Net-Enabled Command Capability

INCREMENT 1 TECHNICAL OPERATIONS ARCHITECTURE

7 December 2007

Version 1.0

Prepared by:

Net-Enabled Command Capability
Joint Program Management Office (JPMO)
P.O. Box 4502
Arlington, VA 22204-4502

In Collaboration with USJFCOM and the NECC Component Program Managers for Navy, Air Force, Army, Marine Corps, and DISA

DISTRIBUTION – Distribution authorized to DoD and DoD Contractors only; for administrative/operational use (December 2007). Other requests for this document shall be referred to the NECC Program Management Office.

DESTRUCTION NOTICE – For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

APPROVAL PAGE

Approved by: _____ Date: 12/11/07

Mark Kuzma

Chief Engineer,

Net-Enabled Command Capability (NECC)

REVISION HISTORY

REVISION NUMBER	REVIEWER / ORG	CHANGES	REVISION DATE	DATE ENTERED	NAME OF PERSON ENTERING CHANGE
1.0	Rock/MITRE	Baselined version.	3 December 2007	3 December 07	Mary Rock
1.0	Brown/JPMO	Edited/formatted document	4 Dec 2007	4 December 07	Dustan Brown
1.0	Brown/JPMO	Merged Dr. Mathews updates with Program Control version - Moved Figure 4; inserted new text in section 2.3, 2.4, 2.5, 3.2.1, 3.2.5.1; Changed list in 2.3; deleted section 2.5.1 and 2.5.2; and deleted the defined NetOps acronym in front of community (but defined the next use as per regulations). Updated TOC.	7 Dec 2007	7 December 07	Dustan Brown

TABLE OF CONTENTS

APPROVAL PAGE ..... **II**

REVISION HISTORY ..... **III**

1 STRATEGY **1**

1.1 RELATED DOCUMENTS 1

2 KEY CONCEPTS **2**

2.1 THE INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL) 3
2.1.1 ITIL Processes and Definitions *3*
2.2 ROLES AND RESPONSIBILITIES 4
2.2.1 Responsibility Matrix *5*
2.2.2 Integrated Service Provider Model *6*
2.3 SERVICE PROVISIONING 7
2.4 END-USER SUPPORT 9
2.5 SERVICE MONITORING AND MANAGEMENT 9
2.6 NECC SERVICE MANAGEMENT SCENARIO 10

3 IMPLEMENTATION **11**

3.1 ROLES AND RESPONSIBILITIES 11
3.1.1 JTOCC *11*
3.1.2 Joint Program Management Office (JPMO) *13*
3.1.3 Component Program Management Office (CPMO) *13*
3.1.4 CM Developer *13*
3.1.5 CM Provider *13*
3.1.6 Host Provider *14*
3.1.7 Service Implementer *15*
3.2 SERVICE PROVISIONING 15
3.2.1 Configuration Management *16*
3.2.2 Change Management *16*
3.2.3 Tool Support *17*
3.3 END-USER SUPPORT 17
3.3.1 Service Desk *17*
3.3.2 Incident Management *18*
3.3.3 Problem Management *18*
3.3.4 Tool Support *19*
3.4 SERVICE MANAGEMENT 19
3.4.1 Service Level Management *19*
3.4.2 Capacity Management *19*
3.4.3 Service Continuity Management *20*
3.4.4 Availability Management *20*
3.4.5 Tool Support *20*
3.5 WAIVER PROCESS 21

4 CONCLUSION **21**

APPENDIX A – ACRONYMS **22**

LIST OF FIGURES

Figure 1: Technical Operations Architecture Taxonomy 2
Figure 2: ITIL Service Management Framework 3
Figure 3: Integrated Service Provider Model 6
Figure 4: ITIL Service Support 8
Figure 5: NECC Service Management Scenario 11
Figure 6: Service Provisioning 15

LIST OF TABLES

Table 1: RASCI Chart of NECC Roles and Responsibilities 5

1 STRATEGY

The Technical Operations Architecture describes how Capability Modules (CMs) and their related Back-Office systems are managed during operational use to ensure seamless delivery of Net-Centric Command Capability (NECC) services to the user community. This document includes a description of the Joint Technical Operations Control Capability (JTOCC) and establishes the operational service management functions for CMs and the Back-Office systems that they use. JTOCC functions are distributed across three core areas of responsibility: Service Provisioning, End-user Support, and Service Management. These functions are described using the processes identified in the Information Technology Infrastructure Library (ITIL)[1]. The ITIL is a framework of best practices that facilitate the creation and delivery of reliable, high quality Information Technology (IT) services. JTOCC roles and responsibilities are shared by multiple stakeholders, including the Joint Program Management Office (JPMO) and the Component Program Management Offices (CPMOs). The JTOCC's principal customers within NECC include the NetOps community, the end-user/Warfighter, and individual CPMOs. JTOCC processes, as well as the roles and responsibilities required to carry out these processes, are outlined in this document. The *NECC JTOCC Execution Plan* and the *NECC NetOps Concept of Operations (ConOps)* documents include more detail on these processes.

CPMOs and the Capability Providers that they manage are responsible for provisioning, operating, and sustaining CMs and any Back-Office systems that they use. The JTOCC is the first line of Service Desk Support. The JTOCC supports NECC functions as part of the broader Global Information Grid (GIG) Network Operations (NetOps), as defined in the Joint ConOps for GIG NetOps.[2] It will work with other GIG NetOps organizations that are responsible for managing the GIG, including the Global Infrastructure Service Management Center (GISMC), to provide and receive appropriate information and resolve anomalies with respect to the NECC services. The JTOCC will work with other GIG operational organizations to define and implement appropriate interfaces to allow mutually beneficial information exchange in support of the GIG NetOps mission.

1.1 Related Documents

NECC Increment 1 Software Architecture, version 1.0

NECC Increment 1 Physical Architecture, version 1.0

NECC Increment 1 Data Architecture, version 1.0

NECC Increment 1 Information Assurance (IA) Architecture, version 1.0

NECC Developer's Handbook, version 1.0

NECC System Development and Demonstration (SDD) Phase Configuration Management Plan, version 1.0

NECC Systems Engineering Plan (SEP), version 1.0

---

[1] http://www.itlibrary.org/

[2] *Joint Concept of Operations for Global Information Grid NetOps*, version 3, 4 August 2006

NECC Joint Technical Operations Control Capability (JTOCC) Execution Plan, version 1.0

NECC NetOps ConOps, version 1.0

NECC Certification & Accreditation (C&A) Process, version 1.0

Context Data Source Adapter (CDSA) specification, Version 2.0

2 KEY CONCEPTS

The elements around which the Technical Operations Architecture is built include the management, provisioning, support (including user-support), and operations of CMs, Capability Packages (CPs), and Back-Office systems. Figure 1 shows the relationships and linkages among these and other elements. The elements in Figure 1 are discussed throughout this document.

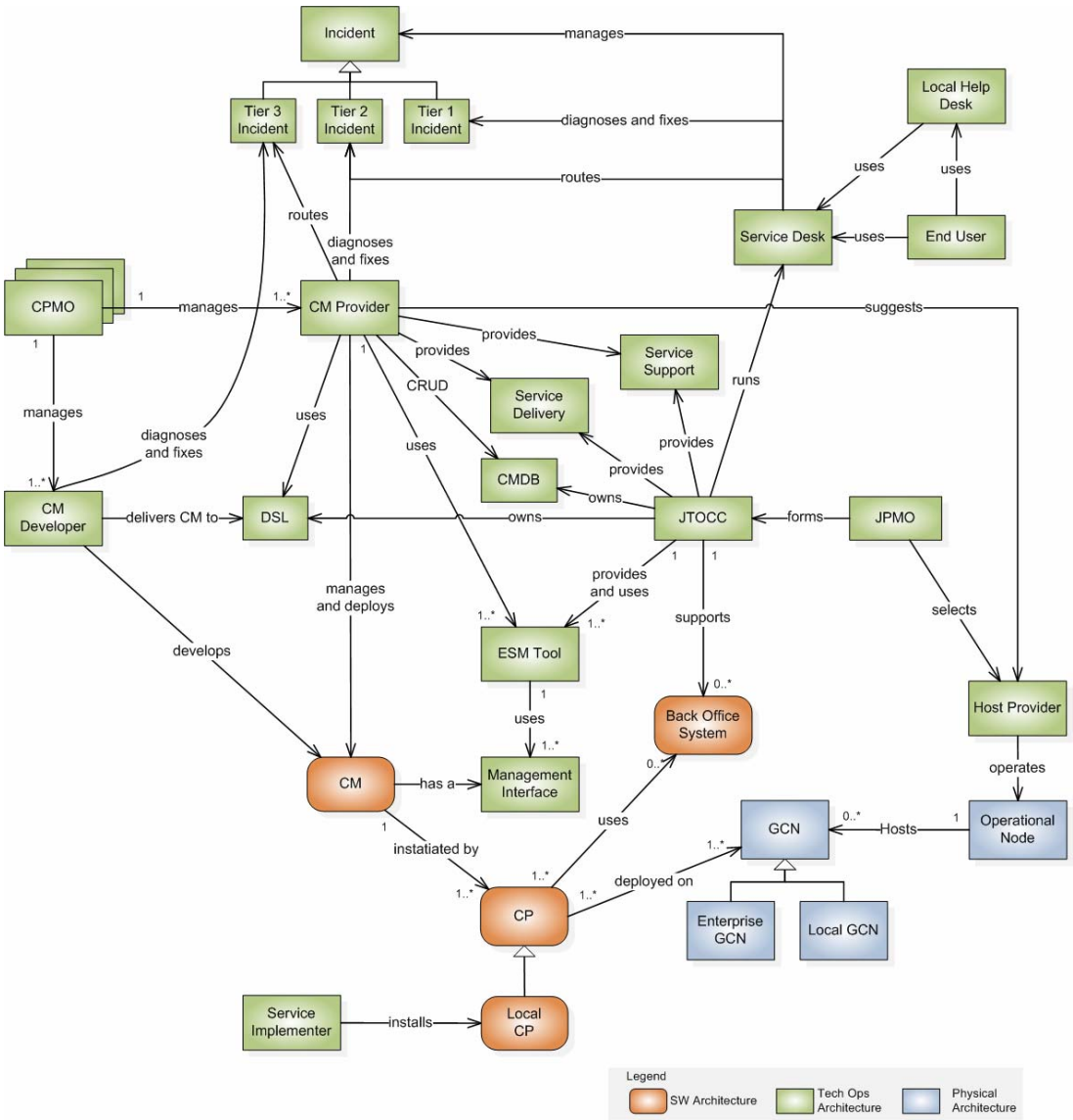

Figure 1: Technical Operations Architecture Taxonomy

2.1 The Information Technology Infrastructure Library (ITIL)

In its role supporting the NECC JPMO, the JTOCC will define Service Management processes using ITIL best practices. ITIL has been in development for over 15 years and is used by major commercial and government organizations, including the Defense Information Systems Agency (DISA) Computing Services Division (CSD), Army Enterprise NetOps Integrated Architecture (AENIA), and the Joint Staff Support Center (JSSC). This document uses ITIL version 2, with the exception of Continual Service Improvement (CSI), which uses version 3. Figure 2 shows the ITIL version 2 framework, with the Service Management processes at the heart of the framework. The Service Management processes are divided into two ITIL areas, Service Delivery and Service Support. NECC will use the ITIL Service Management processes as the framework for developing NECC processes.

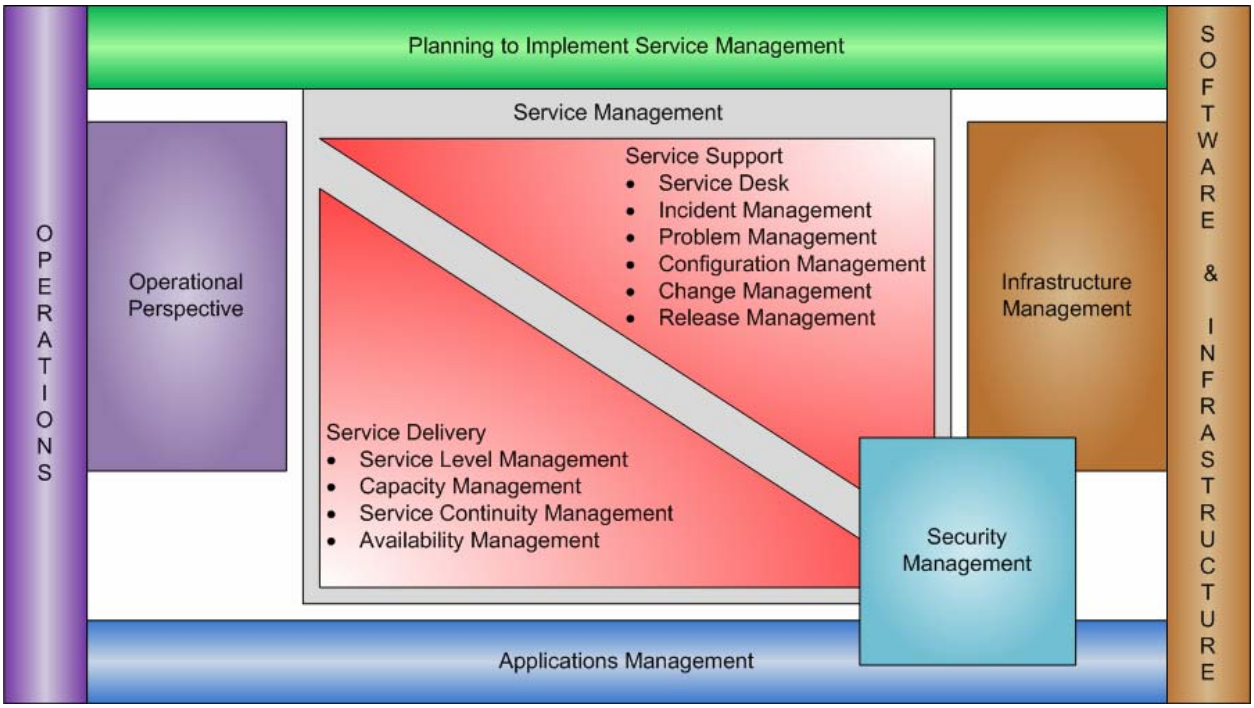

Figure 2: ITIL Service Management Framework[3]

2.1.1 ITIL Processes and Definitions

The following definitions and discussion are based on the ITIL best practices.[4]

Change Management covers the process of IT changes for all types of change, from the request for change, to assessment, to scheduling, to implementing, and finally to the review.

Configuration Management covers the identification of all significant components and recording details of the associated Configuration Items (CIs) in the Configuration Management Database (CMDB). Configuration Management also records relationships between CIs within the CMDB.

---

[3] Adapted from *Planning to Implement Service Management*, ITIL version 2

[4] *Planning to Implement Service Management*, ITIL version 2, p. 175-176.

Release Management consists of the planning, designing, building, and testing of CPs and the Back-Office systems that they use to create a set of release components for an operational environment. It is closely related to Change Management and Configuration Management.

An incident is defined as an event which is not part of the standard operation of a service, and which causes, or may cause, an interruption to, or reduction in, the quality of the service.

Incident Management consists of the processes needed to restore normal service as quickly as possible, following an incident or loss of service. It also seeks to minimize any adverse impact on operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Problem Management consists of the processes needed to minimize the adverse impact of incidents and problems on the system that are caused by errors, and to prevent reoccurrence of these errors. Problem Management seeks to get to the root cause of incidents.

Service Level Management (SLM) is the process of planning, coordinating, drafting, agreeing, monitoring, and reporting on Service Level Agreements (SLAs), and ensuring continued service improvement.

Capacity Management is the focal point for all service performance and capacity issues.

Availability Management ensures that services are available in accordance with mission-critical end-user needs.

2.2 Roles and Responsibilities

There are seven major roles involved in the Technical Operations of NECC.

CM Providers are responsible for the provisioning, run-time management, performance, and availability of the CMs that they provide and any Back-Office systems on which CMs rely.

CM Developers are responsible for the design, development, and support of CMs. They place the CMs into the Definitive Software Library (DSL).

CPMOs manage the efforts of CM Developers and CM Providers. In addition, they are responsible for CM C&A.

Host Providers provide facilities, GIG Computing Nodes (GCNs), and other infrastructure components required for CM Providers to deploy CPs.

The JTOCC is responsible for operating the NECC Service Desk and for the run-time management, performance, and availability of NECC, as a whole.

The JPMO administers the JTOCC and is responsible for overall NECC C&A. In addition, the JPMO can act in the CPMO role of managing CM Providers and CM Developers (e.g., the JPMO plans to act in the CPMO role for several Command and Control (C2) cross-functional CMs).

Service Implementers install NECC capabilities on Local GCNs within their own organizations. The CPMOs coordinate the activities of the Service Implementers.

2.2.1 Responsibility Matrix

The RASCI (Responsible, Accountable, Supportive, Consulted, and Informed) model is used to identify the responsibilities associated with the roles above in carrying out ITIL processes for NECC.[5]

RASCI model definitions are as follows:[6]

- R = Responsible – owns the problem/project
- A = the organization to whom "R" is Accountable – approves work before resources are allocated
- S = can be Supportive – can provide resources or play a supporting role in implementation
- C = should be Consulted – has the information or capability necessary to complete the work
- I = should be Informed – must be notified of results but does not need to be consulted

Table 1: RASCI Chart of NECC Roles and Responsibilities

	CM Provider	CM Developer	JPMO	JTOCC	Host Provider	Service Implementer
Tier 1 Service Desk			A	R		
Tier 2 Service Desk	S		A	R	S	S
Tier 3 Service Desk	S	S	A	R	I	C
Configuration Management	R		A	R	I	S
Change Management	R	C	A	R	C	S
Release Management	R	C	A	R	S	S
Incident Management	S	C	A	R	C	C
Problem Management	S	C	A	R		I
Service Level Management	R		A	R	S	S

[5] Based on the A.R.C.I. model from *Planning to Implement Service Management*, ITIL version 2, p. 85-86.

[6] http://www.valuebasedmanagement.net/methods_raci.html and http://www.12manage.com/methods_raci.html

	CM Provider	CM Developer	JPMO	JTOCC	Host Provider	Service Implementer
Capacity Management	R		A	R	S	S
Continuity Management	R		A	R	S	S
Availability Management	R		A	R	S	S

As depicted in the RASCI chart, the JTOCC and CM Providers are jointly responsible for many of the ITIL processes. CM Provider responsibilities pertain to individual CMs, while JTOCC responsibilities pertain to NECC as a whole.

2.2.2 Integrated Service Provider Model

The roles, responsibilities, and the interrelationships of the JPMO, JTOCC, CPMOs, CM Providers, and CM Developers are depicted in Figure 3, which together will result in NECC services being provided using an integrated service provider model. The JPMO and the CPMOs are organizations that together have the responsibility of an integrated service provider. The JPMO is responsible for establishing, staffing, and managing the JTOCC, and has overall accountability for all NECC services. The JTOCC operates the Service Desk, provides operational management tools, and defines service management processes. CPMOs manage the efforts of CM Providers and CM Developers. CM Providers are responsible for provisioning and managing services that the CM Developers have developed.

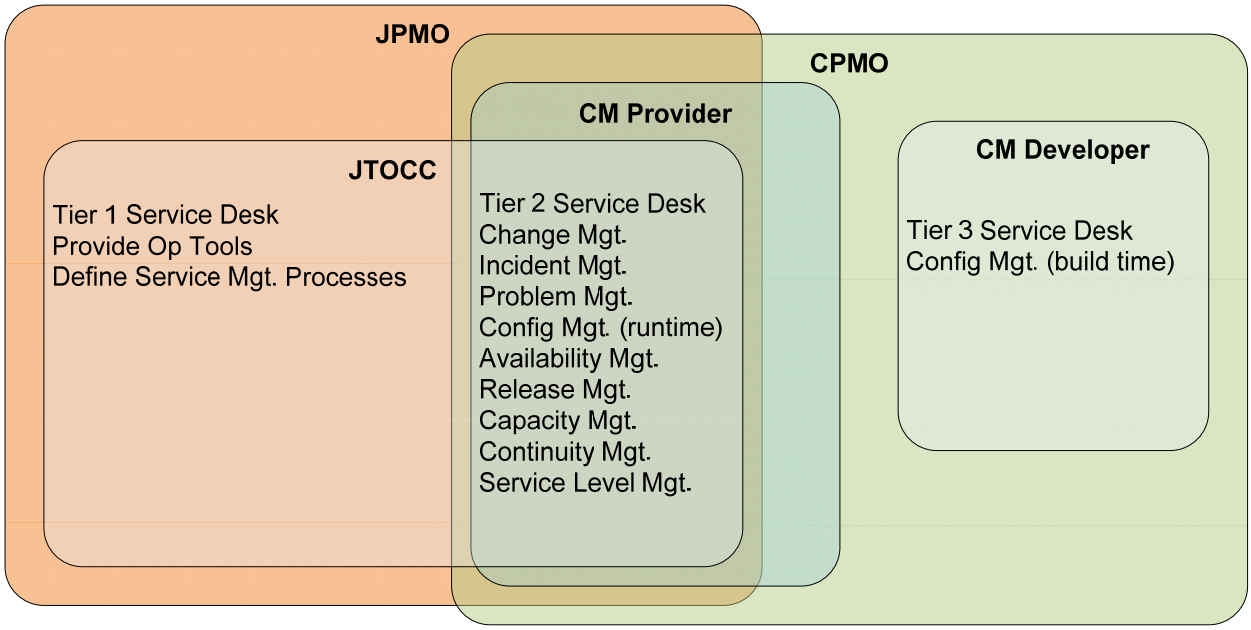

Figure 3: Integrated Service Provider Model

In this service provider model, users are not concerned with the software, applications, and networks required to access information; they expect services to be transparently available to aid them in completion of their mission or tasking. Users don't need to be aware of where software is being hosted, what specific applications are being used, and what network the services must traverse.

The JTOCC will define operational processes based on ITIL best practices. These processes relate to the provisioning and support of services to the user. The Service Desk functions draw on all of the other ITIL Service Management process areas. The JTOCC will provide the end-user Tier 1 Service Desk support for the NECC services. The Service Desk will attempt to solve simple incidents for the end-user and provide fault isolation and routing of complex issues to the appropriate organization for further analysis. The Service Desk is the principal operational interface between Service Providers and end-users (or their Local Help Desk), and it should be considered the front line for IT support to the NECC user.

The JTOCC has the responsibility to define and implement the NECC service management processes. The JTOCC will use the following ITIL process definitions as a framework for defining the NECC specific operational processes:

1. Configuration Management
2. Incident Management
3. Problem Management
4. Change Management
5. Release Management
6. Service Level Management
7. Availability Management
8. Continuity Management
9. Capacity Management

The JTOCC, acting on behalf of the JPMO, is responsible for the overall quality of NECC services, while the CM Provider is responsible for the quality of the services provided by individual CMs. To improve the quality of services, the JTOCC must define apt operational processes and procedures, execute these processes and procedures, and provide oversight to ensure that these processes and procedures are properly executed by both the JTOCC and the CM Provider.

2.3 Service Provisioning

Service Provisioning is the deployment of CPs and Back-Office services. Service Provisioning includes the ITIL Service Support processes listed below and depicted in Figure 4.

1. Release Management
2. Configuration Management
3. Change Management

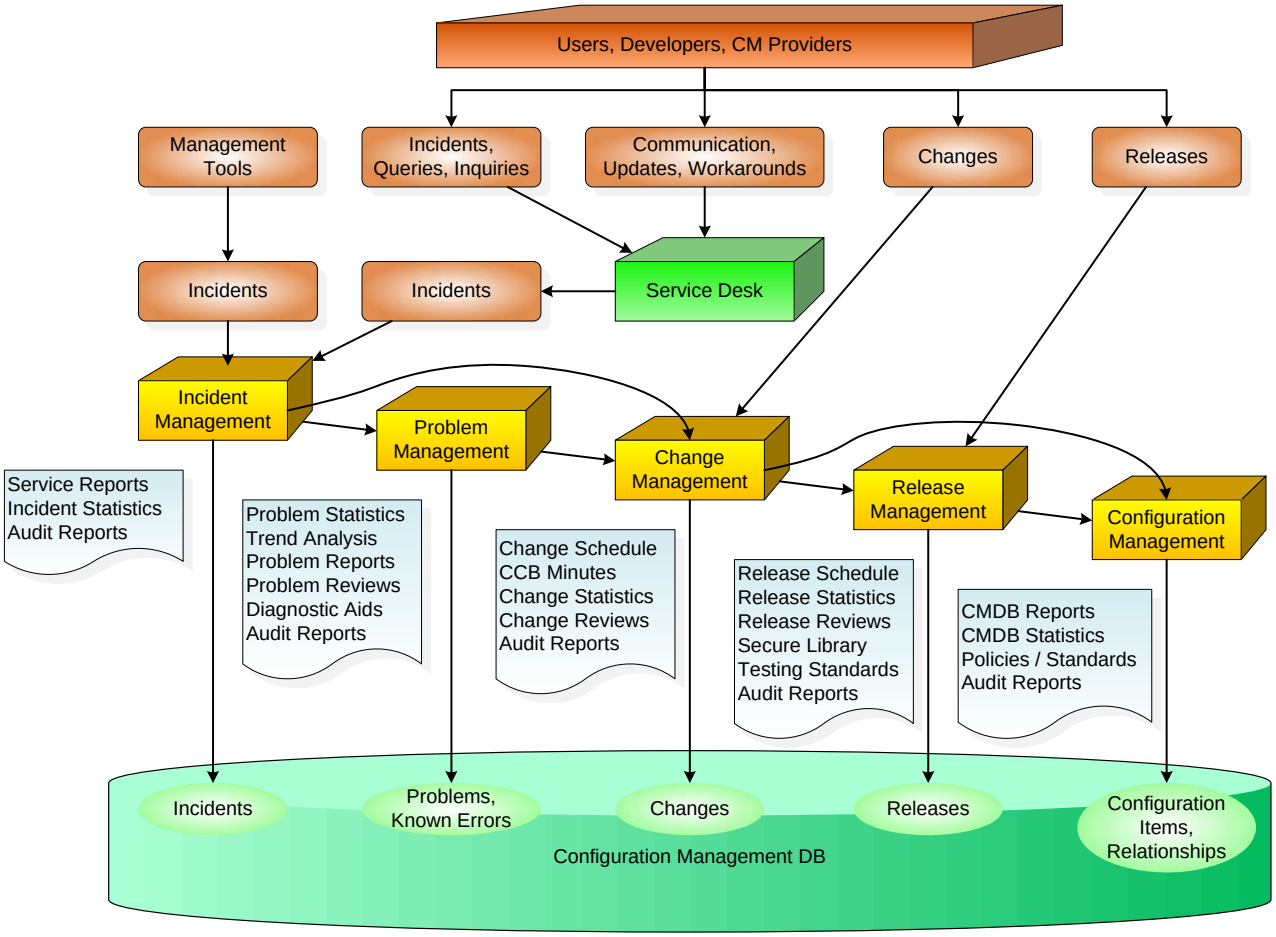

Figure 4: ITIL Service Support[7]

Release Management is very closely linked with Configuration Management and Change Management, and undertakes the planning, design, building, and testing of hardware and software to create a set of CM and Back-Office system releases. NECC release management activities include storing authoritative copies of CM software in the DSL and provisioning CPs to operational sites.

Configuration Management covers the identification of all significant components within the service environment, as well as recording details of these components in the CMDB maintained by the JTOCC. The Configuration Management process ties in closely with the Release Management and Change Management processes.

Change Management covers the process of modification to the services for all types of change, from the RFC, to assessment, to scheduling, to implementing, and finally to the review. It is the Change Management process that produces approval (or otherwise), for any proposed change.

[7] Based on *Planning to Implement Service Management*, ITIL version 2

The approval process for the RFC is described in the *NECC Increment I System Development and Demonstration (SDD) Phase Configuration Management Plan*.

2.4 End-User Support

End-User Support includes the three ITIL Service Support processes listed below and depicted in Figure 4 above.

1. Service Desk
2. Incident Management
3. Problem Management

The Service Desk is directly responsible for supporting the end-users. The NECC Service Desk is implemented as a standard multi-tiered system. The Service Desk provides routing and fault isolation of incidents to the appropriate entity to resolve application, hosting, and network issues, as defined in the *NECC NetOps ConOps*.

In defining the functionality of the Service Desk, it is important to include the Joint Capabilities Integration and Development System (JCIDS) processes with regard to Doctrine, Organization, Training, Leadership and education, Personnel, and Facilities (DOTLPF).

Problem Management seeks to minimize the adverse impact of incidents and problems on the services that are caused by errors, and to prevent recurrence of incidents related to these errors. In order to achieve this goal, Problem Management endeavors to get to the root cause of incidents and then initiates actions to improve or correct the situation. The Problem Management process has both reactive and proactive aspects. The reactive aspect is concerned with solving problems in response to one or more incidents. Proactive Problem Management is concerned with identifying and solving the underlying causes of an incident before it recurs. As a result of an incident or a problem, a Request For Change (RFC) may be generated by the end-user, end-user's Local Help Desk, JTOCC, the JPMO, CM Provider, or CM Developer.

2.5 Service Monitoring and Management

The JPMO is accountable for the compliance of the NECC services to their respective SLAs. The JTOCC and CM Providers are jointly responsible for performing Service Monitoring and Management functions for all services deployed on both Enterprise GCNs and Local GCNs. CM Provider responsibilities pertain to individual CMs, while JTOCC responsibilities pertain to NECC as a whole. The JTOCC will not have insight into services on Local GCNs when these local nodes are disconnected from the wide area network.

CM Providers will manage those CMs and Back-Office systems for which they are responsible. If a Back-Office system is already in place and managed by another organization, the CM Provider will be responsible for the CM, including its interface to the Back-Office system, but the existing organization may continue to be responsible for the Back-Office system itself. If the Back-Office system has no support or must be freshly deployed to support the CM, then the CM Provider will be responsible for supporting the CM, its interface, and the Back-Office system.

Service Monitoring and Management include the ITIL Service Delivery processes below.

1. Service Level Management

2. Capacity Management
3. Service Continuity Management
4. Availability Management

SLM tends to be categorized as a day-to-day operational process. It encompasses activities such as service management, reporting, and measuring actual service delivery to end-users. It also includes proactive measures such as recommending service improvements through the Change Management process.

The Capacity, Service Continuity, and Availability Management processes have a different focus from that of SLM. Instead of day-to-day operations, they are focused on planning for future contingencies. With Capacity Management, NECC will plan for sufficient resource capacity to handle estimated future demand. When the JTOCC executes the Capacity Management process, it must take into account all resources required to deliver a service, the dependencies of NECC services on other components (e.g., GIG bandwidth), and hosting facility capacity and infrastructure constraints. The JPMO will develop a Continuity of Operations (COOP) Plan to address risk identification, recovery, and minimal disruption of service in cases of disaster. Finally, Availability Management covers the processes to better meet user service needs, respond to surges in demand, and improve performance by placing servers in different locales. Availability management must also consider all the services and their dependency chains.

2.6 NECC Service Management Scenario

To better understand how these processes inter-relate, consider the following example of the life-cycle of an NECC Incident:[8] Figure 5 provides a depiction of the processes involved in this scenario.

1. An end-user calls the Service Desk to report response difficulties using an NECC service.
2. The JTOCC uses the Incident Management process to deal with the Incident.
3. The JTOCC uses the Problem Management process to investigate the underlying cause and uses the Capacity Management process to assist. The SLM owner and the CM Provider are alerted that the SLA has been breached. The CM Provider can generate a RFC.
4. The RFC starts the Change Management process.
5. The IT Financial Management process assists with the business case cost justification for any upgrade. Financial Management is a JPMO responsibility, but the JTOCC may provide some financial estimates (e.g., for Capacity Management); the CPMO could also provide some financial estimates (e.g., for work packages).
6. The IT Service Continuity process owner via the JTOCC and CM Provider gets involved in the Change Management process to ensure recovery of the current deployed CM or Back-Office system.

[8] Based on *Service Support*, ITIL version 2

7. The JTOCC and the CM Provider use the Availability Management process in considering the upgrade to ensure that it can meet the required availability and reliability levels as negotiated with the hosting provider.
8. The JTOCC and the responsible CM Providers use the Release Management process, which controls the implementation of the change, by rolling out replacement CMs and any associated Back-Office systems. During the Release Management process, the CM Provider will update the CMDB with details of new releases and versions.
9. The Configuration Management process ensures that the CMDB information is updated throughout the process. It requires input from both the JTOCC and the responsible CM Providers.

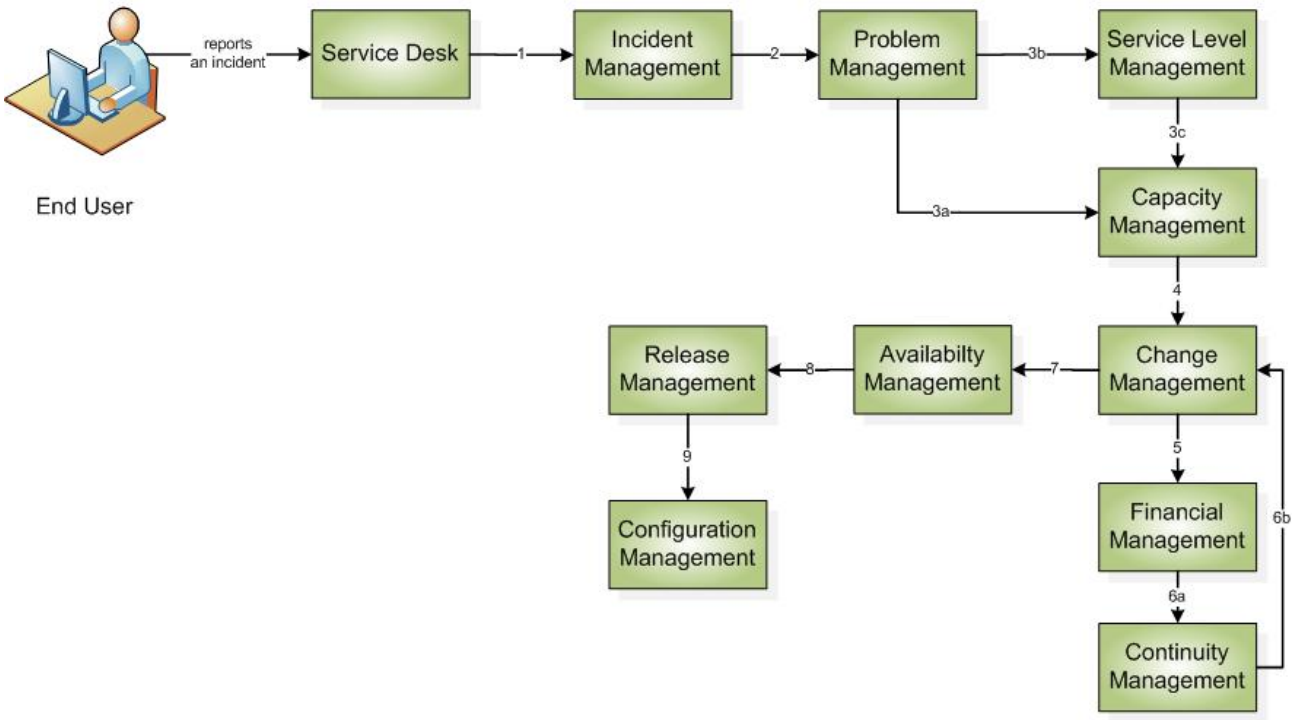

Figure 5: NECC Service Management Scenario

3 IMPLEMENTATION

3.1 Roles and Responsibilities

3.1.1 JTOCC

JTOCC responsibilities include the following:

- Defining and implementing NECC technical operations processes based on ITIL Best Practices

- Providing the tool suite needed to meet the technical operations requirements and execute the technical operations processes
- Run-time Configuration/Change/Release Management(this is a joint responsibility between the JTOCC and the CM Providers)
- Service Desk Tier 1 operations and support
- Service Desk Tier 2 support, troubleshooting and mediation of issues involving multiple CMs or Back-Office systems, and routing anomalies to the responsible organizations
- Coordinating and collaborating with the Joint Task Force – Global Network Operations (JTF-GNO), NetOps and others to resolve interdependent NECC operational impacts
- Service Management operations and support for CMs and Back-Office systems (this is a joint responsibility between the JTOCC and the CM Providers)
- Service Desk and Service Monitoring personnel training and education
- Service Dependency/Interaction modeling
- Supporting CM Providers in deploying CMs and their related Back-Office applications
- Working with CM Providers to make sure that the hosting requirements for Back-Office systems are met
- Exchanging event information with NetOps organizations such as the GISMC, Global Network and Security Center (GNSC) and Theater NetOps Centers (TNCs)
- Recommending dispute resolution processes, policies, and procedures for approval by the NECC Engineering Review Board (ERB) or the Configuration Control Board (CCB)

In keeping with the federated nature of NECC and supporting Communities of Interest (COIs) like the NetOps community, the JTOCC is a distributed capability. The Integrated Service Provider team members made up of the JTOCC, CM Providers, CM Developers, and Host Providers will not be co-located in a single facility, but may be distributed throughout the world. They will, however, share a common set of tools and a common set of policies and procedures so that they can effectively collaborate and provide all NECC users (or the user's Local Help Desk) with a uniformly high quality of service. An example of this distributed approach would be if a User-Defined Operational Picture (UDOP) CP is located in one Host Provider facility, a Blue Force Ground Data CP that feeds the UDOP view is hosted at another Host Provider facility, and the staff and tool suite used to monitor and manage these two CPs is located at a third location.

3.1.1.1 Service Desk

The JTOCC operates the NECC Service Desk and is responsible for tracking, resolving, and recording all incidents relating to NECC services. An end-user should report all incidents related to NECC to the Service Desk. If the user cannot determine whether the issue is NECC related, they should call their Local Help Desk. An end-user's Local Help Desk is their organization's service support Help Desk. If the end-user's Local Help Desk determines that the incident is an NECC service error, then the Local Help Desk should report the incident to the Service Desk. The Service Desk will respond back to the Local Help Desk on the actions taken to respond to the incident. For NECC issues, it is the Service Desk that is responsible for reporting back to the end-user on the conclusion of the incident.

The Service Desk will receive and record all calls from users (and their Local Help Desks) and deal directly with simple requests and complaints; it will provide initial investigation and assessment of all incidents and make first attempts at incident resolution. If an incident cannot be resolved by the Tier 1 Service Desk, the Service Desk will refer the incident to Tier 2 support, which is handled by the CM Provider. If the CM Provider determines that this is not an incident that they can resolve, because it requires changes to the software, then the CM Provider will refer the incident to the Tier 3 CM Developer for resolution. The JTOCC has the lead on all incidents, but it will rely heavily on the CM Providers and CM Developers for Tier 2 and 3 incident resolution. The incident must be referred back to the JTOCC after service restoration or resolution. Only the JTOCC is authorized to close an incident, after informing the incident's originator of its resolution. The JTOCC Service Desk will communicate with the end-user or their local Service Desk via user-generated trouble tickets, e-mail, or telephone calls.

3.1.2 Joint Program Management Office (JPMO)

The JPMO administers the JTOCC and functions as a system integrator of JTOCC requirements, including systems engineering, integration, and increment-level performance responsibilities. The long-term JTOCC governance and administration is predicated on collaboration across multiple Services and the Joint NetOps community. Individuals from the CPMO, JPMO, and other organizations such as the GNSC, GISMC and Global Network Operations Center (GNC) will be represented on the NECC ERB and CCB where governance, administration, and policies are approved for implementation.

3.1.3 Component Program Management Office (CPMO)

CPMOs are responsible for managing the efforts of CM Developers and CM Providers for CMs that they have been tasked to provide. The CPMO is responsible for updating software for individual CMs and any related Back-Office systems. The CPMO is also responsible for working with the JTOCC to deploy legacy applications to the Back-Office environment and to work with the JTOCC to customize the environment as the CPMO deems necessary.

3.1.4 CM Developer

The CM Developer is responsible for end-to-end CM development, certification, and accreditation of a CM through the Federated Development and Certification Environment (FDCE). CM Developers must package their CMs according to the CP specification[9]. They must deliver each CP for the JTOCC's Service Provisioning with Type Accreditation. Acceptance testing is done on a per deployment basis. The CM Developer will support the CM Provider in testing and acceptance of CPs to operational sites.

3.1.5 CM Provider

CM Providers are responsible for the provisioning, performance, availability, and overall operation of their CMs, along with any associated Back-Office systems. The CM provider has the release, change capacity, configuration, availability, service level and service continuity management responsibilities for the CM in operations, ensuring that the CM is meeting its SLA.

---

[9] See the *NECC Increment 1 Physical Architecture* and the *Developer's Handbook*.

The CM Provider is responsible for distributing the CM, along with any associated Back-Office systems to one or more locations in order to meet availability goals specified by the JPMO. The CM Providers may elect to use the Enterprise GCNs that are available at selected hosting providers. The CM Provider is responsible for capabilities deployed on Local GCNs.

CM Provider responsibilities also include:

- Negotiating with the JPMO to determine the Host Providers
- Negotiating SLAs with Host Providers
- Negotiating with Service Implementers, who will be implementing NECC services in their own environment for training and DOTLPF activities
- Responding to all incidents assigned to them by the JTOCC
- Providing the JTOCC an advance maintenance and service delivery report detailing the CM or Back-Office system schedule, including downtime and site-specific configurations
- Providing load balancing and extra capacity support for each CM and any related Back-Office systems for both Enterprise and Local GCNs
- Testing of Information Assurance Vulnerability Alert (IAVA) patches to ensure that the patch does not break the CP or Back-Office system

3.1.6 Host Provider

The Host Provider provides a facility and the GCN with its virtual computing environment required for the CM Provider to deploy the CPs. The Host Provider must provide all permissions necessary for the CM Provider to independently deploy the CPs into the virtual hosting environment. The CM Provider negotiates with Host Providers to create SLAs between the Host Provider and the user community (i.e., the CM Provider acts as the user's representative in the agreement). The CM Provider, acting as a proxy for the user community, specifies the agreed upon threshold and objective measures that the Host Provider must meet as set forth in the SLAs for availability, capacity, service continuity, and computing performance requirements of the hosting environment. The Host Provider will be responsible to the JTOCC for providing reports and the data to back up the reports on compliance with SLAs. The CM Provider maintains overall operational responsibility for the CP.

Host Providers are also responsible for:

- Coordinating with the JTOCC on Service management issues
- Reporting hosting status to the JTOCC
- Providing IA, System Administration, system security, and IAVA updates to the hosting environment (after coordination with CM Provider)
- Operations and maintenance of GCN and back-office hardware, Virtual Machine (VM)ware software, and Operating System (OS) level software (after coordination with the CM Provider)
- Providing CP management capability to the CM Provider or JTOCC personnel

- Reporting network or system availability metrics to the JTOCC

3.1.7 Service Implementer

The Military Services/Components through their CPMOs are responsibility for implementing NECC capabilities within their organizations. As Service Implementers, the CPMOs must plan for the transition from current materiel solutions to NECC. This includes training the organization's personnel to make use of the new capabilities, and supporting the Change Management process as new capabilities are deployed into the operational environment (i.e., the activities necessary to support the DOTLPF functions of that organization).

Service Implementers, along with the CM Providers, are responsible for deploying NECC capabilities on Local GCNs within their organizations. The Service Implementer is also responsible for training System Administrators on the deployed CM. If the Local GCN has robust and reliable connectivity to the GIG, and if the JTOCC or CM Provider can actively manage the CM or Back-Office system from a remote location, then the Service Implementer may request deployment support by the JTOCC.

3.2 Service Provisioning

The CM Provider will deploy CMs as one or more CPs. As shown in Figure 6, once the CM has been certified through the FDCE, the CM Developer places the CPs contained within the CM into the DSL and the CPs become part of the operational baseline. The CM Provider is then responsible for executing the provisioning process to deploy CPs onto GCNs and to deploy any associated Back-Office systems to the operational environment. The CM Provider may arrange for the JTOCC to act as a CM Provider proxy to deploy CPs. These processes will be described in detail in the *NECC JTOCC Execution Plan*. For the sake of agility and responsiveness, NECC provisions capabilities on a CM-by-CM basis and not as an entire increment baseline.

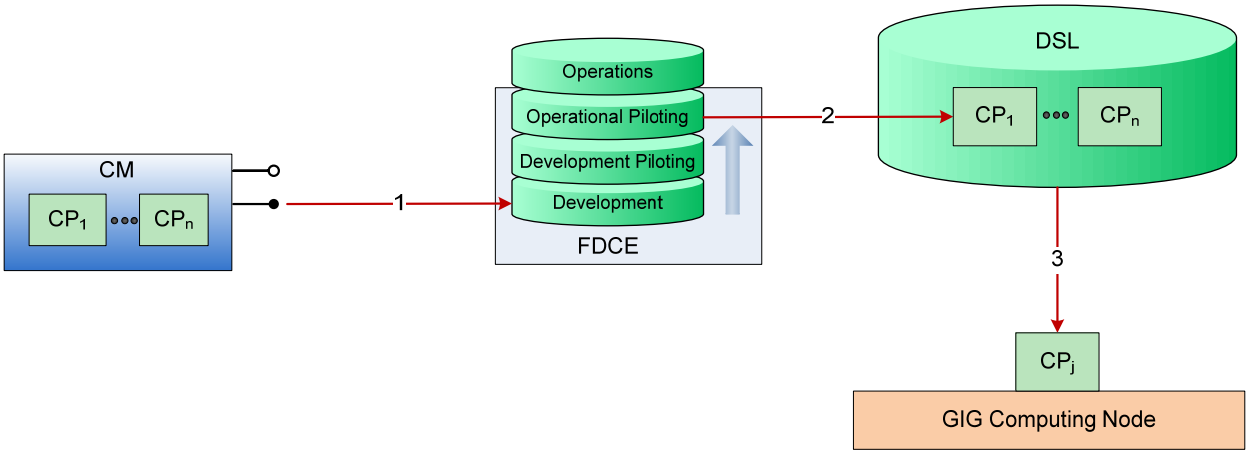

Figure 6: Service Provisioning

The CM Providers are responsible for deploying their CPs onto Enterprise GCNs. The Local GCNs may be deployed by the CM Provider, a Service Implementer, or both. The CM Provider may deploy a CP or Back-Office system onto Local GCNs with the help and assistance of the Service Implementer to set up the CP or Back-Office system.

3.2.1 Configuration Management

The JTOCC will operate and maintain a CMDB for tracking NECC CIs. Configuration Management of CIs begins with the CM Developer using the FDCE process as the CMs are being developed and tested. The CM Developer maintains their own configuration management process for development CIs. When the CM is ready to become part of the operational baseline, and has been delivered to the DSL, the JTOCC and CM Provider share configuration management responsibilities. CM Providers are responsible for configuration management of each of the CMs that they provide, while the JTOCC has responsibility for the overall NECC operational baseline.

Each CP contained in a CM, as well as the CM itself, will be given a version number. The guidelines for assigning version numbers are detailed in the *NECC Developers Handbook*. The following NECC CIs must be versioned:

- **Capability Module:** the NECC-assigned version number indicates a distinct set of CPs
- **Capability Packages:** the NECC-assigned version number of each CP also designates a distinct set of components
- **Guest OS:** the version of the OS used in the CP (e.g., Windows 2000 SP2)
- **COTS/GOTS Infrastructure:** the version numbers of any Government-off-the-shelf (GOTS) or Commercial-off-the-Shelf (COTS) infrastructure applications (e.g., Oracle 10g)
- **NECC Services:** all distinct Services within a CP must also have an NECC-assigned version number
- **Clients:** the version number may be NECC-assigned if developed by NECC, or it may use the client developer's version number

As part of its responsibility to manage the deployed baseline, the JTOCC will also track what CP version is deployed on each GCN. All version information will be stored in the CMDB and accessible to authorized users via a web interface. The CMDB will contain fields for CMs and any associated Back-Office systems. The CMDB will also capture the relationships between interdependent CIs. The relationship between the build-time and run-time CIs will be reflected in the CMDB.

The processes for Configuration Management of the NECC CIs are further defined in the *System Development and Demonstration (SDD) Phase Configuration Management Plan*.

3.2.2 Change Management

The CM Provider is also responsible for Change Management. Change Management is a process for managing change in the deployed baseline. Managing a significant change in infrastructure products such as a switch from one relational database to another would be done according to the Change Management process. Change management also has a significant Systems Engineering (SE) component which goes beyond Technical Operations and is discussed in the *NECC Systems Engineering Plan* (SEP).

3.2.3 Tool Support

3.2.3.1 Configuration Management Database

The CMDB stores version information for all CIs for all the CMs and any associated Back-Office systems. The JTOCC is responsible for the design, implementation, and operations of the CMDB. The JTOCC and CM Providers are responsible for entering and updating all the version information. Authorized NECC users will be able to access and search the version information stored in the CMDB.

3.2.3.2 Definitive Software Library

The DSL is NECC's central point for the configuration-controlled baseline of CPs. This library provides a stable source of CPs and other applications, such as thick clients. GCNs can obtain the CPs, updates, and data from the DSL, which is a secure, trusted repository. As these capabilities evolve through Increment 1, the DSL will be replicated throughout the GIG for reasons of performance and Continuity Management. Since the repository will maintain digest values on all content, the enterprise management system can execute a consistency check on any GCN, especially at the time of modification of the application.

The DSL is a logical repository and may actually consist of one or more physical software libraries or file stores. The locations for development and test file storage areas should be separate from the DSL. The DSL may also include a physical store (e.g., a fireproof safe) to hold master copies of software. Only authorized software is accepted into the DSL; acceptance into the DSL is strictly controlled by Change Management and Release Management processes.

Changes, upgrades, and bug-fixes are envisioned during the life-cycle of a CM. The repository facilitates CM life-cycle management by providing version control, dynamic provisioning (such as copying software onto multiple nodes), and a relay point when sharing application archives across administrative domains. The Back-Office system software will also be housed and controlled in the DSL.

3.3 End-User Support

3.3.1 Service Desk

The JTOCC Service Desk is built on a standard 3-tier model and will handle end-user incidents related to NECC. The JTOCC performs basic incident handling and manages operations in support of Tier 1. The JTOCC and CM Providers provide Tier 2 support, with the JTOCC performing fault isolation to handle issues that involve multiple CMs and the applicable CM Provider handling issues that have been isolated to a single CM. CM Providers, in conjunction with CM Developers, handle Tier 3 issues.

The CM Provider Tier 2 functions handle CM problems that do not require software fixes, but may require configuration changes to the installed baseline. The CM Provider Tier 3 Service Desk personnel require familiarity with the CM software and must know how to resolve complex problems related to fixing CM software.

For the Service Desk to operate in a distributed environment, it uses a Virtual Service Desk (VSD) model. The VSD consists of geographically separated JTOCC elements that collaborate and cooperate on Service Desk issues, such as incidents and problems, using a shared, web-based tool. From the end-user or the Local Help Desk’s perspective, however, it remains a single

Service Desk with a single access point. Information on incidents will be available to NetOps organizations, such as the GISMC, as one or more web-based services, as deemed necessary for Situational Awareness (SA).

Within the VSD, the CM Providers provide Tier 2 support for each of their CMs. They also manage input to the Virtual Tier 1 Environment, but not the upkeep of the resource. Each CM Provider identifies a representative to support the JTOCC, to monitor and coordinate routine management functions for their CMs.

In addition to Tier 2 support, CM Providers will also provide Tier 3 support. The CM Provider will coordinate with the CM Developer to investigate the incident or problem. If they discover that the incident's resolution will require significant additional software development, or it involves a substantial enhancement to the CM, the CM provider through the applicable CPMO will submit a RFC, thus starting the Change Management process.

3.3.2 Incident Management

Incident Management includes handling any event that disrupts, or could disrupt, a service. This includes events which are communicated by users, either physically via the VSD, or through an interface from the service monitoring and management tools. Incidents can also be reported and logged by JTOCC technical staff (including the Tier 2 and 3 Service Desks). Not all events are incidents; events include routine items such as reporting normal operations status for a given service or configuration item. The Service Desk will execute the Incident Management processes.

3.3.3 Problem Management

Problem Management includes the activities required to diagnose the root cause of incidents and to resolve them. It is also responsible for ensuring that the resolution is implemented through the appropriate control procedures, especially Change Management and Release Management. Problem Management will maintain information about problems and the appropriate workarounds and resolutions such that NECC is able to reduce the number and impact of incidents over time. In this respect, Problem Management is a key input to the Knowledge Base component of the VSD.

For the purposes of JTOCC implementation, these process requirements are more focused on reactive Problem Management than proactive Problem Management. Proactive problem management is part of the normal SE processes associated with defining improvements in services and CMs for future development spirals. Although Problem Management and Incident Management are separate processes, they are closely related. They use similar categorization, impact, and priority coding schemes, and they may even use the same tools.

ITIL version 3 Continual Service Improvement is, as its name implies, an ongoing activity woven into the fabric of an organization, as opposed to a reactive response to a specific situation or a temporary crisis.[10] NECC will use the CSI concepts to help provide a proactive approach to improving the NECC services for Incident and Problem Management.

---

[10] *Continual Service Management*, ITIL version 3

3.3.4 Tool Support

3.3.4.1 Trouble Management System

A Trouble Management System (TMS) is a software component that manages and maintains a database of IT-related issues. It is the key tool for enabling the VSD. It is used to create, update, and resolve issues reported by end-user and other stakeholders. The TMS will use a knowledge base with information on each customer, resolutions to common problems, and other related information. The Knowledge Base will be independent of the DSL and the CMDB. The Knowledge Base will be created, owned, and maintained by the JTOCC. The JTOCC and the CPMOs will provide input into the Knowledge Base.

Using the TMS, an end-user, or the end-user's Local Help Desk, can create new issues, read existing issues, add details to existing issues, or resolve an issue. Whenever a user of the system makes a change, the TMS will record the history of the issue, (e.g., who initiated it, how it was resolved, etc.). Each user of the system may have issues assigned to them; that user is then responsible for the proper resolution of that issue.

3.4 Service Management

3.4.1 Service Level Management

The main function of SLM is monitoring and reporting on SLA compliance. The JTOCC will serve as the clearinghouse for reporting statistics, verifing compliance with SLAs, and providing availability performance metrics. These metrics will be available to the NetOps community as a web-enabled service. The focus for the JTOCC in the SLM function is to aggregate the results of Enterprise Service Management (ESM) reports from the various CM Providers and to provide metrics on issues such as quality of service and SLA compliance. The Service Management team will also maintain a close relationship with the Service Desk team as well as the DISA NetOps Centers for Network Situational Awareness and NetCop reporting guidelines. This relationship will be further defined in the *NECC NetOps ConOps*.

3.4.2 Capacity Management

Capacity Management is the process by which the JTOCC tracks host capacity requirements for real-time and long-term planning associated with providing a service to the end-user within the user's expectations of performance. It also provides the basis for managing the capacity required to provide the service such that when demand exceeds current capacity, actions can be taken to provide additional capacity. Finally, Capacity Management also supports the development of trend analyses that provide the underpinning for medium and long-term capacity planning.

The primary objectives of the Capacity Management process are to measure actual capacity provided against the capacity required to meet a service's specification as codified in the SLA, and to support determination of additional capacity that may be required in the immediate and long-term to support user mission objectives. The overall goal is to ensure the user gets the service performance that is driven by the user's mission objectives. Furthermore, it must plan the host and network capacity to support the user's mission objectives both now and in the future.

Capacity Management includes the activities required to monitor the performance and throughput of NECC services and the supporting infrastructure, support tuning of the services

with respect to hosting capacity, understand current demands for host and infrastructure resources, and be able to derive forecasts for future capacity requirements. Capacity management also includes the support for the development of a Capacity Plan that outlines the predicted infrastructure resources required over time to meet the agreed to service levels across the baseline of NECC.[11] Requirements for growth must measure the trends and take into account the need for additional service capacity. Growth will be a natural extension for NECC service adoption and must be considered as part of the planning process. Determination of the rate of growth and planning for the growth is part of the Capacity Management process.

3.4.3 Service Continuity Management

Under the Service Continuity Management process, the JTOCC—in conjunction with the NECC SE team—will develop a continuity plan for service failover and recovery in the event of outages caused by natural disasters, power failures, hostile action, hacking, etc. The JPMO will establish risk identification, avoidance, and mitigation strategies. The continuity plan will describe the approach to ensure that all NECC services, in accordance with their SLA and mission criticality, can be restored as quickly as possible, and with the least possible disruption to users. The NECC SE team shall approve the continuity plan and the Host Providers will implement it. As the CMs and mission requirements evolve, so must the continuity plan. It shall, therefore, be updated with each major CM revision.

3.4.4 Availability Management

Ensuring that services are available in accordance with mission-critical end-user needs is the goal of Availability Management. The JTOCC will monitor deployed systems and record factors that impact their availability. These factors include service design flaws, environmental issues, such as poor connectivity and high network latency, and unexpected interactions with other deployed (non-NECC) systems. The GISMC, in their role as intermediary between the JTOCC and other NetOps organizations such as the GNSC and the GNC, will need to provide attributes that reflect the impact of the operational status of network and other resources on the availability of NECC services.[12] The JPMO also has a responsibility to provide the availability status of NECC Services to the GISMC for use by the NetOps community.

Some of these availability issues can be overcome with configuration changes and workarounds. These will be noted in the issue database of the TMS. For other more serious issues, the JTOCC will create RFCs for them and work these issues according to the Change Management process. Web-based services will publish availability metrics to provide information on availability status to NetOps organizations.

3.4.5 Tool Support

3.4.5.1 Enterprise Service Management

The ESM tool suite provides the JTOCC with the ability to actively manage deployed services throughout the GIG. Using this set of tools, the JTOCC can determine which services are functioning, what version of software the CM Provider is running, and whether they are meeting

---

[11] *Service Delivery*, ITIL version 2

[12] *Joint Concept of Operations for Global Information Grid NetOps*, version 3, 4 August 2006

their SLAs. The tools will alert the JTOCC to problems with the networking infrastructure so that they can contact the appropriate external agency. The ESM tool suite gives the JTOCC insight into the overall operation of NECC, so that the JTOCC can help diagnose issues as they occur, and to anticipate and prevent potential issues before they become problems. NECC will leverage the NCES ESM services to provide web service management to the fullest possible extent. The CM Provider will also have access to the ESM tools provided by the JTOCC. The CM Provider may use their own management toolset as well. Information and data collected by the ESM suite may also be published to the VSD and viewed by multiple communities including the NetOps community.

The JTOCC will manage all NECC services deployed at GCNs using the ESM tool and the heartbeat interface contained within each NECC service, as required by the CDSA specification.[13] The GISMC, in their NetOps role, is required to provide the status of the networks and resources that the NECC services rely on, via a web-based service.

3.5 Waiver Process

Under certain circumstances, materiel developers may request, and the JPMO may grant, waivers for compliance with the specifications contained in this document. All specifications are required, unless there is a waiver. Some specifications and standards can be waived, some cannot be waived, and some can be waived for a limited period of time.

Specific waiver guidance for the Technical Operations Architecture (TOA) is:

- Full implementation of the heartbeat interface may be temporarily waived, provided the materiel developer presents a schedule for full compliance.

4 CONCLUSION

The NECC TOA addresses the provisioning, management, and support of CMs, CPs, and Back-Office systems by the JTOCC, JPMO and CPMOs. This document describes the information exchange requirements with external NetOps organizations. The TOA relies heavily on using the ITIL Service Management processes[14] as an IT industry accepted best practices. ITIL is used as a framework in the TOA and adapted to meet NECC needs.

[13] *Context Data Source Adapter (CDSA) Specification*, version 2.0

[14] *Planning to Implement Service Management*, ITIL version 2

APPENDIX A – ACRONYMS

Acronym	Definition
A.R.C.I.	Accountable, Responsible, Consulted, Informed
AENIA	Army Enterprise NetOps Integrated Architecture
C&A	Certification and Accreditation
C2	Command and Control
CCB	Configuration Control Board
CDSA	Context Data Source Adaptor
CI	Configuration Item
CM	Capability Module
CMDB	Configuration Management Data Base
COI	Community of Interest
ConOps	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial off-the-Shelf
CP	Capability Package
CPMO	Component Program Management Office
CRUD	Create, Read, Update, Delete
CSD	Computer Services Division
CSI	Continual Service Improvement
CTK	Conformance Test Kit
DISA	Defense Information Systems Agency
DoD	Department of Defense
DOTLPF	Doctrine, Organization, Training, Leadership and education, Personnel, and Facilities
DSL	Definitive Software Library
ERB	Engineering Review Board
ESM	Enterprise Service Management
FDCE	Federated Development and Certification Environment
GCN	GIG Computing Node
GIG	Global Information Grid
GISMC	Global Infrastructure Service Management Center

Acronym	Definition
GNC	Global Network Operations Center
GNSC	Global Network and Security Center
GOTS	Government off-the-Shelf
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JCIDS	Joint Capabilities Integration and Development System
JPMO	Joint Program Management Office
JSSC	Joint Staff Support Center
JTF-GNO	Joint Task Force - Global Network Operations
JTOCC	Joint Technical Operations Control Capability
NCES	Net-Centric Enterprise Services
NECC	Net-Enabled Command Capability
NetOps	Network Operations
OS	Operating System
RASCI	Responsible, Accountable, Supportive, Consulted, Informed
RFC	Request For Change
SA	Situational Awareness
SDD	System Development and Demonstration
SE	Systems Engineering
SEP	System Engineering Plan
SLA	Service Level Agreement
SLM	Service Level Management
TMS	Trouble Management System
TNC	Theater NetOps Center
TOA	Technical Operations Architecture
UDOP	User-Defined Operational Picture
VM	Virtual Machine
VSD	Virtual Service Desk