information Environment (JIE) Operations Concept of Operations (CONOPS), 25 January 2013; https://army.deps.mil/army/cmds/hqda_ciog6_Project/JIE/CONOPs/Forms/AllItems.aspx
20. Joint Publication 6-0 Joint Communications System, 10 June 2010; https://jdeis.js.mil/jdeis/index.jsp?pindex=27&pubId=235

A-3. Other References

21. Committee on National Security Systems (CNSS);
22. http://www.cnss.gov/
23. Committee on National Security Systems Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems, 15 March 2012;
24. http://www.sandia.gov/FSO/PDF/flowdown/Final_CNSSI_1253.pdf
25. National Information Exchange Model (NIEM);
26. http://www.ise.gov/national-information-exchange-model-niem
27. NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems;
28. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
29. NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
30. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
31. NIST Interagency Report 7298 Revision 2, Glossary of Key Information Security Terms, May 2013;
32. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
33. OMB Management Act and Agency Privacy Management; http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf
34. OMB M-10-15 — FY 2010 Reporting Instructions for the Federal Information Security
35. ISO/IEC 20000, The Information Technology – Service Management standards; http://www.iso.org/iso/home.htm

Appendix B
Glossary of Acronyms

a. The following acronyms are applicable within this document.

Acronym	Description
AAIC	Army Architecture Integration Center
AcM	Access Management
ACOM	Army Commands
AEN	Army Enterprise Network
AESD	Army Enterprise Service Desk
AESM	Army Enterprise Service Management
AESMF	Army Enterprise Service Management Framework
AM	Asset Management
AMF	Application Management (Function)
ANCP	Army Network Campaign Plan
AR	Army Regulation
ArCADIE	Army Capability-Based Architecture Development and
ARCYBER	Army Cyber
ARSTAF	Army Staff
ASCC	Army Service Component Commands
AV	All Viewpoint
AvM	Availability Management
BRM	Business Relationship Management
C4IM	Command, Control, Communications, Computers, and
CAC	Common Access Card
CapM	Capacity Management
CfM	Configuration Management
ChM	Change Management
CI	Configuration Item
CIO/G-6	Chief Information Officer/G-6
CIRP	Computing Infrastructure Readiness Principles
CIRR	Computing Infrastructure Readiness Business Rules
CNSSI	Committee on National Security Systems Instruction
COBIT	Control Objectives for Information and Related Technology
COE	Common Operating Environment
CONOPS	Concept of Operations
CSF	Critical Success Factors
CSI	Continuous Service Improvement
CV	Capability Viewpoint
DA	Department of the Army
DC	Design Coordination

DESMF	Defense Enterprise Service Management Framework
DISR	DoD Information Technology Standards Registry
DISA	Defense Information Systems Agency
DM	Demand Management
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoD IEA	Department of Defense Information Enterprise Architecture
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network
EA	Enterprise Architecture
EIEMA	Enterprise Information Environment Mission Area
EM	Event Management
ENGF	Engineering (Function)
EOC	Enterprise Operations Center
ESD	Enterprise Services Domain
ESM	Enterprise Service Management
ESR	Enterprise Strategy and Implementation Roadmap
EVAL	Change Evaluation
EXORD	Execution Order
FM	Financial Management for IT Services
FY	Fiscal Year
GIG	Global Information Grid
GP	Global Principle (DoD IEA)
GTP	Global Information Grid Technical Profiles
HQDA	Headquarters, Department of the Army
IE	Information Enterprise
IEA	Information Enterprise Architecture
IM	Incident Management
IMO	Information Management Office
ISO/IEC	International Organization for Standardization / International
ISM	Information Security Management
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITMR	Information Technology Management Reform
ITOMF	IT Operations Management (Function)
ITSCM	IT Service Continuity Management
ITSKM	IT Services Knowledge Management
ITSM	Information Technology Service Management
JCA	Joint Capability Area

JIE	Joint Information Environment
JRSS	Joint Regional Security Stack
KPI	Key Performance Indicator
LWN	LandWarNet
NetOps	Network Operations
NCD	Network Capacity Domain
NEC	Network Enterprise Centers
NETCOM	Network Enterprise Technology Command
NIEM	National Information Exchange Model
NIST	National Institute of Standards & Technology
NPRM	Navy Process Reference Model
NSD	Network Operations & Security Domain
OMB	Office of Management and Budget
OPR	ORA-Derived Operational Rules
ORA	Operational Reference Architecture
OV	Operational Viewpoint
PEO	Program Executive Office
PEO EIS	Program Executive Office for Enterprise Information Systems
PM	Problem Management
PMP	Process Management Plans
PRM	Problem Management
QA	Quality Assurance
RA	Reference Architecture
RCC	Regional Cyber Centers
RDM	Release and Deployment Management
RF	Request Fulfillment
SA	Situational Awareness
SAP	Secured Availability Principles
SCM	Service Catalog Management
SD	Service Design
SDF	Service Desk (Function)
SDP	Service Design Package
SGM	Strategy Generation Management
SIR	Shared Infrastructure Business Rules
SLA	Service Level Agreement
SLM	Service Level Management
SME	Subject Matter Expert
SMP	Service Management Plans
SO	Service Operations
SOP	Standard Operating Procedure

SP	Special Publication
SPM	Service Portfolio Management
SPOC	Single Point of Contact
SS	Service Strategy
SSM	Service Support Model
ST	Service Transition
StdV	Standard Viewpoints
SUP	Supplier Management
SVT	Service Validation and Testing
TMF	Technical Management (Function)
TNOSC	Theater Network Operations Support Center
TPS	Transition Planning and Support
TTP	Tactics, Techniques, and Procedures
UAP	Unified Action Partners
UCMS	Unified Contact Management System

Appendix C
Integrated Dictionary (AV-2)

a. In context with this RA, vocabulary and terms will be referred to as the All Viewpoint (AV)-2 Integrated Dictionary.

Term	Description	Reference
Access	Ability to make use of any information system resource.	NIST Interagency Report 7298 Revision 2, Glossary of Key, Information Security Terms, May 2013
Activity	A set of actions designed to achieve a particular result. Activities are usually defined as part of processes or plans, and are documented in procedures.	ITIL® V3 Glossary, v1.0, 2011
Application	Software that provides functions which are required by an IT service. Each application may be part of more than one IT service. An application runs on one or more servers or clients. *See also* application management.	ITIL® V3 Glossary, v1.0, 2011
Application Management	This function is responsible for managing applications throughout their life-cycle. It is performed by the IT teams that are involved in providing control of and operational support for applications. Application management plays a key role in designing, testing and improving applications; this represents the functional part of an IT service. Application Management teams are also involved in system and software development projects.	Army Cyber Command & Second Army, Army Enterprise Service Management Concept of Operations, Version 1.0, 18 December 2014
Army Operations Process	Army's framework for exercising mission command is the operations process - The major mission command activities performed during operations: planning, preparing, executing, and continuously assessing the operation. Commanders, supported by their staffs, use the operations process to drive the conceptual and detailed planning necessary to understand, visualize, and describe their operational environment; make and articulate decisions; and direct, lead, and assess military operations.	Army Doctrinal Publication 5-0; The Operations Process, 17 May 2012

Term	Description	Reference
Asset	Resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service. Assets can be one of the following types: Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, or Financial Capital.	ITIL® V3 Glossary, v1.0, 2011
Capacity	(*ITIL Service Design*) The maximum throughput that a configuration item or IT service can deliver. For some types of CI, capacity may be the size or volume – for example, a disk drive.	ITIL® V3 Glossary, v1.0, 2011
Command, Control, Communications and Computers Information Management (C4IM) Services List	The C4IM Services List is the foundation for the LWN Services Catalog. The LWN Services Catalog is the customer-facing document that will be used to identify standards for delivery of services based on funding constraints. The catalog provides standard descriptions and performance standards of C4IM services that are available to support Army organizations residing on U.S. Army posts, camps, and stations based on the amount of resources received.	Secretary of the Army Memorandum, "Army Command, Control, Communications, Computers and Information Management Service List Version 3.0, 28 July 2011
Configuration Item (CI)	Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each CI is recorded in a configuration record within the configuration management system and is maintained throughout its life-cycle by service asset and configuration management. CIs are under the control of change management. They typically include IT services, hardware, software, products buildings, people, and formal documentation such as process documentation and service level agreements.	Defense Information Systems Agency (DISA) ITSM Instruction

Term	Description	Reference
Continual Service Improvement (CSI)	(*ITIL Continual Service Improvement*) A stage in the life-cycle of a service. Continual service improvement ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes. The performance of the IT service provider is continually measured and improvements are made to processes, IT services, and IT infrastructure in order to increase efficiency, effectiveness and cost effectiveness. Continual service improvement includes the 7 Step Improvement Process. Although this process is associated with continual service improvement, most processes have activities that take place across multiple stages of the service life-cycle.	ITIL® V3 Glossary, v1.0, 2011
Critical Success Factors (CSF)	Something that must happen if an IT service, process, plan, project, or other activity is to succeed. Key performance indicators are used to measure the achievement of each critical success factor. For example, a critical success factor of "protect IT services when making changes" could be measured by key performance indicators such as "percentage reduction of unsuccessful changes," "percentage reduction in changes causing incidents," etc.	ITIL® V3 Glossary, v1.0, 2011
Customer	Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees the service level targets. The term is also sometimes used informally to mean user – for example, "This is a customer-focused organization."	ITIL® V3 Glossary, v1.0, 2011

Term	Description	Reference
Event	(*ITIL Service Operation*) A change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item, or monitoring tool. Events typically require IT operations personnel to take action (e.g., logging incidents).	ITIL® V3 Glossary, v1.0, 2011
Enterprise Service	An enterprise service is any capability provided for broad use across the DoD that enables awareness of, access to, or delivers information across DoD networks. Enterprise services may be provided by any source within the DoD or any trusted partners. Enterprise services providing data or information must be authoritative and, therefore, trusted as being accurate, complete, and having assured integrity. Authoritative information has a pedigree that can be traced to a trusted source. Enterprise services include environments that are composed of multiple service layers such as the infrastructure, infrastructure services, platform services, common user services, enterprise service management, and mission assurance services.	DoD Instruction (DoDI) 8330.01, Interoperability of IT including National Security Systems, 21 May 2014
Function	A team or group of people and the tools or other resources they use to carry out one or more processes or activities – for example, the service desk. The term also has two other meanings: An intended purpose of a configuration item, person, team, process, or IT service. For example, one function of an email service may be to store and forward outgoing mails, while the function of a business process may be to dispatch goods to customers. To perform the intended purpose correctly, as in “The computer is functioning.”	ITIL® V3 Glossary, v1.0, 2011

Term	Description	Reference
Incident	(*ITIL Service Operation*) An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident – for example, failure of one disk from a mirror set.	ITIL® V3 Glossary, v1.0, 2011
IT Service Management (ITSM)	A set of specialized organizational capabilities to manage IT services through a set of defined, repeatable, measurable, implemented, and integrated processes that control the quality, performance, and reliability of IT services.	DoDI 8440.cc Draft
Key Performance Indicator (KPI)	(*ITIL Continual Service Improvement*) (*ITIL Service Design*) A metric that is used to help manage an IT service, process, plan, project, or other activity. Key performance indicators are used to measure the achievement of critical success factors. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service, or activity. They should be selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed.	ITIL® V3 Glossary, v1.0, 2011
Live Environment	(*ITIL Service Transition*) A controlled environment containing live configuration items used to deliver IT services to customers.	ITIL® V3 Glossary, v1.0, 2011
Metric	(*ITIL Continual Service Improvement*) Something that is measured and reported to help manage a process, IT service or activity. See also *key performance indicator*.	ITIL® V3 Glossary, v1.0, 2011
Problem	(*ITIL Service Operation*) A cause of one or more incidents. The cause is not usually known at the time a problem record is created, and the problem management process is responsible for further investigation.	ITIL® V3 Glossary, v1.0, 2011

Term	Description	Reference
Process	The Army's framework for exercising mission command is the operations process—the major mission command activities performed during operations: planning, preparing, executing, and continuously assessing the operation.	Army Doctrine Reference Publication THE OPERATIONS PROCESS 5-0; 17 May 2012
Product	A CI or collection of CIs that have physical characteristics, are manufactured, and are used to deliver a capability or function or series of capabilities and functions.	ITIL® V3 Glossary, 30 May 2007
Release	(*ITIL Service Transition*) One or more changes to an IT service that are built, tested, and deployed together. A single release may include changes to hardware, software, documentation, processes, and other components.	ITIL® V3 Glossary, v1.0, 2011
Request Fulfillment	The process responsible for managing the life-cycle of all service requests.	ITIL® V3 Glossary, 30 May 2007
Service	A service is a means of delivering value comprising people, processes, and technology perceived by customers and users as a self-contained, single, coherent entity that enables them to achieve mission objectives and functions.	ISO 20000, COBIT 5, ITIL V.2 & 3
Service Catalog	(*ITIL Service Design*) (*ITIL Service Strategy*) A database or structured document with information about all live IT services, including those available for deployment. The service catalog is part of the service portfolio and contains information about two types of IT service: customer-facing services that are visible to the business; and supporting services required by the service provider to deliver customer-facing services.	ITIL® V3 Glossary, v1.0, 2011
Service Design Package (SDP)	(*ITIL Service Design*) Document(s) defining all aspects of an IT service and its requirements through each stage of its life-cycle. A service design package is produced for each new IT service, a major change to a service, or IT service retirement.	ITIL® V3 Glossary, v1.0, 2011

Term	Description	Reference
Service Knowledge Management Systems	A set of tools and databases that is used to manage knowledge, information and data. The service knowledge management system includes the configuration management system as well as other databases and information systems. The service knowledge management system includes tools for collecting, storing, managing, updating, analyzing, and presenting all of the knowledge, information, and data that an IT service provider will need to manage the full life-cycle of IT services.	ITIL® Glossary and abbreviations, ©AXELOS 2011
Service Improvement Plan	(*ITIL Continual Service Improvement*) A formal plan to implement improvements to a process or IT service.	ITIL® V3 Glossary, v1.0, 2011
Service Level	Measured and reported achievement against one or more service level targets. The term is sometimes used informally to mean service level target.	ITIL® V3 Glossary, v1.0, 2011
Service Level Agreement (SLA)	(*ITIL Continual Service Improvement*) (*ITIL Service Design*) An agreement between an IT service provider and a customer. A service level agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single agreement may cover multiple IT services or multiple customers. Compare with Operational Level Agreement used in Army AESM CONOPS, Version 1.0,18 December 2014.	ITIL® V3 Glossary, v1.0, 2011

Term	Description	Reference
Service Provider	(*ITIL Service Strategy*) An organization supplying services to one or more internal customers or external customers. Service provider is often used as an abbreviation for IT service provider. Examples of organizations that provide IT services: DISA and Army IT organizations (including Headquarters, Department of the Army [HQDA] CIO/G-6, Program Executive Office for Enterprise Information Systems [PEO EIS], Army Cyber [ARCYBER] & Second Army, and Network Enterprise Technology Command [NETCOM]).	ITIL® V3 Glossary, v1.0, 2011
Service Request	(*ITIL Service Operation*) A formal request from a user for something to be provided – for example, a request for information or advice; to reset a password; or to install a workstation for a new user. Service requests are managed by the request fulfillment process, usually in conjunction with the service desk. Service requests may be linked to a request for change as part of fulfilling the request.	ITIL® V3 Glossary, v1.0, 2011
Shared IT Service	An IT service that is consumed by more than one DoD Component or other Federal Agency.	DoDI 8440.cc Draft
Supplier	(*ITIL Service Design*) (*ITIL Service Strategy*) A third party responsible for supplying goods or services required to deliver IT services. Examples of suppliers include commodity hardware and software vendors, network and telecom providers, and outsourcing organizations.	ITIL® V3 Glossary, v1.0, 2011
Technical Management	(*ITIL Service Operation*) The function responsible for providing technical skills in support of IT services and management of the IT infrastructure. Technical management defines the roles of support groups, as well as the tools, processes, and procedures required.	ITIL® V3 Glossary, v1.0, 2011

Term	Description	Reference
Unified Action Partners (UAP)	Those military forces, governmental and nongovernmental organizations, and elements of the private sector with whom Army forces plan, coordinate, synchronize, and integrate during the conduct of operations.	Army Doctrine Reference Publication, No. 3-0, Unified Land Operations, 16 May 2012
Unified Capabilities (UC)	UCs are the integration of voice, video, and/or data services delivered ubiquitously across a secure and highly available network infrastructure, independent of technology, to provide increased mission effectiveness to the warfighter and business communities.	Air Force and Army UC Implementation Plan, Version 1.0, October 2013
User	A person who uses the IT service on a day-to-day basis. Users are distinct from customers, as some customers do not use the IT service directly.	ITIL® V3 Glossary, v1.0, 2011

Appendix D
Technical Standards Profiles (StdV-1 & StdV-2)

a. Army standards are identified under the DoD Information Technology Standards Registry (DISR) service areas found within Appendix C to Annex A of LandWarNet 2020 and Beyond Enterprise Architecture: Army Standards Profile Guidance In Support of Common Operating Environment (COE) v3.

b. The Standards Profile (StdV-1), Standards Forecast (StdV-2), and Non-DISR Standards can be found on http://ciog6.army.mil/Architecture/tabid/146/Default.aspx.

Appendix E
Principles/Rules in Enterprise Reference Architecture

a. Guiding principles represent the highest level of guidance for IT planning and decision making. They are high-level statements that apply to specific warfighting and business requirements.

b. Table 13 below illustrates how these principles and rules are presented in CIO/G-6 Enterprise Reference Architectures. The table is organized as follows:

(1) Applicable enterprise guiding principles and rules (derived from the DoD IEA and Army sources) are shown here.

(2) Associated with each guiding principle is a reference to applicable DoD IEA capability and AEN capability.

(3) Gaps within the current network are identified as related to specific JCAs.

(4) From identified gaps, a set of rules are listed; desired outcomes are results of applied rules.

(5) If implementation of a rule warrants additional consideration (or if a known risk exists), this information will be provided to facilitate future risk mitigation and serve as documentation of the current challenges associated with AESM.

Table 13. Enterprise Reference Architecture Principle & Rule Illustration

<table>
<tr><th colspan="2"><b>Guiding Principle</b>
DoD IEA GP x.x., Global Principles (or Rules) extracted from the DoD IEA.
Army Principle Title, Army Principle(s) derived from DoD IEA Principles.</th></tr>
<tr><td>DoD IEA/JIE Capability</td><td>AEN Capability</td></tr>
<tr><td>Identified capabilities.</td><td>Identified capabilities.</td></tr>
<tr><td colspan="2">JCA or Army Capability Gap(s)</td></tr>
<tr><td colspan="2">Identified gaps in a specific capability area.</td></tr>
<tr><td>Architecture Rule(s) that Mitigate Capability Gap</td><td>Desired Outcome(s)</td></tr>
<tr><td>Architectural rules (constraints /guidance) that need to be adhered to in order to satisfy the capability gap & standards to follow.</td><td>Specific outcomes that will be achieved with successful implementation of the rules.</td></tr>
<tr><td colspan="2">Known Risk(s) with Mitigation</td></tr>
<tr><td colspan="2">Identified considerations, risks, challenges and mitigation associated with implementing the identified rules.</td></tr>
</table>

Administrative Information

Approval Authority. HQDA CIO/G-6.

Recommendations, concerns, and questions. Please send these to the Document Custodian.

Next scheduled document update. There currently is no scheduled update.

Distribution and Use Restrictions. This document is intended for use by US Government agencies and their Contractors doing business with the U.S. Army.

Document Custodian. The Custodian for this document is HQDA CIO/G-6, SAIS-AEA, usarmy.pentagon.hqda-cio-g-6.list.architecture@mail.mil.

---Nothing follows--------------------------------------