

PMW 205
Naval Enterprise Networks



NGEN Process Definition Model (NPDM)

Version: 1.2

DATE: 9 March 2012

Program Executive Office Enterprise Information Systems

Program Manager, Naval Enterprise Networks

1325 10th Street, SE, Suite 301

Washington, DC 20374

Executive Summary

The NEN Process Definition Model (NPDM) describes a set of high-priority Navy Information Technology Service Management (ITSM) processes in effect during the CoSC transition period.

These process descriptions represent the optimized current state CoSC operational period until the NGEN target state is achieved. During this time, ITSM processes will be designed in alignment with the Navy NGEN Process Development Model (NNPDM) target state vision. NGEN target state is a multi contractor management system with enhanced Command and Control (C2) and Situational Awareness (SA) by government employees.

During CoSC, the NPDM will be iteratively and collaboratively improved, under government direction, to enable coordination and integration across contractor and government segments.

The NPDM enables a smooth transition from CoSC to NGEN by providing detailed activity and task-level process models for each high priority ITSM process. It also serves as the foundation for process continual improvement efforts.

By documenting key process touch points between the incumbent contractor and the government, as well as interfaces and information exchange between processes, the model optimizes process interoperability, including:

- Describing processes in a standard way – all processes are described using standardized descriptions and structure, in accordance with international standards. This makes it easy to understand the content and workflow of each process.
- Providing process components that may be used by multiple processes – key process components such as activities, tasks, roles, work products, and tool interfaces are consistently documented so that other processes can interface with those components
- Activities and tasks are defined consistently so one process that must interface with another process will be able to easily identify those points of entry and exit within that process;
- Roles are defined to facilitate collaboration between roles that participate in the same tasks;
- Work products are defined so interfacing processes will understand what work products are exchanged between processes.

The NPDM provides the foundation for detailed design of priority NGEN ITSM processes. During transition, successor contractor(s) will work with the government to iteratively and collaboratively identify, define, plan, document, and schedule all of the integrated activities and

tasks required to effectively transition ITSM capabilities from the then-current service contractor environment to the target state environment.

Table of Contents
PART A

1.	Introduction.....	1
1.1	Purpose of Document	1
1.2	Objectives.....	1
1.3	Scope.....	1
1.4	Process Interface Conventions	1
1.5	Workflow Diagram Conventions	2
1.6	Role Naming	2
2.	Change Management [CHA]	4
2.1	Process Purpose.....	4
2.2	Process Policies	4
2.2.1	DoD and DON Policies	4
2.2.2	Process-Specific Policies	4
2.3	Process Outcomes.....	4
2.4	Process Scope.....	5
2.4.1	Includes.....	5
2.4.2	Excludes.....	6
2.5	Process Interfaces	6
2.6	Process Functional Requirements.....	10
2.7	Process Activities	10
2.7.1	Process Diagram.....	10
2.7.2	Process Activity Descriptions	11
2.8	Roles and Organizations	21
2.9	R/A/C/I.....	23
2.10	Resource Requirements	27
2.10.1	Resources Required to Execute the Process	27
2.10.2	Knowledge, Skills and Abilities (KSAs)	27
2.10.3	Identification and Training of Government Personnel.....	27
2.11	Data and Information Requirements.....	27

2.12	Information Work Products (IWPs)	27
2.13	Reporting Requirements	27
2.14	Current Process Metrics	28
2.15	Desired Metrics and Compliance Controls	29
2.16	Tool Requirements	29
2.17	Tools Used to Support the Process	29
2.18	Interface Requirements	30
2.19	Integration Approach	30
2.19.1	Use Case Selection	30
2.19.2	Workshops and Simulations	30
2.20	Validation Results and Remediation	30
3.	Event Management [EVE]	31
3.1	Policies	31
3.2	Outcomes	31
3.3	Scope	31
3.3.1	Includes	32
3.3.2	Excludes	32
3.4	Process Interfaces	32
3.5	Activity-Level Workflow	32
3.6	Activities	33
3.6.1	[EVE1] Establish Event Management Framework	33
3.6.2	[EVE2] Detect Event	37
3.6.3	[EVE3] Filter and Log Event	37
3.6.4	[EVE4] Correlate Event	38
3.6.5	[EVE5] Trigger Response	39
3.6.6	[EVE6] Execute Auto Response	40
3.6.7	[EVE7] Generate Alert	40
3.6.8	[EVE8] Close Event Record	41
3.6.9	[EVE9] Monitor, Manage and Report Event Management	42
3.6.10	[EVE10] Evaluate Event Management Performance	42

3.7	Roles	44
3.8	Information Work Products	45
3.9	Performance Metrics.....	46
3.10	Organizational RACI.....	46
4.	Incident Management [INC]	48
4.1	Purpose.....	48
4.2	Policies.....	49
4.3	Outcomes	49
4.4	Scope.....	49
4.4.1	Includes.....	49
4.4.2	Excludes.....	50
4.5	Process Interfaces	50
4.6	Activity-Level Workflow.....	53
4.7	Activities	54
4.7.1	[INC1] Establish Incident Management Framework	54
4.7.2	[INC2] Identify, Report and Log Incident	55
4.7.3	[INC3] Categorize and Prioritize Incident.....	58
4.7.4	[INC4] Investigate and Diagnose Incident	59
4.7.5	[INC5] Resolve and Recover Incident.....	60
4.7.6	[INC6] Close Incident	61
4.7.7	[INC7] Monitor, Manage and Report Incident Management	63
4.7.8	[INC8] Evaluate Incident Management Performance	65
4.8	Roles	67
4.9	Information Work Products	71
4.10	Performance Metrics.....	71
4.11	Organizational RACI.....	71
5.	Information Security Management [ISM]	76
5.1	Purpose.....	76
5.2	Policies.....	77
5.3	Outcomes	77

5.4	Scope.....	77
5.4.1	Includes.....	77
5.4.2	Excludes.....	78
5.5	Process Interfaces	78
5.6	Activity-Level Workflow.....	80
5.7	Activities	81
5.7.1	[ISM1] Establish Security Management Framework.....	81
5.7.2	[ISM2] Create and Sustain Information Security Policy.....	85
5.7.3	[ISM3] Categorize Information Systems for C&A.....	89
5.7.4	[ISM4] Analyze Security Threats, Vulnerabilities and Risks.....	91
5.7.5	[ISM5] Plan and Implement Security Practices	94
5.7.6	[ISM6] Direct/Perform Security Protection Operations.....	97
5.7.7	[ISM7] Monitor, Manage and Report Information Security Management.....	102
5.7.8	[ISM8] Evaluate Security Management Performance.....	105
5.8	Roles	107
5.9	Information Work Products	109
5.10	Performance Metrics.....	111
5.11	Organizational RACI.....	111
6.	IT Asset Management [ITAM]	119
6.1	Process Purpose.....	119
6.2	Process Policies	119
6.2.1	DoD and DON Policies	119
6.2.2	Process-Specific Policies	125
6.3	Process Outcomes.....	126
6.4	Process Scope.....	127
6.4.1	Includes.....	127
6.4.2	Excludes.....	127
6.5	Process Interfaces	128
6.6	Process Functional Requirements.....	129
6.7	Process Activities	131

6.7.1	Process Diagram.....	131
6.7.2	Process Activity Descriptions	133
6.8	Roles and Organizations	136
6.9	R/A/C/I.....	137
6.10	Resource Requirements	138
6.10.1	Resources Required to Execute the Process	138
6.10.2	Knowledge, Skills and Abilities (KSAs).....	138
6.10.3	Identification and Training of Government Personnel.....	138
6.11	Data and Information Requirements.....	139
6.12	Information Work Products (IWPs)	139
6.13	Reporting Requirements	139
6.14	Current Process Metrics.....	139
6.15	Desired Metrics and Compliance Controls	141
6.16	Tool Requirements	141
6.17	Tools Used to Support the Process.....	141
6.18	Interface Requirements	141
6.19	Integration Approach.....	142
6.19.1	Use Case Selection	142
6.19.2	Workshops and Simulations	142
6.20	Validation Results and Remediation	142
7.	Data management [dat].....	147
7.1	Purpose.....	147
7.2	Process Policies	148
7.2.1	DoD and DON Policies	148
7.2.2	Process-Specific Policies	149
7.3	Process Outcomes.....	150
7.4	Process Scope.....	150
7.4.1	Includes.....	150
7.4.2	Excludes.....	151
7.5	Process Interfaces	151

Data Management Dependencies with Other ITSM Processes.....	151
7.6 Process Functional Requirements.....	151
7.7 Process Activities	152
7.7.1 Process Diagram.....	152
7.7.2 Process Activity Descriptions	152
7.8 Roles and Organizations	160
7.9 R/A/C/I.....	160
7.10 Resource Requirements	161
7.10.1 Resources Required to Execute the Process	161
7.10.2 Knowledge, Skills and Abilities (KSAs)	162
7.10.3 Identification and Training of Government Personnel.....	162
7.11 Data and Information Requirements.....	164
7.12 Information Work Products (IWPs)	164
7.13 Reporting Requirements	165
7.14 Current Process Metrics	165
7.15 Desired Metrics and Compliance Controls	167
7.16 Tool Requirements	168
7.17 Tools Used to Support the Process.....	168
7.18 Interface Requirements	169
7.19 Integration Approach.....	170
7.19.1 Use Case Selection	170
7.19.2 Workshops and Simulations	170
7.20 Validation Results and Remediation	170
8. Problem Management [PRB].....	171
8.1 Purpose.....	171
8.2 Policies.....	171
8.3 Outcomes	171
8.4 Scope.....	171
8.4.1 Includes.....	172
8.4.2 Excludes.....	172

8.5	Process Interfaces	172
8.6	Activity-Level Workflow.....	174
8.7	Activities	175
8.7.1	[PRB1] Establish Problem Management Framework	175
8.7.2	[PRB2] Identify and Log Problem	177
8.7.3	[PRB3] Categorize and Prioritize Problem.....	181
8.7.4	[PRB4] Investigate and Diagnose Problem	183
8.7.5	[PRB5] Resolve Problem.....	185
8.7.6	[PRB6] Close and Review Problem	188
8.7.7	[PRB7] Monitor, Manage and Report Problem Management	191
8.7.8	[PRB8] Evaluate Problem Management Performance	192
8.8	Roles	194
8.9	Information Work Products	195
8.10	Performance Metrics.....	197
8.11	Organizational RACI	197
9.	Configuration management [CM]	204
9.1	Process Purpose.....	204
9.2	Process Policies	204
9.2.1	DoD and DON Policies	204
9.3	Process Outcomes.....	205
9.4	Process Scope.....	206
9.4.1	Includes.....	206
9.4.2	. Excludes.....	206
9.5	Process Interfaces	207
	Process Functional Requirements	208
1.12	Process Activities.....	209
1.12.1	Process Diagram.....	209
1.12.2	Process Activity Descriptions	210
	Roles and Organizations	213
1.14	R/A/C/I.....	214

1.15 Resource Requirements.....	214
1.15.1 Resources Required to Execute the Process	214
Stakeholder Resources	215
1.15.2 Knowledge, Skills and Abilities (KSAs)	215
1.15.3 Identification and Training of Government Personnel.....	215
Data and Information Requirements.....	216
1.17 Information Work Products (IWPs).....	216
1.18 Reporting Requirements.....	216
Current Process Metrics	217
1.20 Desired Metrics and Compliance Controls	218
Tool Requirements	220
1.23 Tools Used to Support the Process	220
Interface Requirements	220
1.24 Integration Approach	221
1.24.1 Use Case Selection	221
1.24.2 Workshops and Simulations	221
1.25 Validation Results and Remediation.....	221
10. Release and Deployment Management [RDM]	222
10.1 Process Purpose.....	222
10.2 Process Policies	222
10.2.1 DoD and DON Policies	222
10.2.2 Process-Specific Policies	222
10.3 Process Outcomes.....	222
10.4 Process Scope.....	223
10.4.1 Includes	224
10.4.2 Excludes.....	225
10.5 Process Interfaces	225
10.6 Process Functional Requirements.....	227
10.7 Process Activities	227
10.7.1 Process Diagram.....	227

10.7.2	Process Activity Descriptions	229
10.8	Roles and Organizations	236
10.9	R/A/C/I.....	237
10.10	Resource Requirements	238
10.10.1	Resources Required to Execute the Process	238
10.10.2	Knowledge, Skills and Abilities (KSAs)	239
10.10.3	Identification and Training of Government Personnel.....	239
10.11	Data and Information Requirements.....	239
10.12	Information Work Products (IWPs)	239
10.13	Reporting Requirements	239
10.14	Current Process Metrics.....	240
10.15	Desired Metrics and Compliance Controls	241
10.16	Tool Requirements	241
10.17	Tools Used to Support the Process.....	241
10.18	Interface Requirements	242
10.19	Integration Approach.....	242
10.19.1	Use Case Selection	242
10.19.2	Workshops and Simulations	242
10.20	Validation Results and Remediation	242
Appendix A – Change Management Standard Operating Procedure.....		1
11.	Purpose.....	1
12.	Scope.....	1
13.	PROCESS ACTIVITIES Overview	1
13.1	Procedures.....	1
13.1.1	[CHA1] Establish Change Management Process Framework	1
13.1.2	[CHA2] Create Request for Change (RFC).....	7
13.1.3	[CHA3] Assess and Prioritize RFC.....	10
13.1.4	[CHA4] Authorize ROM Development.....	13
13.1.5	[CHA5] Conduct Systems Engineering.....	16
13.1.6	[CHA6] Change Package Approval	21

13.1.7	[CHA8] Review and Close Change.....	25
Appendix B – Data Management Standard Operating Procedure		
14.	Purpose.....	1
15.	Scope.....	1
16.	PROCESS ACTIVITIES Overview	1
16.1	Procedures.....	1
16.1.1	[DAT 1] Establish a Data Management Process Framework.....	1
16.1.2	[DAT 2] Plan Data Portfolio Architecture.....	7
16.1.3	[DAT 3] Acquire and Prepare Data.....	12
16.1.4	[DAT 4] Control, QA, Deploy and Maintain Data	16
16.1.5	[DAT 5] Back-up and Restore	27
16.1.6	[DAT 6] Archive and Dispose	32
16.1.7	[DAT 7] Monitor, Report and Manage Data Management	36
16.1.8	[DAT 8] Evaluate Data Management.....	38
Appendix C – Configuration Management Standard Operating Procedures		
17.	Purpose.....	1
18.	Scope.....	1
19.	PROCESS ACTIVITIES Overview	1
19.1	Procedures.....	2
19.1.1	[CM-1] Establish Configuration Management Framework.....	2
19.1.2	[CM-2] Configuration Identification.....	6
19.1.3	[CM-3] Configuration Control.....	10
19.1.4	[CM-4] Configuration Status Accounting	13
19.1.5	[CM-5] Configuration Verification and Audit.....	17
Appendix D – Release and Deployment Management Standard Operating Procedure.....		
20.	Purpose.....	1
21.	Scope.....	1
22.	PROCESS ACTIVITIES Overview	1
22.1	Procedures.....	1
22.1.1	[RDM1] Establish the Framework	1

22.1.2	[RDM 2] Develop Release and Deployment Plan	6
22.1.3	[RDM3] Design and Build Release.....	11
22.1.4	[RDM4] Test and Verify Release.....	16
22.1.5	[RDM5] Prepare Deployment Capabilities & Perform Transition Administration	19
22.1.6	[RDM6] Perform and Verify Deployment.....	24
22.1.7	[RDM7] Review and Close Deployment.....	28
22.1.8	[RDM8] Monitor, Manage and Report Release and Deployment	31
22.1.9	[RDM9] Evaluate Release and Deployment Management Performance	35

Table of Figures

Figure 1 - Process Interface Diagram Convention.....	2
Figure 2 - Process Workflow Diagram Convention	2
Figure 3 - Change Management Interfaces	Error! Bookmark not defined.
Figure 4 - Change Management Workflow	Error! Bookmark not defined.
Figure 5 - CHA1 Workflow.....	Error! Bookmark not defined.
Figure 6 - CHA2 Workflow.....	Error! Bookmark not defined.
Figure 7 - CHA3 Workflow.....	Error! Bookmark not defined.
Figure 8 - CHA4 Workflow.....	Error! Bookmark not defined.
Figure 9 - CHA5 Workflow.....	Error! Bookmark not defined.
Figure 10 - CHA6 Workflow.....	Error! Bookmark not defined.
Figure 11 - CHA7 Workflow.....	Error! Bookmark not defined.
Figure 12 - CHA8 Workflow.....	Error! Bookmark not defined.
Figure 13 - CHA9 Workflow.....	Error! Bookmark not defined.
Figure 14 - CHA10 Workflow.....	Error! Bookmark not defined.
Figure 15 – Event Management Interfaces.....	32
Figure 16 - Event Management Workflow.....	33
Figure 17 - EVE1 Workflow	34
Figure 18 - EVE2 Workflow	37
Figure 19 - EVE3 Workflow	38
Figure 20 - EVE4 Workflow	39
Figure 21 - EVE5 Workflow	40
Figure 22 - EVE6 Workflow	40
Figure 23 - EVE7 Workflow	41
Figure 24 - EVE8 Workflow	41
Figure 25 - EVE9 Workflow	42
Figure 26 - EVE10 Workflow	43
Figure 27 - Incident Management Interfaces.....	53
Figure 28 - Incident Management Workflow	54

Figure 29 - Information Security Management Interfaces	80
Figure 30 - Information Security Management Workflow	81
Figure 31 - ISM1 Workflow	82
Figure 32 - ISM2 Workflow	86
Figure 33 - ISM3 Workflow	89
Figure 34 - ISM4 Workflow	92
Figure 35 - ISM5 Workflow	95
Figure 36 - ISM6 Workflow, part 1	98
Figure 37 - RDM6 Workflow, part 2	99
Figure 38 - ISM7 Workflow	103
Figure 39 - ISM8 Workflow	106
Figure 40: Directly Interfacing Processes	Error! Bookmark not defined.
Figure 41 - IT Asset Management Workflow	Error! Bookmark not defined.
Figure 42 - ITAM1 Workflow	Error! Bookmark not defined.
Figure 43 - ITAM2 Workflow	Error! Bookmark not defined.
Figure 44 - ITAM3 Workflow	Error! Bookmark not defined.
Figure 45 - ITAM4 Workflow	Error! Bookmark not defined.
Figure 46 - ITAM5 Workflow	Error! Bookmark not defined.
Figure 47 - ITAM6 Workflow	Error! Bookmark not defined.
Figure 48 - ITAM7 Workflow	Error! Bookmark not defined.
Figure 49 - ITAM8 Workflow	Error! Bookmark not defined.
Figure 50 - Data Management Interfaces	Error! Bookmark not defined.
Figure 51 – High-level Data Management Workflow	Error! Bookmark not defined.
Figure 52 – DAT1 – Establish Data Management Process Framework	Error! Bookmark not defined.
defined.	
Figure 53 - Problem Management Interfaces	174
Figure 54 - Problem Management Workflow	175
Figure 55 - PRB1 Workflow	176
Figure 56 - PRB2 Workflow	178
Figure 57 - PRB3 Workflow	181
Figure 58 - PRB4 Workflow	184
Figure 59 - PRB5 Workflow	186
Figure 60 - PRB6 Workflow	189
Figure 61 - PRB7 Workflow	192
Figure 62 - PRB8 Workflow	193
Figure 63 – Configuration Management Interfaces	Error! Bookmark not defined.
Figure 64 – Configuration Management High-Level Workflow	Error! Bookmark not defined.
Figure 65 - Release and Deployment Management Interfaces	Error! Bookmark not defined.
Figure 66 - Release and Deployment Management Workflow	Error! Bookmark not defined.
Figure 67 - RDM1 Workflow	Error! Bookmark not defined.
Figure 68 - RDM2 Workflow	Error! Bookmark not defined.
Figure 69 - RDM 3 Workflow, part 1	Error! Bookmark not defined.
Figure 70 - RDM3 Workflow, part 2	Error! Bookmark not defined.
Figure 71 - RDM4 Workflow	Error! Bookmark not defined.
Figure 72 – RDM4 Workflow	Error! Bookmark not defined.
Figure 73 - RDM5 Workflow	Error! Bookmark not defined.

Figure 74 - RDM6 Workflow**Error! Bookmark not defined.**
Figure 75 - RDM7 Workflow**Error! Bookmark not defined.**
Figure 76 - RDM8 Workflow**Error! Bookmark not defined.**
Figure 77 - RDM9 Workflow**Error! Bookmark not defined.**

1. INTRODUCTION

1.1 Purpose of Document

The NPDM provides the foundation for detailed design of priority NGEN ITSM processes. During transition, successor contractor(s) will work with the government to iteratively and collaboratively identify, define, plan, document, and schedule all of the integrated activities and tasks required to effectively transition ITSM capabilities from the then-current service contractor environment to the target state environment.

1.2 Objectives

The objectives of this document are to:

- Define detailed activity and task-level process models for each high priority ITSM process operating within the Navy CoSC period of performance;
- Identify key process touch points between the incumbent contractor and the government;
- Describe all processes using standardized descriptions and structure to promote process interoperability and reuse;
- Provide the foundation for continual process improvement efforts;
- Provide foundation for the development of priority NGEN ITSM processes.

1.3 Scope

The NEN Process Definition Model (NPDM) describes a set of high-priority Navy Information Technology Service Management (ITSM) processes in effect during the CoSC transition period.

1.4 Process Interface Conventions

Process interfaces are shown in a bulleted list and also shown in an interface diagram similar to that shown below.

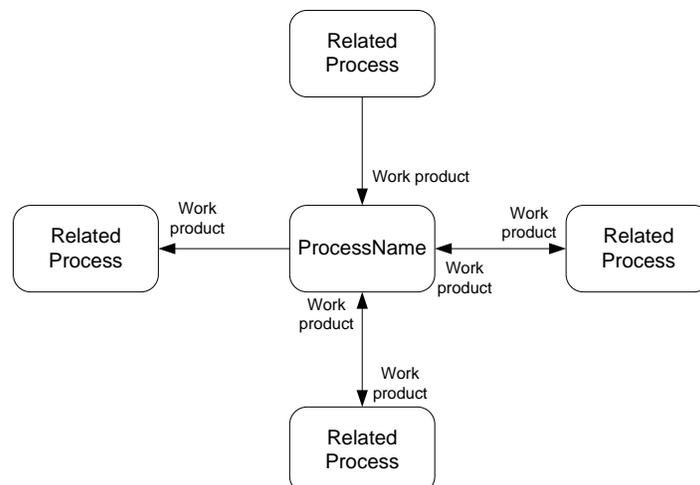


Figure 1 - Process Interface Diagram Convention

1.5 Workflow Diagram Conventions

Workflow diagrams are drawn in a single swim lane. The workflow identifies the activities in a process and the primary flow of work between activities. These are referred to as high-level or Level 1 diagrams. Common activities should be shown. Figure 2 provides an illustrative example.

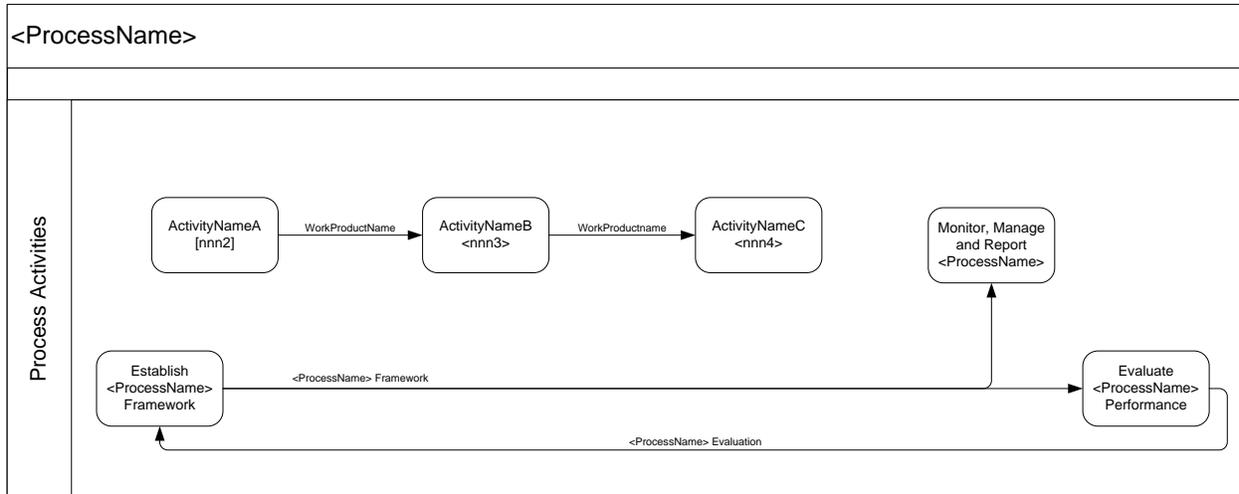


Figure 2 - Process Workflow Diagram Convention

1.6 Role Naming

Each process, at a minimum, has the following roles:

- Process Owner –Has the high-level accountability and responsibility for the direction of the process.
- Process Manager – Runs the day-to-day operation of the process.

Additional roles are also included in each process.

A table is included after the description of each role. The Responsible, Accountable, Consulted, Informed (RACI) table is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks. Full definitions for each of the roles mapped out in the RACI matrix include:

Responsible	Individuals who execute one or more process activities. There may be multiple “R” roles for a process activity.
Accountable	Individual ultimately accountable for the work. Individual with final decision authority. There is only one “A” per process activity.
Consulted	Individual who needs to be consulted before a final decision can be rendered. Two-way

	communication is assumed.
Informed	Individual(s) who must be informed when decision is made or action taken. One-way communication is assumed.

Table 1 - RACI Definitions

2. CHANGE MANAGEMENT [CHA]

2.1 Process Purpose

The purpose of Change Management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all proposed changes.

A change can be anything that alters the status of a configuration item (CI); including additions, deletions and modifications to the IT environment consisting of standard hardware, software and associated documentation.

Recording changes to configuration items via Change Request also falls within this process. A Change Request document proposes changes in IT resources or capabilities and can be triggered for many reasons from various sources.

2.2 Process Policies

2.2.1 DoD and DON Policies

This section defines the key DoD and DON Policies that govern the process.

The policies governing the NGEN Change Management process are listed in the main body of the PWS.

2.2.2 Process-Specific Policies

Policy Ref.	Policy Name	Requirement
TBD	TBD	TBD

2.3 Process Outcomes

The key qualitative and quantitative outcomes (objectives) of the Process are:

- Requests for Change are recorded and classified
- Changes are introduced within an agreed to schedule and approach.
- Requests for Change are assessed using defined criteria and approved before development
- Impacts of proposed changes are assessed.

- Change incidents and the resulting risks are minimized
- Appropriate balance is created and sustained between the need for solutions, innovations and stability within a system or IT environment.
- Unsuccessful changes are reversed or remedied

2.4 Process Scope

The domain of Change Management is usually initiated by creation of a Change Request. This document details the proposed changes in order to inform other operational and technical assessments, seeking endorsement and eventually applying the change.

Establishing classification and categorization schemes to assist with change assessment activities also defines the implementation approaches that will be assigned to approve changes. This also works to systemize supervisory control levels in conjunction with the assessment recommendations.

Some activities in the process require examination of several or all changes collectively rather than on an individual basis. For example, this examination needs to consider and identify scheduling conflicts with changes within the same target dates and environments.

2.4.1 Includes

- Planned changes, standard changes (pre-approved by policy), and emergency changes (policy exception request)
- Establishing both recurring and one-time only schedules (change windows) during which changes can be performed without negatively affecting commitments, such as project schedules, projected availability, or service level agreement (SLA) commitments
- Enforcement of standard methods and procedures from Change Request through post implementation review
- Establishing regular meetings and communication schedules to evaluate proposed changes and schedules
- Control and manage coordination of approved change implementations
- Maintenance of open channels of communications to promote smooth transition when changes take place

- Increased visibility and communication of changes to both operational, technical, and support staff

2.4.2 Excludes

- Requirements Management
- Creation of new or revised functionality
- Building the packaging for the delivery of new or revised functionality (Release and Deployment Management)
- Technical implementation, such as distribution, preparation, installation, and back out if necessary (Release and Deployment Management)
- Configuration Management, although the interface to this process must be managed
- Asset Management, although the interface to this process must be managed

2.5 Process Interfaces

This section summarizes the interfaces between the process and other ITSM processes. A direct interface occurs when a process provides a work product (input or output) to another process.

Primary interfaces with other processes include the following:

Any process can submit a Request for Change (RFC) to Change Management. However, the processes that typically submit RFCs include:

- Availability Management
- Capacity Management
- Event Management
- Facilities Management
- Financial Management
- Incident Management
- Information Security Management
- IT Asset Management
- IT Service Continuity Management
- Configuration Management
- Knowledge Management

- Problem Management
- Request Fulfillment
- Release and Deployment Management
- Service Catalog Management
- Service Level Management
- Service Portfolio Management
- Service Validation and Testing
- Transition Planning and Support

Change Management may ask processes to provide assessments of a proposed change before it is evaluated for approval. Change Management sends a Change Assessment Information Request, and the receiving process sends back Change Assessment Information. Included among those processes are:

- Availability Management
- Asset Management
- Capacity Management
- Facilities Management
- Financial Management
- Information Security Management
- IT Asset Management
- IT Service Continuity Management
- Release and Deployment Management
- Service Level Management
- Supplier Management

Evaluation – Change assessments and post-change reviews are carried out by Change Management with involvement by Evaluation.

Once authorized, other processes may be called upon to implement the change, including:

- Access Management – to make changes to user identities and access
- Data Management – to perform backups or restores

- Facilities Management – when a change involves some adjustment to facilities
- Information Security Management - to implement service security mechanisms
- IT Asset Management – when assets must be moved
- IT Service Continuity Management – to plan service continuity when services are added, changed, or removed
- Knowledge Management – to create or update knowledge assets
- Release and Deployment Management – when a change must be packaged and/or prepared before deployment
- Service Catalog Management – to update the service catalog
- Transition Planning and Support – to initiate a complex service transition

Change Information is used by a number of processes to gain an understanding of recent changes or understand the status of changes currently being implemented. This includes the following processes:

- Availability Management
- Capacity Management
- Incident Management
- IT Service Continuity Management
- Problem Management
- Request Fulfillment
- Service Catalog Management
- Service Portfolio Management
- Transition Planning and Support

Changes authorized by change management may require a release to be created by Release and Deployment Management. Such releases require a Release Acceptance from Change Management prior to deployment.

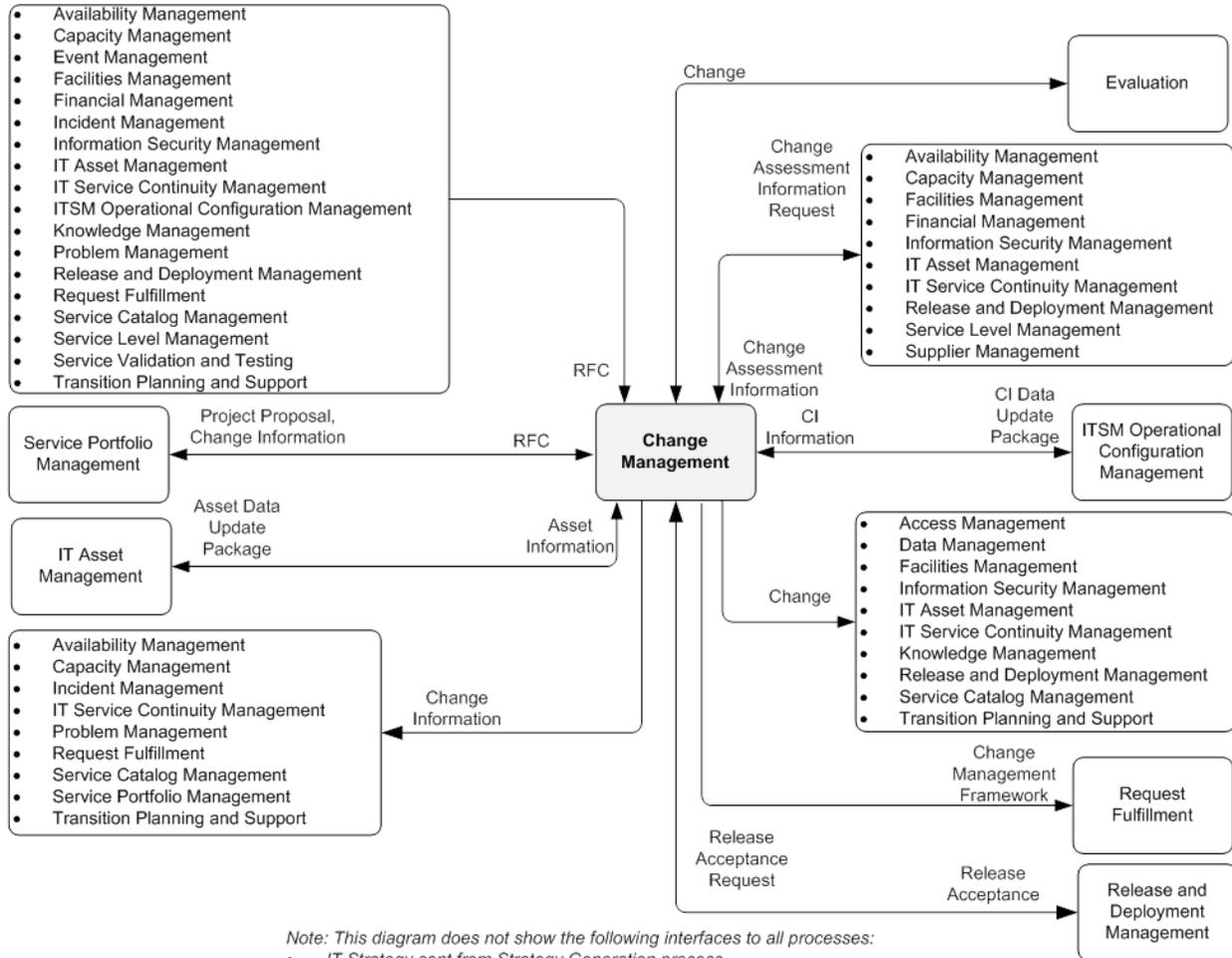
When assessing a proposed change, Configuration Management can identify configuration items that are affected by the change. During implementation of a change, updates to CI information are provided to CM as CI Data Update Packages. Similarly, information about assets is provided

by IT Asset Information. When asset information is changed, it is sent as an Asset Data Update Package to ITAM.

Request Fulfillment utilizes the list of standard changes, as defined by the Change Management Framework, to route standard changes to the appropriate process for implementation. This process is affected by the strategic direction described in the IT Strategy, generated by the Strategy Generation process. This process provides content in the form of Knowledge Items to the Knowledge Management process. In addition, Knowledge Management organizes and processes that content into Knowledge Assets.

Compliance Management identifies specific Compliance Plans and Controls that should be adhered to by this process to meet standards and regulations that should be complied with. In return, this process provides an evaluation of how those standards and regulations were complied with.

The following diagram graphically depicts process interface relationships and work products:



Note: This diagram does not show the following interfaces to all processes:

- IT Strategy sent from Strategy Generation process
- Compliance Plans and Controls from Compliance Management process
- Knowledge Assets from Knowledge Management process

In addition, this diagram does not show the following interface to Knowledge Management from all processes:

- Knowledge Items sent to the Knowledge Management process

Figure 3 – Change Management Interfaces

2.6 Process Functional Requirements

This section defines all of the NGEN Functional Area Requirements applicable to the process in a requirements traceability matrix (RTM).

ID	Date Recorded	Functional Area	Requirement
1	01/04/12	DA/TA	The DA/TA shall have the ability to review and veto any proposed change to the network infrastructure that materially impacts network architecture.

2.7 Process Activities

2.7.1 Process Diagram

This section defines the high level process activities in a standardized swim lane format (the process model should always be aligned to the current version of the NNPDM document):

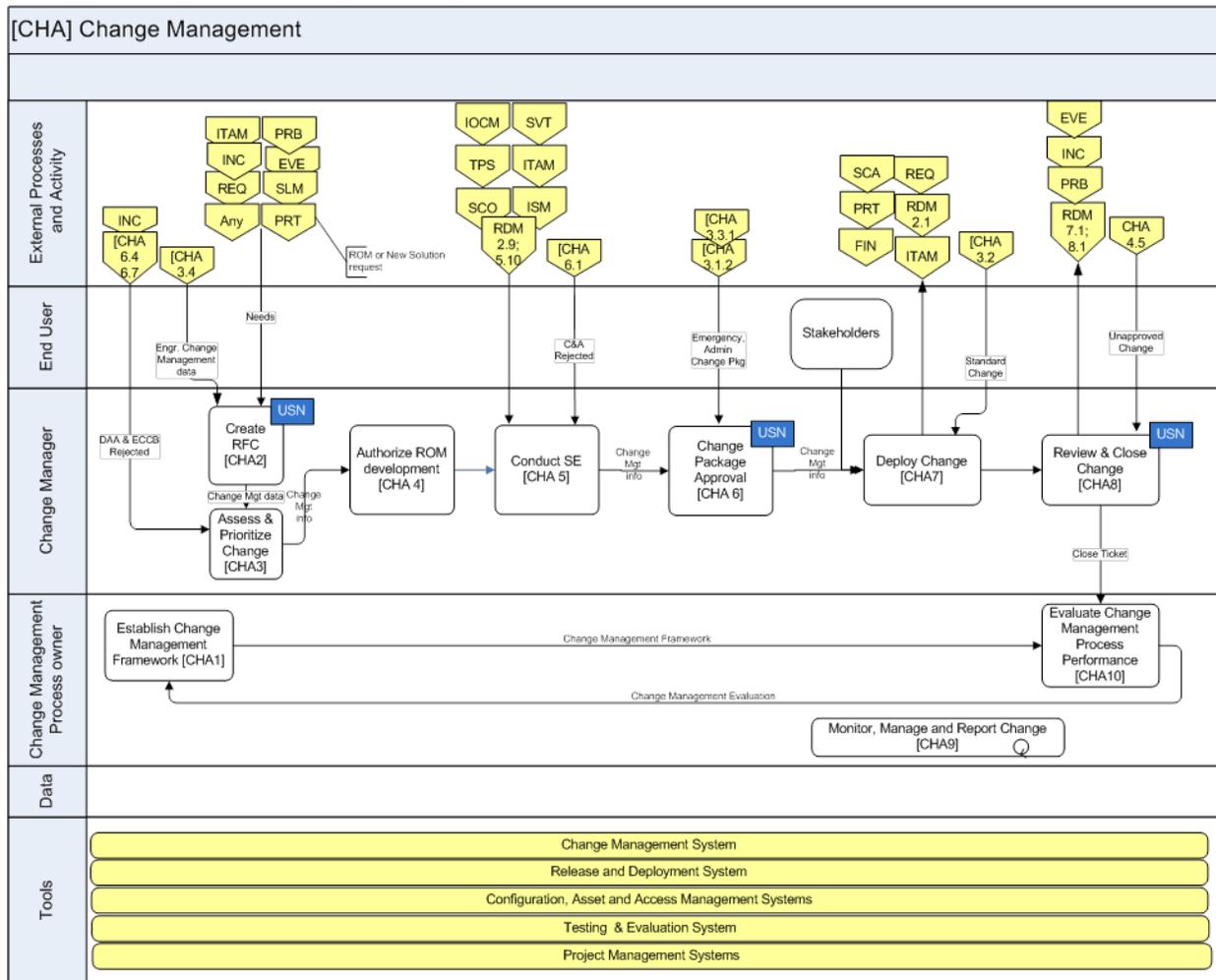


Figure 4 – Change Management Process Model

2.7.2 Process Activity Descriptions

This section defines the details of each activity in the process model:

CHA1	Establish Change Management Framework
Description:	<p>This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the “process framework” and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for making changes and improvements to the process framework. The process framework is a collection of information, not necessarily a single document, which includes:</p>

	<ul style="list-style-type: none"> • Process purpose, scope, goals, and capabilities • Process policies, standards, and conceptual models • Process data requirements • Role responsibilities • Organizational responsibilities <p>Detailed procedures and best practices, including, but not limited to:</p> <ul style="list-style-type: none"> o Scope of a “standard change” o Change classifications, such as major, minor, emergency, etc. o Change review practices o Change Advisory Board management practices • Interfaces with other processes and programs • Measurements and controls • Tool requirements
Supplier:	<ul style="list-style-type: none"> • Change Management Process Owner • Change Management Manager • Change Analyst • Change Approver (ECCB/CAB/E-CAB) • CAB Members (HP Deployment CAB) • Service Provider Enterprise Operations Manager • HP-ES Change & Program Manager
Inputs:	<ul style="list-style-type: none"> • Change Management Evaluation
Standard Operating Procedures (SOPs):	<p>SOPs Exist for This Activity? Yes</p> <ul style="list-style-type: none"> • CHA_Establish_Process_Framework_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • Change Management Activity Data • Change Management Framework • Project Proposal
Customer:	All PM NEN data owners, authors, editors, users
Assumptions:	<ul style="list-style-type: none"> • Establishing the framework is a collaborative effort between the Government and Contractor • The Government will approve the final framework prior to

		<p>implementation</p> <ul style="list-style-type: none">• The Framework will adopted by all Government and Contractor personnel to achieve standardization and quality objectives
--	--	---

CHA2		CREATE RFC	
	Description:	<p>This activity involves formulating and storing the information about any proposed or after-the-fact change.</p> <p>The request will contain a defined outline of informational sections which have been established as necessary in order for it to progress into an assessment and the further activities of Change Management. Information can vary depending upon the context, scale, and potential impact of the requested change.</p>	
	Supplier:	<ul style="list-style-type: none"> • NetOps 1 • Authorized Submitters 	
	Inputs:	<ul style="list-style-type: none"> • Request for Change • Tuning and Capacity Delivery Allocation Outcomes 	
	Standard Operating Procedures (SOPs):	<p>SOPs Exist for This Activity? Yes</p> <ul style="list-style-type: none"> • CHA_Create_RFC_SOP_v1.0 	
	Outputs:	<ul style="list-style-type: none"> • Change Management Activity Data • Request for Change 	
	Customer:	All PM NEN data owners, authors, editors, users	
	Assumptions:	<ul style="list-style-type: none"> • 	

CHA3		ASSESS AND PRIORITIZE CHANGE	
	Description:	<p>This activity begins with the examination of the change request to determine if it should be accepted for consideration. To accept a change request all required information must be logged; omitted or incomplete information can cause a change request to be returned. The return of the change request will usually indicate that the request can be re-submitted if the missing or inadequate information is provided. After initial acceptance, the change request is Prioritized and categorized.</p>	
	Supplier:	<ul style="list-style-type: none"> • NetOps 1 	

	<ul style="list-style-type: none"> • Authorized Submitters
Inputs:	<ul style="list-style-type: none"> • CI Information • Request for Change
Standard Operating Procedures (SOPs):	<p>SOPs Exist for This Activity? Yes</p> <ul style="list-style-type: none"> • CHA_Assess and Prioritize_Change_SOP_v1.0 • Architecture Baselines and Roadmaps • Service Catalog
Outputs:	<ul style="list-style-type: none"> • Change Information • Change Management Activity Data • Request for Change
Customer:	All PM NEN data owners, authors, editors, users
Assumptions:	<ul style="list-style-type: none"> •

CHA4	AUTHORIZE ROM DEVELOPMENT
Description:	<p>This activity analyzes each change to determine its impact on existing and planned CIs, as well as the impact on resources required to build and deploy the change. This involves identifying the appropriate change model for handling the change, scheduling a CAB meeting if specified by the change model, and obtaining a complete set of analysis results and issues.</p> <p>In this activity, the impact of a change is evaluated from both the IT and organizational perspectives, ensuring that the change can be successfully implemented with a minimal impact to committed services and still meet government and organizational requirements.</p>
Supplier:	<ul style="list-style-type: none"> • System Engineering • Change Management Analyst • Change Assessor • Change Authority • Change Owner
Inputs:	<ul style="list-style-type: none"> • Asset Request Status

	<ul style="list-style-type: none"> • Change Assessment Information • CI Information • Project Plan • Request for Change • Solution Design
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • CHA_Authorize_ROM_Development_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • Asset Deployment Inquiries and Requisitions • Change Management Activity Data • Change Assessment Information Request • Change Information
Customer:	All PM NEN data owners, authors, editors, users
Assumptions:	<ul style="list-style-type: none"> •

CHA5	CONDUCT SYSTEMS ENGINEERING	
Description:	TBD	
Supplier:	<ul style="list-style-type: none"> • 	
Inputs:	<ul style="list-style-type: none"> • TBD 	
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • CHA_Conduct_Systems_Engineering_SOP_v1.0 	
Outputs:	<ul style="list-style-type: none"> • TBD 	
Customer:	All PM NEN data owners, authors, editors, users	
Assumptions:	<ul style="list-style-type: none"> • 	

CHA6		CHANGE PACKAGE APPROVAL	
Description:	TBD		
Supplier:	•		
Inputs:	• TBD		
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • CHA_Change_Package_Approval_SOP_v1.0 		
Outputs:	• TBD		
Customer:	All PM NEN data owners, authors, editors, users		
Assumptions:	•		
CHA7		DEPLOY CHANGE	
Description:	TBD		
Supplier:	•		
Inputs:	• TBD		
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? No <ul style="list-style-type: none"> • TBD 		
Outputs:	• TBD		
Customer:	All PM NEN data owners, authors, editors, users		
Assumptions:	•		

CHA8		REVIEW AND CLOSE CHANGE	
Description:	This activity contains the tasks involved in reviewing all implemented changes, after a predefined period has elapsed or another review trigger has been activated. The activity ensures the change had the desired effect and met its objectives, and that users and customers are content with the results, or to identify any shortcomings. The review activity determines whether the implementation plan and the back-out		

		<p>plan worked correctly, and whether the change was implemented on time and cost. It determines whether any follow up actions (such as the creation of a new change request) are required.</p> <p>A formal close of the change is performed. The closure of a change includes updating other process areas of the status of the change. It should be noted that this activity is shared with the Evaluation process.</p>
	Supplier:	<ul style="list-style-type: none"> •
	Inputs:	<ul style="list-style-type: none"> • TBD
	Standard Operating Procedures (SOPs):	<p>SOPs Exist for This Activity? Yes</p> <ul style="list-style-type: none"> • CHA_Review and Cllose_Change_SOP_v1.0
	Outputs:	<ul style="list-style-type: none"> • TBD
	Customer:	All PM NEN data owners, authors, editors, users
	Assumptions:	<ul style="list-style-type: none"> •

CHA9	MONITOR, MANAGE, AND REPORT CHANGE MANAGEMENT	
	Description:	<p>This activity involves the overall monitoring of work within the process and reporting on specific items or general status to stakeholders. This activity involves the following:</p> <ul style="list-style-type: none"> • All process work is monitored to determine if Requests for Change and changes are being processed properly and in a timely manner • If monitoring indicates issues with the processing of Requests for Change and changes, then actions may be performed to resolve processing issues • Reports are generated, either upon request or at scheduled intervals, for stakeholders interested in specific work items or in the process as a whole
	Supplier:	<ul style="list-style-type: none"> •
	Inputs:	<ul style="list-style-type: none"> • Release and Deployment Management Report • Report Request

		<ul style="list-style-type: none"> Request Fulfillment Report
	Standard Operating Procedures (SOPs):	<p>SOPs Exist for This Activity? No</p> <ul style="list-style-type: none"> TBD
	Outputs:	<ul style="list-style-type: none"> Change Information Change Management Activity Data Change Management Report
	Customer:	All PM NEN data owners, authors, editors, users
	Assumptions:	<ul style="list-style-type: none">

CHA10		EVALUATE CHANGE MANAGEMENT PERFORMANCE
	Description:	This activity describes the tasks required to assess the efficiency and effectiveness of the change management process. It includes the capture of information on change records, the relationship with other process areas, and the suitability of procedures and training. It is used as a basis to ensure CHA remains fit for purpose and identifies where changes to the process might be required.
	Supplier:	<ul style="list-style-type: none">
	Inputs:	<ul style="list-style-type: none"> Change Management Activity Data
	Standard Operating Procedures (SOPs):	<p>SOPs Exist for This Activity? No</p> <ul style="list-style-type: none"> TBD
	Outputs:	<ul style="list-style-type: none"> Change Management Evaluation
	Customer:	All PM NEN data owners, authors, editors, users
	Assumptions:	<ul style="list-style-type: none">

*Note: see appendix E for additional details of process information captured during the COSC/C2 summits between the government and HP Enterprise Services.

ORGANIZATION AND ROLES

2.8 Roles and Organizations

This section defines the roles (e.g. Process Owner, Process Manager, Analyst, etc.) and functional organizations (e.g. DA/TA, Logistics, NetOps, etc.) involved in executing the process.

Role Name	Brief Role Description and Responsibilities
Change Management Process Owner	<p>The Change Management Process Owner is accountable to senior management for the proper design, execution, and improvement of the process. This individual ensures that the process is being carried out, but does not run the day-to-day operation of the process. The Change Management Process Owner receives regular updates concerning the performance of the process and represents this process concerning all decisions being made by senior management. The Change Manager is accountable to the Change Management Process Owner. This role:</p> <ul style="list-style-type: none"> Carries out the Process Owner responsibilities for the Change Management Process Keeps informed of the process's operational status and critical level changes. Assists in making high-level decisions and involving senior level management when necessary.
Change Manager	<p>The Change Manager is primarily responsible for the overall quality of the Change Management process. He/she is the main coordinator within this process and is the focal point regarding changes for both the customer and the IT organization. Therefore, all managers in the IT organization should support the individual in this role.</p> <p>The Change Process Manager is accountable to the Change Management Process Owner. This role:</p> <ul style="list-style-type: none"> Accepts, prioritizes, and categorizes RFCs Rejects any change request that is completely out of scope or out of policy for Change Management Chairs the Change Advisory Board (CAB) and Emergency Change Advisory Board (ECAB) meetings Ensures that all preparations have been made for a CAB meeting, including creating of agenda, circulation of RFCs to be considered, and inviting of participants Has the ability to review all planned changes Obtains authorization for submitted RFCs from the Change Authority Ensures post review of exception changes to evaluate if the change addressed a real or a perceived exception condition Utilizes the Change Management reporting system to monitor and track changes Negotiates end-user down time for change implementation Creates consolidated change schedule and resolve any scheduling conflicts Identifies RFCs that have not been acted upon in a timely manner and takes appropriate action Create and distribute Change Management reports Reviews all implemented changes to ensure that they have been successfully completed Closes RFCs Carries out the Process Manager responsibilities for the Change Management Process

Role Name	Brief Role Description and Responsibilities
Change Analyst	<p>The Change Analyst uses deep technical knowledge and subject matter expertise to understand organizational, operational and technical issues and impacts regarding proposed change. Analysis involves the understanding of causes and effects. The analyst uses the knowledge gained from analysis to make recommendations or resolutions. This role:</p> <ul style="list-style-type: none"> Provides subject matter expertise to understand the impacts of proposed changes. Provides business or technical information. Provides recommendations to Change Assessors.
Change Assessor	<p>The Change Assessor is responsible for assessing a change request and assigning it to one of the approval statuses. Change Assessors are typically representatives of groups directly involved in or impacted by the change. This role:</p> <ul style="list-style-type: none"> Provides timely assessment of a requested change from a specific perspective. (It should be noted that a change can be approved from the perspective of various Change Assessors, but the change is not authorized until the Change Authority reviews the feedback from all Change Assessors and authorizes the change) Ensures all applicable changes are reviewed Assesses impacts (business, technical, scheduling, implementation, and so on) of a change Communicates any issues or concerns with a change to the Requestor with a copy to the Change Manager and all pre-defined Assessors Identifies an alternate Assessor to the Change Manager, when applicable. Communicates an alternate Assessor to the Change Manager Considers how the change implementation may impact schedules
Change Authority	<p>The Change Authority has the power to authorize a change. This right may be provided to a manager, an executive, or a team of people. This role:</p> <ul style="list-style-type: none"> Reviews all assessments concerning a proposed change Weighs the pros and cons of a proposed change Makes the final decision concerning whether the change is authorized or not
Change Implementer	<p>The Change Implementer is the person assigned by the Change Manager to manage the promotion of the change to the pre-production and/or production environments. This role may involve different team members depending on the type of change and the subject matter. The Change Implementer receives day-to-day direction from the Change Manager and is responsible to the Change Manager for successful implementation of the change. This role:</p> <ul style="list-style-type: none"> Ensures timely implementation of the requested change Attempts to resolve any issues with the implementation of the required change Execution of change remediation procedures, in case of a failure during one of the implementation procedures Follows time guidelines for executing remediation procedures Creates a incident ticket for changes that failed implementation Updates status of change ticket Notifies Operations and/or Service Desk with the status of the change Updates Configuration Management of status of Configuration Items (CI) Updates manuals and/or operating instructions when applicable

Role Name	Brief Role Description and Responsibilities
Change Owner	<p>The Change Owner is responsible for an individual change. The Change Owner follows the change from beginning to end, bringing in analysts and specialists as needed to complete the project. The Change Owner is responsible for seeing that analysts and specialists bring the change to a close. This role:</p> <ul style="list-style-type: none"> Obtains assessments of requested changes from stakeholder processes in accordance with Change Management policy Presents proposed changes to the CAB Builds the change Creates and tests the change Carrying out the test plan to its completion Prepares a remediation approach in the case of unsuccessful implementation of the change Creates Implementation Plan Develops a viable change plan and timeline Updates manuals and/or operating instructions when applicable Conducts post review to assure successful implementation along with identification of any external impacts or new requirements Notifies the Change Manager of unsuccessful changes. If an unplanned outage occurred, the Change Owner must explain how it occurred Identifies and coordinates activities relating to the changes Closely monitors the progress of exception changes Closes the change
Requestor	<p>The Requestor submits requests to the IT organization. These requests may come in the form of an incident, problem, problem, a service request, or a request for change. This role:</p> <ul style="list-style-type: none"> Utilizes IT services to perform business tasks. Contacts the Service Desk for Requests for Information, Service Requests, incidents, or RFCs. Provides information, as needed, for incidents submitted, problems related to incidents opened by the Requestor, or change requests submitted. Ensures that a change request is complete with accurate information at a sufficient level of detail to implement the change Works with the Change Manager to resolve any data inconsistencies with the request. Responds to all issues/concerns raised by the Approvers. Ensures all issues/concerns with each submitted request are resolved.
Stakeholder	<p>A stakeholder is anyone who has a vested interest in the results of a task. Stakeholders represent organizational and functional entities other than those already identified. This role participates in:</p> <ul style="list-style-type: none"> Information-gathering or requirements gathering. Analysis results Troubleshooting results Plans that may impact the work done by the stakeholder

2.9 R/A/C/I

This section contains a process-level RACI chart that shows the relationship between the activities and roles within the organization.

Processes may span departmental boundaries; therefore, procedures and work instructions within the process need to be mapped to roles within the process. These roles are then mapped to job functions, IT staff and departments. The Process Owner is accountable for ensuring process interaction by implementing systems that allow smooth process flow.

The Responsible, Accountable, Consulted, Informed (RACI) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks. Listed below are the roles that have been identified in the process.

R (Responsible) – A Responsible organization is involved in the daily execution of process activities. There may be more than one organization responsible for a given activity. Designating an organization as “Responsible” implies that they fall under the guidance and review of the “Accountable” party. Responsible organizations may or may not be organizationally aligned under the Accountable organization.

A (Accountable) – An Accountable organization serves as the overall owner of process quality and end results. There should only be one Accountable organization per process activity.

C (Consulted) – A Consulted organization provides knowledge and/or information to an activity. These organizations function as “part-time” actors in the process by contributing to specific situations, providing insight to others, performing very clear tasks, etc.

I (Informed) – An Informed organization receives specific information about process execution, status, etc.

Process Activity	Change Process Owner	Change Manager	Change Analyst	Change Assessor	Change Authority	Change Implementer	Change Owner	Requestor
[CHA1] Establish Change Management Framework	A/R	R/C	I		I		I	
[CHA2] Create RFC		C/I					I	A/R
[CHA3] Assess and Prioritize Change		A					R	C
[CHA4] Authorize ROM Development		A/R	R	R	I		R/C/I	I
[CHA5] Conduct Systems Engineering		A	I		R/I		R/I	C/I
[CHA6] Change Package Approval		R/I			I		A/R	I
[CHA7] Deploy Change		A			I	R/I	R/I	C/I
[CHA8] Review and Close Change		A/R/I			I		R/I	C/I
[CHA9] Monitor, Manage and Report Change Management	I	A/R	R/I					

Process Activity	Change Process Owner	Change Manager	Change Analyst	Change Assessor	Change Authority	Change Implementer	Change Owner	Requestor
[CHA10]Evaluate Change Management Performance	A	R/I	R/I					

2.10 Resource Requirements

2.10.1 Resources Required to Execute the Process

TBD

2.10.2 Knowledge, Skills and Abilities (KSAs)

TBD

2.10.3 Identification and Training of Government Personnel

TBD

DATA AND INFORMATION

2.11 Data and Information Requirements

This section summarizes the data and information management requirements of the process, and identifies the key consumers (e.g. roles, organizations) of process information work products.

2.12 Information Work Products (IWPs)

This section details the process IWPs including their usage and target audience. IWPs will be used either internally within the process which generated them, or by another process which receives the work product. IWPs will contribute to the Command and Control (C2) analysis and decisions used in managing the process:

IWP	Target Audience	Description/Usage
TBD	TBD	TBD

2.13 Reporting Requirements

This section defines process reports:

Report Elements	Amplifying Information
Report Name	TDB
Report Description	TDB
Report Audience	TDB
Report Owner	TDB
CSFs In Report	TDB
KPIs/Metrics Used In	TDB

Report	
Report Frequency	TDB

PERFORMANCE MANAGEMENT

2.14 Current Process Metrics

This section lists the Critical Success Factors (CSFs) and Key Performance Indicators (KPIs) used to baseline and measure process transition success.

Effective day-to-day operation and long-term management of the process requires measuring the process. Reports must be defined, produced and distributed to enable the management of process-related issues and initiatives. Daily performance management occurs with the process manager. Long-term trending analysis and management of significant process activities occurs at the process owner.

A powerful vision and well-defined mission statement are critical to defining enterprise goals and objectives. Process governance starts with establishing objectives for the enterprise, and continuous performance management aids direction of activities aligned with those set objectives. The Process Owner is responsible for measuring and providing value-based reporting. Critical Success Factors (CSFs) identify the most important actions for achieving control over the process and Key Performance Indicators (KPIs) measure whether or not a control is meeting its objective.

Continual service improvement depends on accurate and timely process measurements and relies on obtaining, analyzing, and using information that is practical and meaningful to the process. Measurements of process efficiency and effectiveness enable NGEN management to track process performance and improve overall end-user satisfaction.

The following table summarizes the relationships between process CSFs and KPIs. See Appendix D for a complete list of CSFs and KPIs.

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	TBD	1	TBD
		2	TBD
		3	TBD
		4	TBD
		5	TBD
		6	TBD
		7	TBD
2	TBD		TBD
			TBD
			TBD
			TBD

*Note: Additional metric details incl. threshold and objective values are defined in the SOPs.

2.15 Desired Metrics and Compliance Controls

This section provides a narrative description of additional metrics and compliance controls applicable to the process, but not currently in place to support Transition.

TBD

TOOLS AND TECHNOLOGY

2.16 Tool Requirements

This section defines key tool automation capability, interface, and interoperability requirements:

Requirement	Process Activity
Change Ticketing Management System	Creating, tracking, closing and management of changes
Configuration Management System	Allow for the tracking and management of new and changed CIs

2.17 Tools Used to Support the Process

This section defines the requirements met by COSC tools today and documents key gaps:

Requirement	COSC Tool Used Today	Measure -ment	Gap	Recommendation
Change Tracking	BMC Remedy	Partially Meets		TBD

INTEGRATION AND VALIDATION

2.18 Interface Requirements

This section defines the key interfaces with other processes, tools, governance bodies, and resources (service owners, vendors):

Interface ID	Interface Description
TBD	TBD

2.19 Integration Approach

2.19.1 Use Case Selection

TBD

2.19.2 Workshops and Simulations

TBD

2.20 Validation Results and Remediation

TBD

Error ID	Validation Scenario	Step Description	Type of Error Found	Error Description
		TBD	TBD	TBD

3. EVENT MANAGEMENT [EVE]

The purpose of the Event Management process is to monitor all events that occur throughout the enterprise IT infrastructure providing detecting and escalating exception conditions and Situational Awareness (SA). An event is any detectable or discernible occurrence that is significant for the management of the IT infrastructure or the delivery of an IT service. The Event Management process provides notifications created by an IT service, Configuration Item (CI), or monitoring tool. Event Management may also be used as the basis for automating many operational management activities.

3.1 Policies

- This process is governed by the terms and conditions of the Continuity of Service Contract (CoSC)

3.2 Outcomes

There are several qualitative and quantitative benefits that can be achieved by implementing an effective and efficient Event Management process. The value of EVE is to provide:

- Improved SA of all Critical Services and infrastructure components/systems
- Enhanced ability to make informed C2 decisions, based on the mission of the war fighter
- Improves service availability by automatically escalating exception conditions to the Incident Management Process

Defined warning criteria, used to display alerts in Network Operations Centers (NOCs), enable improved visibility into potential Service disruptions and allow C2 decisions/actions to proactively lessen potential impacts.

3.3 Scope

Event Management can be utilized to capture/display near real-time SA data enabling increased C2 of the infrastructure, defined service levels and evaluation of process performance.

Examples of events which may require monitoring include:

- Information Security related activity (e.g. intrusion detection)
- Performance of CIs (e.g. network devices or servers)
- Environmental conditions potentially impacting normal IT operations (e.g. data center temperature, humidity, fire or smoke)
- Desired normal operational activity (e.g. server backups completed or user logon/logoff attempts)

3.3.1 Includes

- Both real time and historical event information
- Examination and analysis of individual events
- Correlation and filtering of events, to identify alert notifications and other conditions
- Creation of incident records from event information
- Capture, logging and administration of data generated by the activities within this process

3.3.2 Excludes

- System monitoring (while system monitoring is a primary input to the Event Management process, the activities of configuring CIs to interface with the Event Management System [EMS] are outside the scope of the Event Management process)

3.4 Process Interfaces

Primary interfaces with other processes include the following:

- Event Management may identify specific events, sequences of events, or combinations of events as an incident, based on event handling rules. These incidents are logged by Incident Management. Such events may either be handed off to Incident Management for resolution or may be automatically responded to and closed by Event Management. Event Management may make use of incident information to determine whether some events should be sent to Incident Management.
- Some events may require a change request to resolve the event. For instance, an event may indicate that a system is down and needs to be replaced. In such instances, an RFC is sent to Change Management to resolve the outage.
- Problem Management makes use of information about events to help identify existing or potential service outages

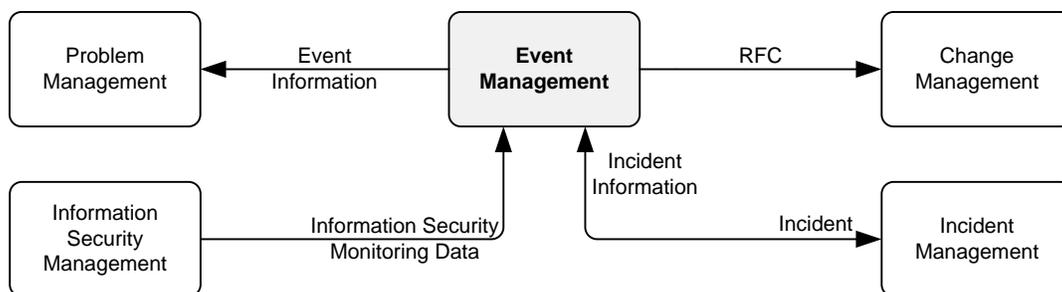


Figure 5 – Event Management Interfaces

3.5 Activity-Level Workflow

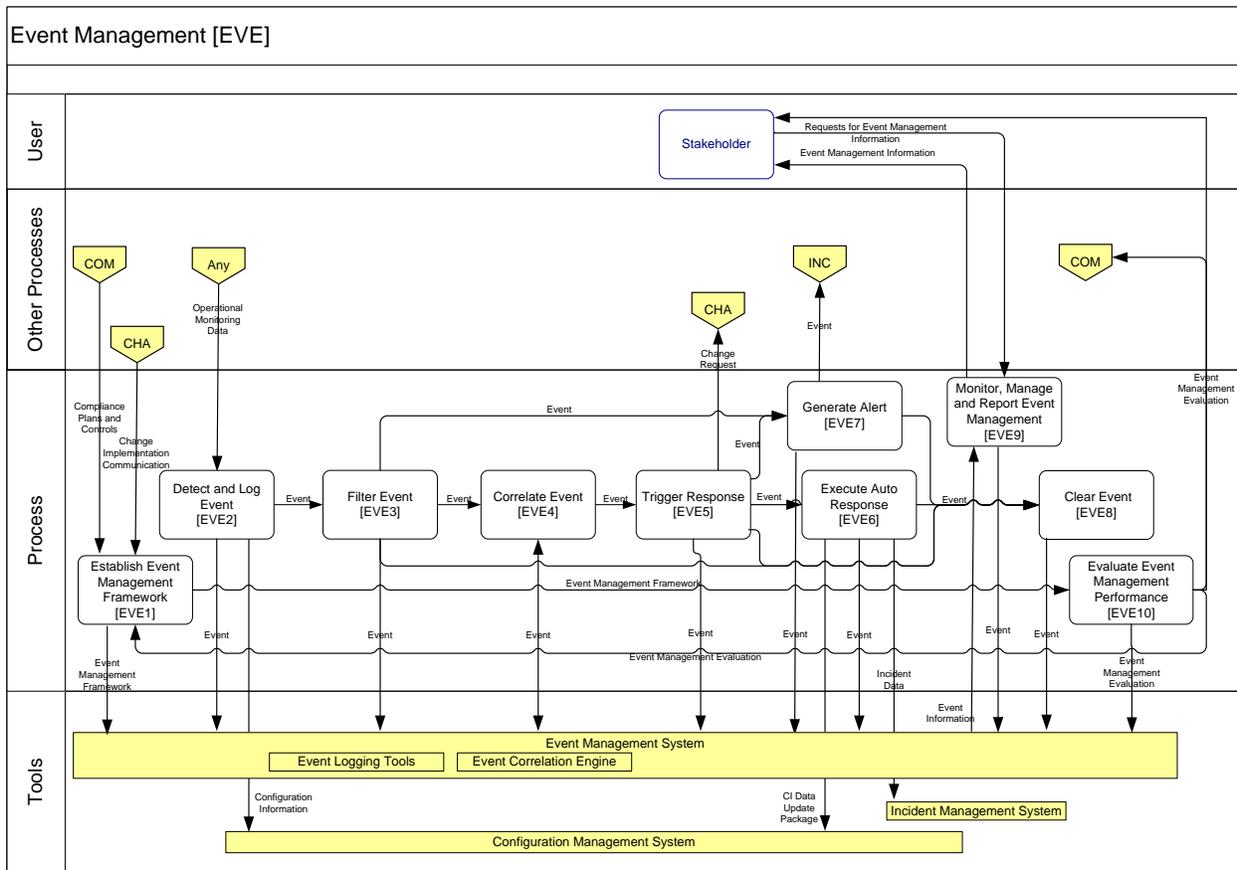


Figure 6 - Event Management Workflow

3.6 Activities

3.6.1 [EVE1] Establish Event Management Framework

This activity consists of tasks that establish the foundation of the Event Management process. Establishing the Event Management Framework also includes the continuous improvement of Event Management, including the review of process evaluation results and the implementation of recommended improvement actions.

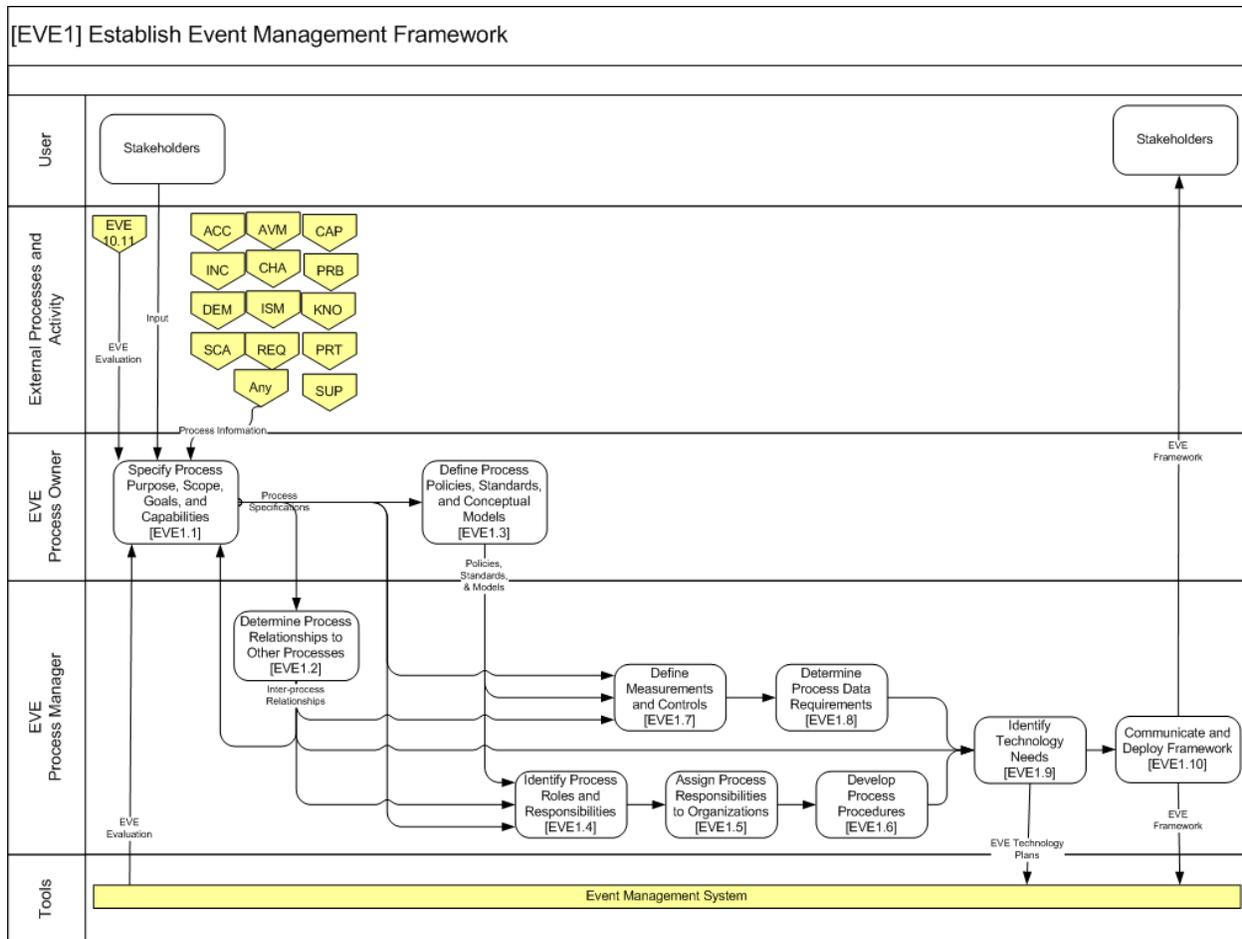


Figure 7 - EVE1 Workflow

3.6.1.1 TASKS

- Specify Process Purpose, Scope, Goals, and Capabilities
- Determine Process Data Requirements
- Define Process Policies, Standards, and Conceptual Models
- Identify Process Roles and Responsibilities
 - Assign Process Responsibilities to Organizations
 - Develop Process Procedures
 - Define Measurements and Controls
 - Determine Process Relationships to Other Processes
 - Identify Technology Needs
 - Communicate and Deploy Framework

3.6.1.2 DECISION TIMELINES

N/A

3.6.1.3 GAPS

The headings in these tables are described in more detail in Appendix A.

Description	Severity	Mitigation	Timeline	Tools
Define method to coordinate the agenda for Service Operation	Moderate	Dial in as required or ad hoc meeting as required	30 days	N/A
Format for EVE Framework change proposals	Moderate	N/A	30 days	N/A
Define process for changing EVE framework (internal govt)	Critical	Ad-hoc	30 days	N/A
SOP for EVE	Moderate	N/A	180 days	N/A
Other PO have appendices to EVE SOP	Moderate	N/A	60 days following applicable C2 Offsite	N/A

3.6.1.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools
Incident Management	Automated	Terminate	Netcool/Ops Manager, SSIM	N/A
Problem Management	Automated	Terminate	Netcool/Ops Manager, SSIM	N/A
Change Management	Automated	Terminate	Netcool/Ops Manager, SSIM	N/A

3.6.1.5 LOCATION

N/A

3.6.1.6 MEETINGS

Purpose	Live/Virtual	Methodology	Lifespan	Tools	Comments
---------	--------------	-------------	----------	-------	----------

Purpose	Live/Virtual	Methodology	Lifespan	Tools	Comments
Discuss EVE Framework	Live/Virtual	HP runs meeting	on-going	Power point	Leverage existing bi-weekly Service Operation meeting. Expanding from INC to involve EVE

3.6.1.7 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Access Point(s)	Tools
EVE Framework change proposal	TBD	as required	Distribution / PEO-EIS portal	email, Microsoft SharePoint	N/A

3.6.1.8 METRICS

N/A

3.6.1.9 ORGANIZATIONS

Process Point	Position	Org	Name	Contact Data	Tools
EVE PO		NNWC	NetOps 1 Director		
HP EVE		HP	Data Center Operations (DCO)		

3.6.1.10 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools
CoSC				

3.6.2 [EVE2] Detect Event

This activity involves receipt of all predefined events detected into the Event Management System (EMS) monitoring within the IT environment. When an event is actively or passively detected, it is the responsibility of those managing the device to ensure a message is sent, in an agreed format and that protocol is adhered to. To protect the integrity and performance of the EMS, event notifications will only be accepted from pre-authorized devices.

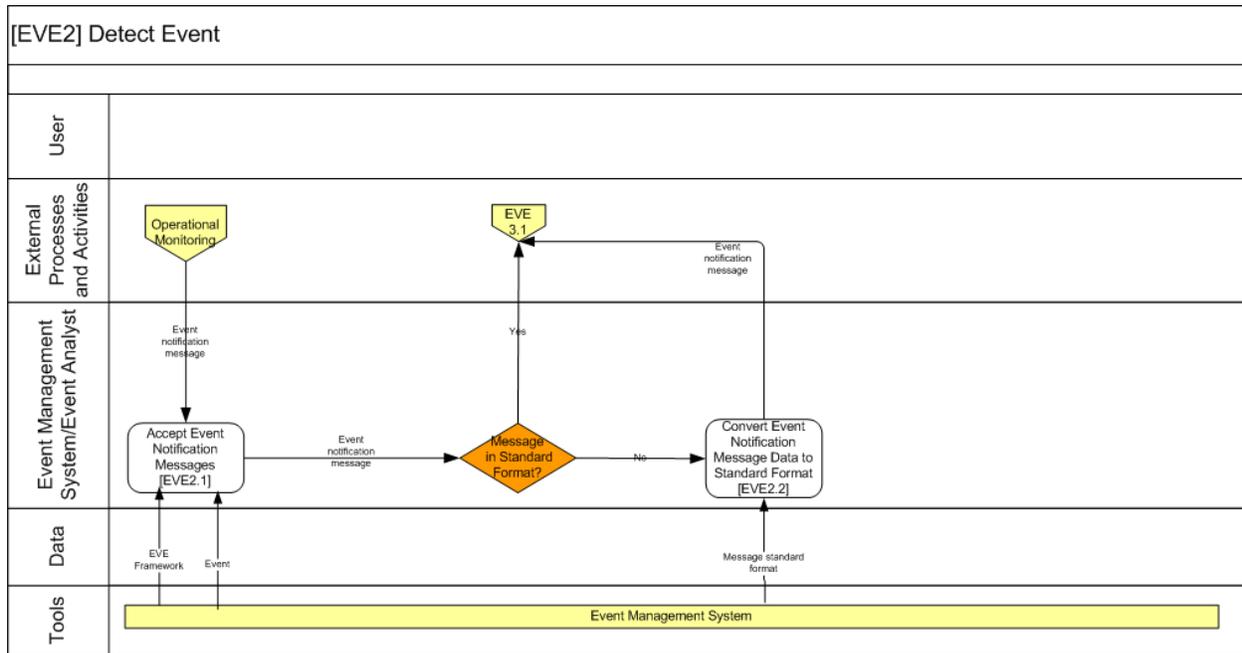


Figure 8 - EVE2 Workflow

3.6.2.1 TASKS

- Accept Event Notification Messages
- Convert Event Notification Message Data to Standard Format

3.6.3 [EVE3] Filter and Log Event

This activity determines if the event must be communicated or ignored based on predefined criteria. The specific event resulting from either a status change of a monitored device or application is recorded into the Event log. Events are categorized as:

- Informational - used for logging purposes (no action required, but should be retained as necessary for forensics)
- Warning - used whenever a threshold is being approached or breached
- Exception - an event that is impacting the mission and needs to be elevated to Incident Management.

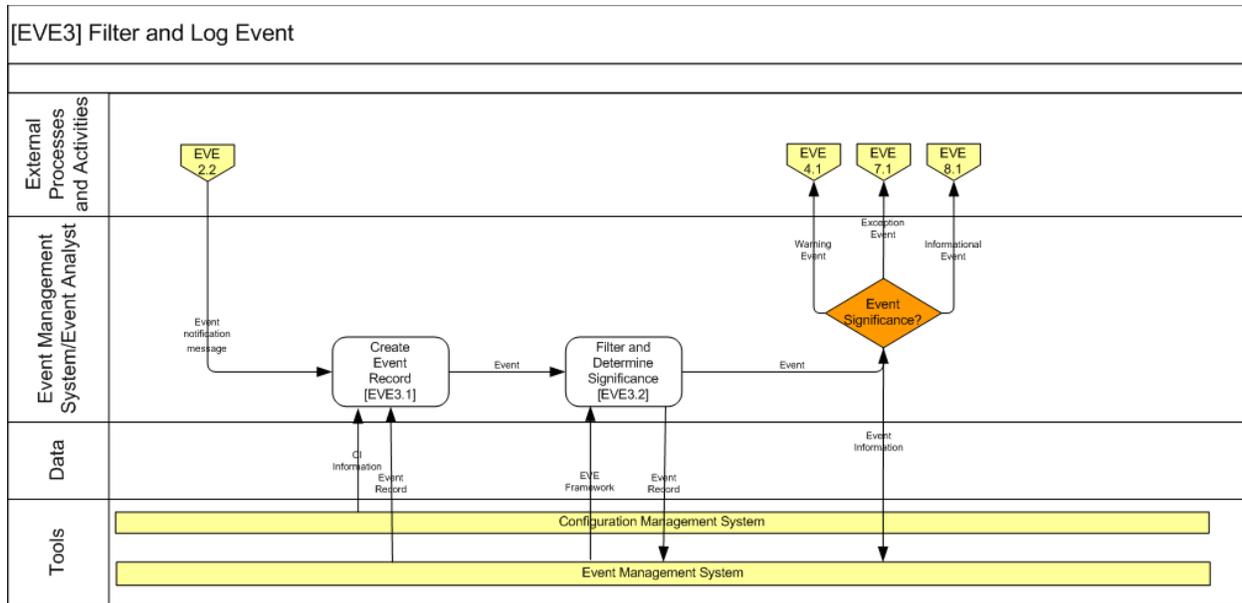


Figure 9 - EVE3 Workflow

3.6.3.1 TASKS

- Create Event Record
- Filter and Determine Significance

3.6.4 [EVE4] Correlate Event

This activity describes the tasks involved in reviewing service requests. The predefined mission goals are applied to warning events to determine what actions are required. Events are correlated by the EMS to determine commonalities and appropriate response action. This activity correlates multiple events, which throttles processing of repeated events, and at the same time, it eliminates duplicate events.

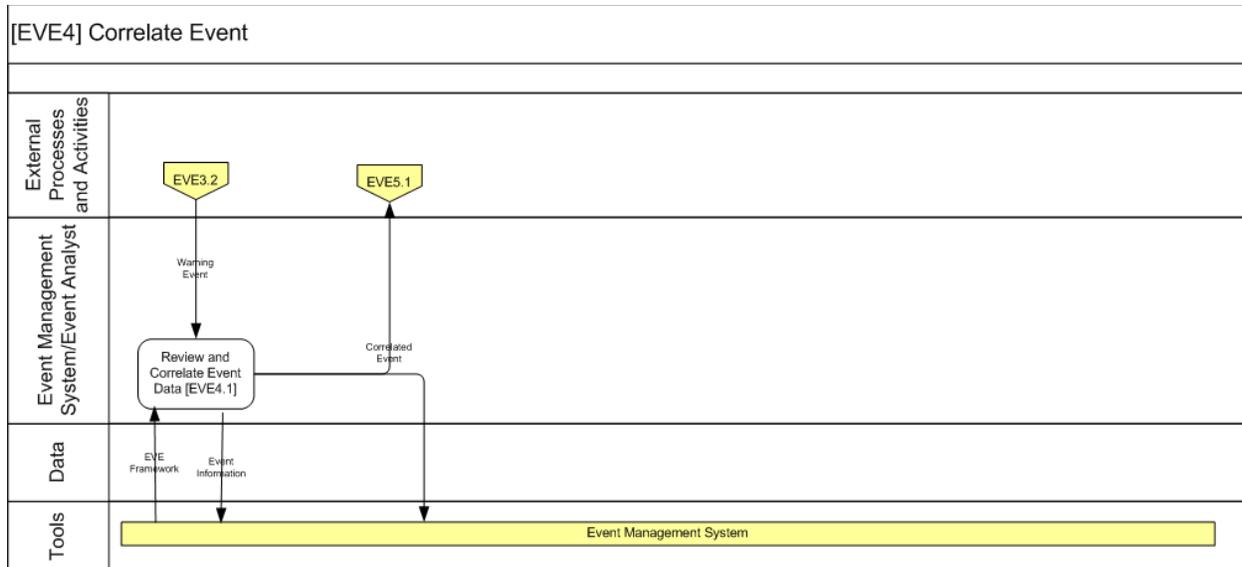


Figure 10 - EVE4 Workflow

3.6.4.1 TASKS

- Review and Correlate Event Data

3.6.5 [EVE5] Trigger Response

In this activity, after a warning event is detected, filtered and correlated, the appropriate and specific event notification / response activities are initiated. The response includes forwarding for an alert to be generated in the case of exception events, or forwarding the event for automated recovery. The criticality of the event is assessed to determine if escalation path should be taken.

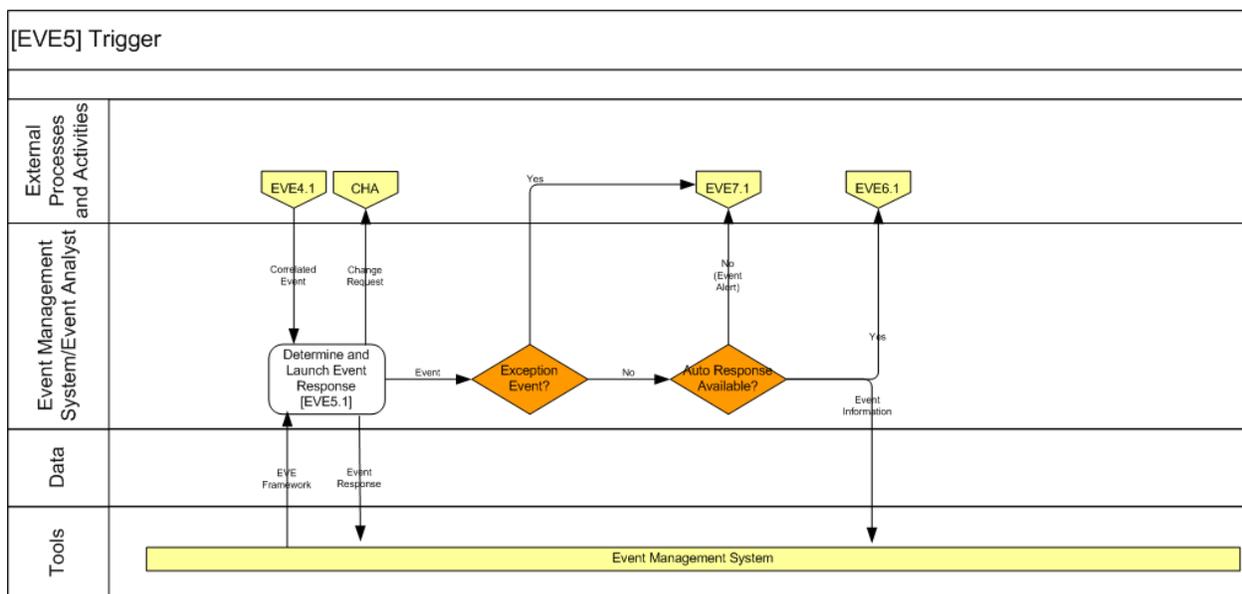


Figure 11 - EVE5 Workflow

3.6.5.1 TASKS

- Determine and Launch Event Response

3.6.6 [EVE6] Execute Auto Response

In this activity, pre-defined automated response is initiated by the EMS (e.g. rebooting and/or restarting a device, initiating a batch job, etc.). These responses do not require human intervention.

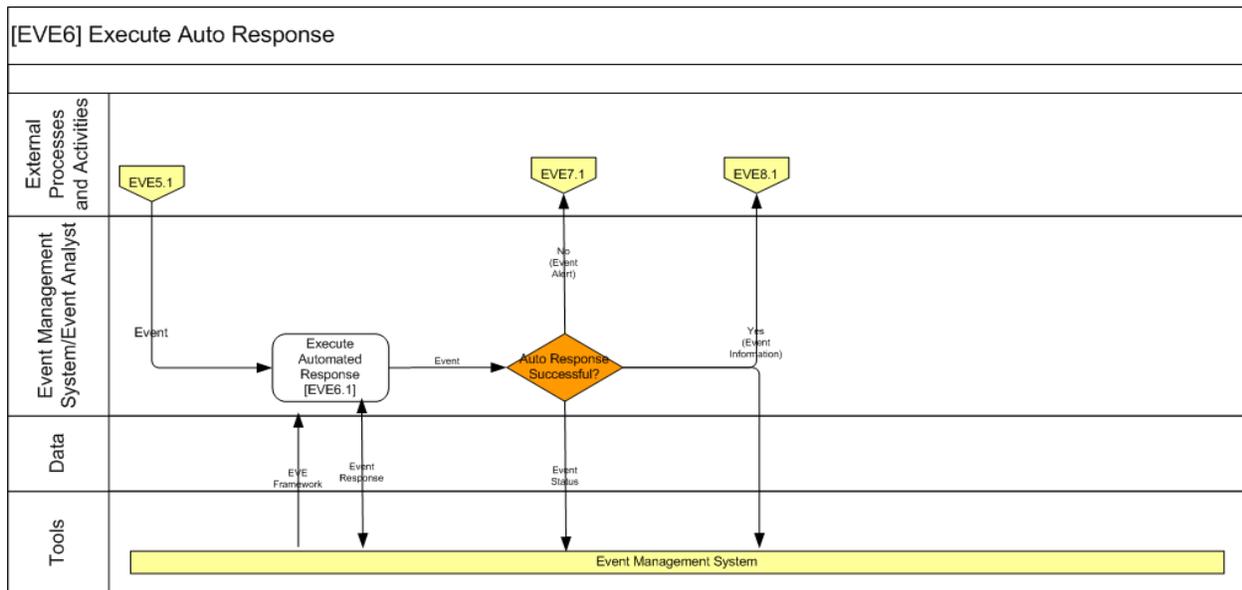


Figure 12 - EVE6 Workflow

3.6.6.1 TASKS

- Execute Automated Response

3.6.7 [EVE7] Generate Alert

This activity identifies those events requiring human intervention and provides necessary information to determine appropriate action to be taken. Additionally, this activity transmits the event information to Incident Management, which manages routing / escalation to the proper level for resolution.

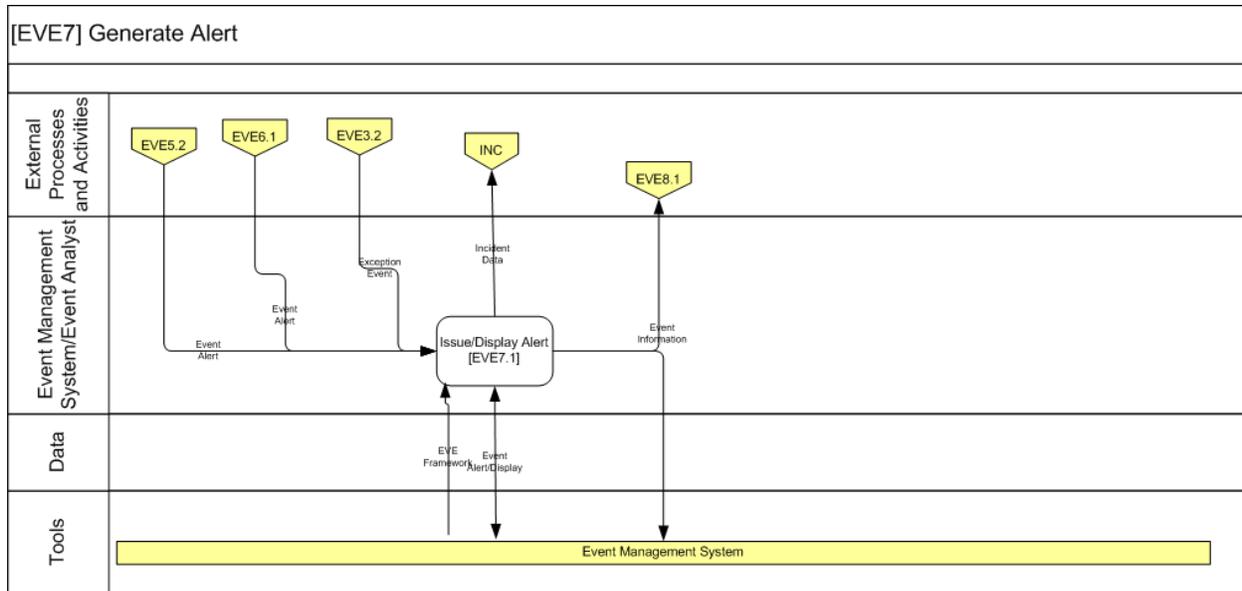


Figure 13 - EVE7 Workflow

3.6.7.1 TASKS

- Issue/Display Alert

3.6.8 [EVE8] Close Event Record

In this activity, the status of the event is confirmed as cleared and appropriate updating of event records is made.

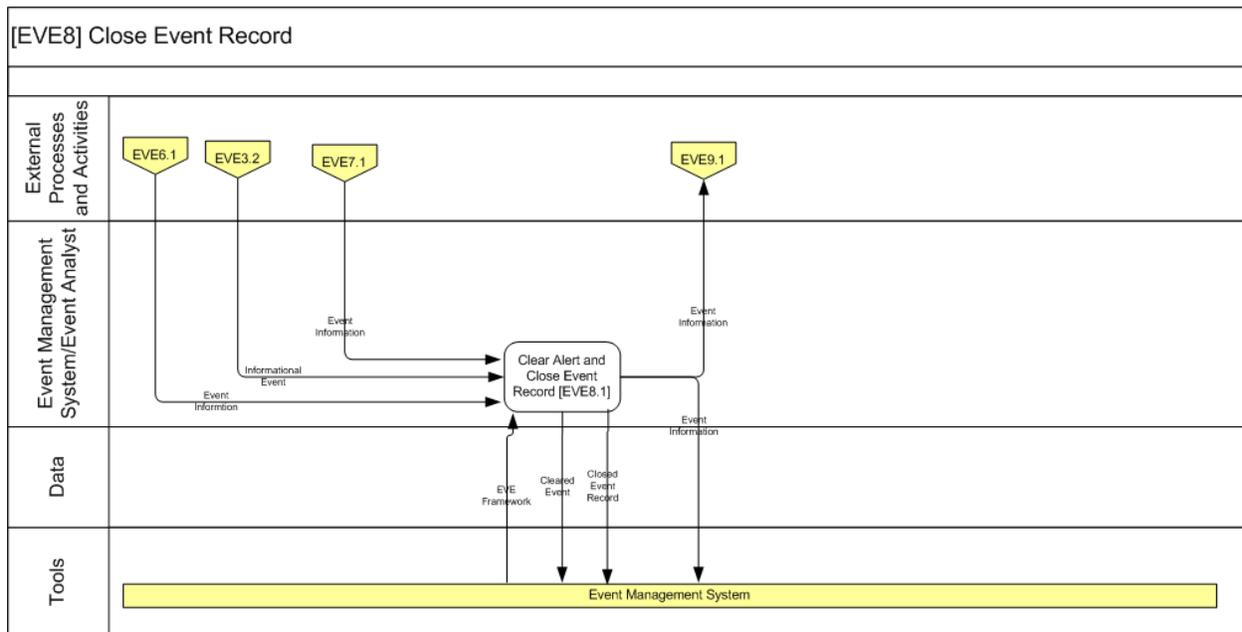


Figure 14 - EVE8 Workflow

3.6.8.1 TYPICAL TASKS

- Clear Alert and Close Event Record

3.6.9 [EVE9] Monitor, Manage and Report Event Management

In this activity, all Event Management activity is monitored to determine whether suitable progress is being made. Unsatisfactory results are reported and may result in actions taken to address any issues.

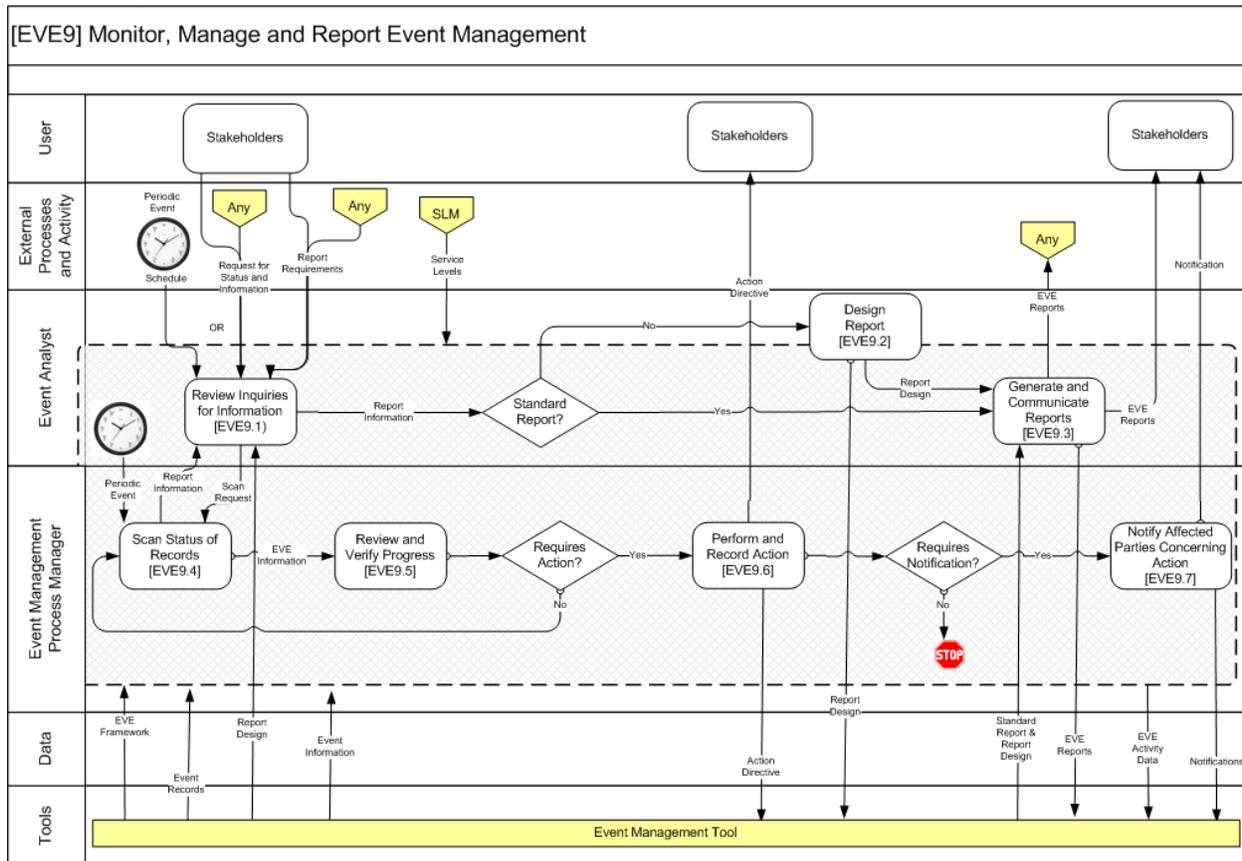


Figure 15 - EVE9 Workflow

3.6.9.1 TASKS

- Review Inquiries for Information
- Design Report
- Generate and Communicate Reports
- Scan Status of Records
- Review and Verify Progress
- Perform and Record Action
- Notify Affected Parties Concerning Action

3.6.10 [EVE10] Evaluate Event Management Performance

This activity describes the tasks involved in providing ongoing assessment and management of the Event Management process. Performance evaluation of the Event Management process assists in identification of improvement areas for the overall process (e.g., the foundation and interfaces of the process, activities, and accomplishments, degree of automation, and roles and responsibilities). The evaluation of process performance is achieved by identifying suggested improvements to the process, determining how to improve the quality of information received, and analyzing stakeholder needs.

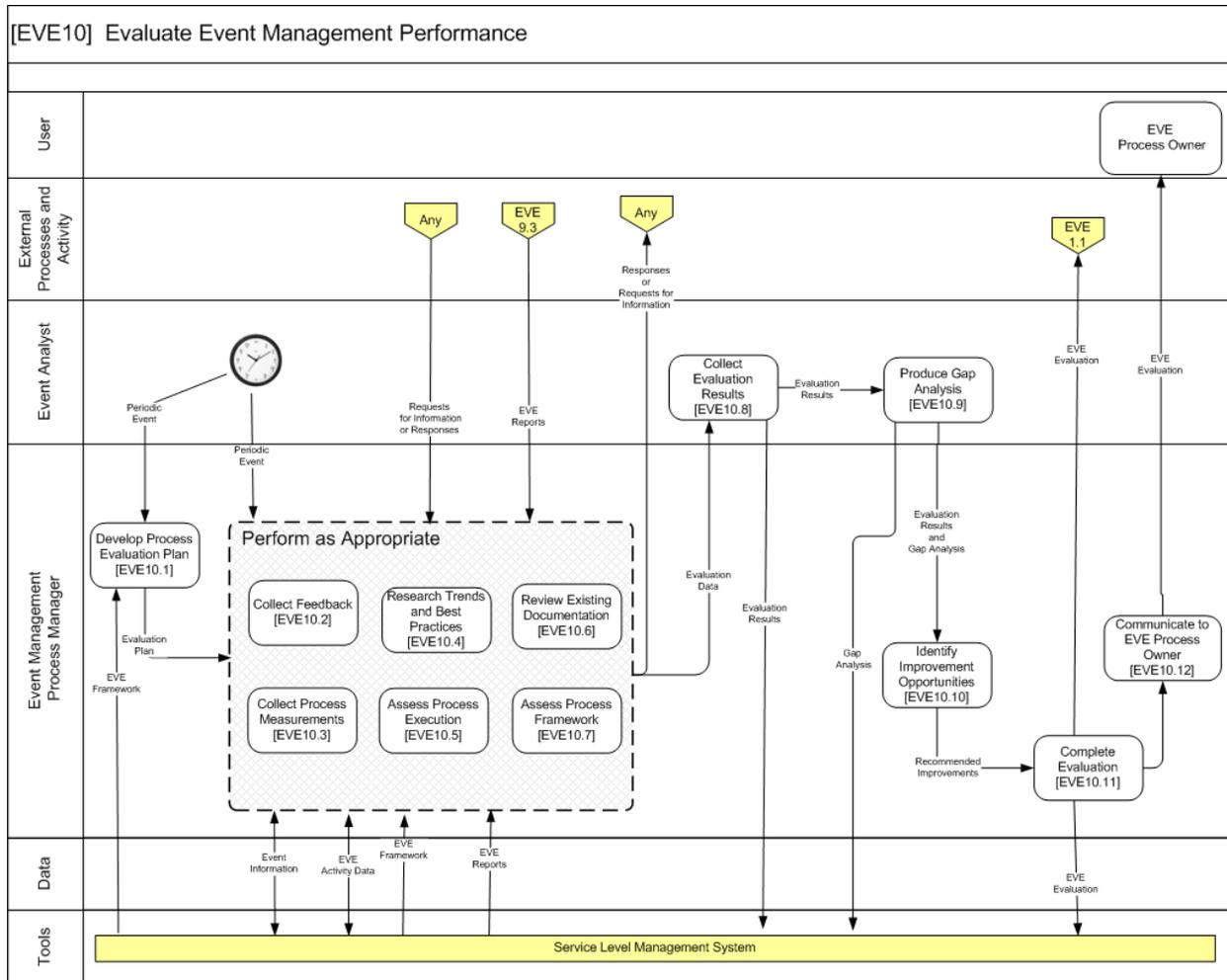


Figure 16 - EVE10 Workflow

3.6.10.1 TASKS

- Develop Process Evaluation Plan
- Collect Feedback
- Collect Process Measurements
- Research Trends and Best Practices
- Assess Process Execution

- Review Existing Documentation
- Assess Process Framework
- Collect Evaluation Results
- Produce Gap Analysis
- Identify Improvement Opportunities
 - Complete Evaluation
 - Communicate to EVE Process Owner

3.7 Roles

Role Name	Brief Role Description and Responsibilities
Event Management Process Owner	The strategic role accountable for the process. The Event Management Process Owner is accountable for the proper design, execution, and improvement of the process. This individual ensures that the process is being carried out, but does not run the day-to-day operation of the process. The Event Management Process Owner receives regular updates concerning the performance of the process and represents this process concerning all decisions.
Event Manager	This tactical role performs the day-to-day operational and managerial tasks demanded by the process activities and is responsible for coordination across processes, primarily responsible for the overall quality of the Event Management process.
Event Management System	Generates and correlates events and provides overall automation support for events.
Event Analyst	This role is the technical subject matter expert responsible for assessing, planning and monitoring Event Management supporting tools (e.g. network infrastructure monitoring tools).

Table 2 - Event Management Roles

Activity	Event Management Process Owner	Event Manager	Event Analyst
[EVE1] Establish Event Management Framework	A	R	R
[EVE2] Detect and Log Event	A	R	R
[EVE3] Filter Event	A	R	R
[EVE4] Correlate Event	A	R	R
[EVE5] Trigger Response	A	R	R

Activity	Event Management Process Owner	Event Manager	Event Analyst
[EVE6] Execute Auto Response	A	R	R
[EVE7] Generate Alert	A	R	R
[EVE8] Close Event Record	A	R	I/C
[EVE9] Monitor, Manage, and Communicate Event Management	A	R	R/C/I
[EVE10] Evaluate Event Management Performance	A	R	C/I

Table 3 - Event Management RACI

3.8 Information Work Products

The work products indicated in the process workflows include:

- Action Directive
- Change Request
- CI Information
- Cleared Event
- Closed Event Record
- Correlated Event
- EVE Activity Data
- EVE Evaluation
- Evaluation Data
- Evaluation Plan
- Evaluation Results
- Gap Analysis
- Recommended Improvements
- EVE Framework
- EVE Technology Plans
- Inter-Process Relationships
- Policies, Standards and Models
- EVE Reports
- Event
- Event Alert
- Event Alert/Display

- Event Information
- Event Notification Message
- Event Record
- Event Records
- Event Response
- Event Status
- Exception Event
- Incident Data
- Informational Event
- Input
- Message Standard Format
- Notification
- Notifications
- Periodic Event
- Process Information
- Process Specifications
- Report Design
- Report Information
- Report Requirements
- Request for Status and Information
- Requests for Information or Responses
- Responses or Requests for Information
- Scan Request
- Service Levels
- Standard Report and Report Design
- Warning Event

3.9 Performance Metrics

TBD

3.10 Organizational RACI

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
EVE	Event Management		NNWC			A					
EVE1	Establish Event Management Framework	Developing Method to Coordinate Agenda for Service Operations Format for EVE Framework Change Proposals Define Process for EVE Framework Changes SOP for EVE Other PO Appendices in EVE SOP Process Meetings	NNWC			R	I				
EVE2	Detect and Log Event		NNWC			R		R	R		

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
EVE3	Filter Event		NNWC			R		R	R		
EVE4	Correlate Event		NNWC			R		R	R		
EVE5	Trigger Response		NNWC			R		R	R		
EVE6	Execute Auto Response		NNWC			R		R	R		
EVE7	Generate Alert		NNWC			R		R	R		
EVE8	Close Event Record		NNWC				R	R			
EVE9	Monitor, Manage, and Report Event Management		NNWC			R	I	R	R		
EVE10	Evaluate Event Management Performance		NNWC			R	R	R			

Table 4 – Event Management RACI Chart

4. INCIDENT MANAGEMENT [INC]

4.1 Purpose

The primary goal of the INC process is to restore normal service operation as quickly as possible to minimize the adverse impact on mission operations, thus ensuring that the best possible levels of service quality and availability are maintained. An Incident is defined as an unplanned service disruption or degradation. “Normal service operation” is defined here as service operation within Service Level Agreement (SLA) limits. The Service Level Management process oversees SLAs, and as such, is a major stakeholder (contributor or supporter) of the policies identified within the document. Another major stakeholder of the identified policies is the Service Desk.

4.2 Policies

- Commanders Critical Information Requirement (CCIR)
- Chairman of the Joint Chiefs Manual (CJCSM) 6510.01a
- This process is governed by the terms and conditions of the CoSC
- Global Network Operations and Security Center (GNOSC) Incident Management SOP
- Secretary of the Navy Instruction (SECNAVINST) 5239.19

4.3 Outcomes

There are several qualitative and quantitative benefits that can be achieved by implementing an effective and efficient INC process. The value of INC is to provide:

- Following interruptions, IT Infrastructure services are rapidly restored
- IT service availability is sustained at a high level
- Known workarounds to resolve similar service interruptions are accessible to appropriate personnel
- Potential improvements to services are identified
- Incidents are recorded, categorized, prioritized and analyzed for resolution and closure
- Incidents which are in danger of breaching agreed service levels are escalated
- Information regarding the status and progress of reported incidents or service requests is communicated to affected parties

4.4 Scope

The scope of the Incident Management Process is to define a “best practices” approach to manage incidents from identification through closure. These standards must be applied across supporting timely response and coordinated restoration of services. The management of the lifecycle of incidents (i.e., receipt, logging, acknowledgement, classification, response, tracking and reporting) for all components involved in the IT service is included.

4.4.1 Includes

- Incidents reported by users or discovered within the IT organization by automation or people
- Determining how incidents will be identified, documented and processed from first notification to final resolution
- Identifying potential channels from which an incident may be reported
- Establishing a consistent Prioritization model and associated escalation procedure to define incident priority based on situational urgency and operational impact

- Defining the criteria for a major incident and how the processing will differ from normal
- Identifying functional and hierarchical escalation triggers and procedures
- Defining Incident Management Key Performance Indicators/Critical Success Factors
- Identifying the roles and responsibilities of stakeholders involved in the Incident Management process
- Handling (automatically or with human assistance) of system events that have been identified as incidents by the Event Management process
- Creation of workarounds
- Implementing workarounds (with Change Management, where required by the change policy)
- Participation involving several processes working in conjunction for handling 'major incidents'
- While service restoration has the highest priority, consideration has to be made of the risk that a workaround could exacerbate the original incident. For example, certain virus infections might spread beyond their initial scope if a simple service restoration is put into effect.

4.4.2 Excludes

- Monitoring
- Responding to business-as-usual perturbations in the running of services (Event Management)
- Service Request activities are not covered and will be addressed by the Request Fulfillment Process Design Team
- IT Resilience – ensuring the continued readiness and integrity of the IT services (Resilience category processes)
- The Service Desk Function, while intimately related to Incident Management, is out of scope for INC process development activities. The Service Desk will leverage the INC process in further defining its own roles, responsibilities, processes and procedures. The Service Desk functional owner is considered an essential stakeholder, and will be directly involved in the continued development of the INC process once identified.

4.5 Process Interfaces

Primary interfaces with other processes include the following:

- IT Asset Management provides asset related information that pertains to an incident. If an asset needs updating due to an incident, INC will provide the needed updates to IT Asset Management.

- Event Management passes event information to INC for escalation. Incident Management then provides updated incident information back to Event Management.
- During the resolution of an incident, Incident Management may send a service request to Request Fulfillment. Examples include providing access to a user or resetting a password.
- Facilities-related incidents are routed to INC. INC is responsible for addressing the incident. However, roles within Facilities Management may be used to troubleshoot and resolve facility related incidents.
- Problem Management identifies known errors within the IT infrastructure. INC provides incident information that is used to identify incident trends, which may indicate a problem. In addition, INC provides details, history, and classification of incidents to be used as an input for determining known errors, validation that incidents have not recurred for known errors that have been resolved, and actions taken or workarounds used to resolve incidents. Conversely, problems and known errors are referred to by INC when responding to new incidents.
- The resolution of an incident may require a Request for Change (RFC) to be submitted to Change Management for approval. Change Management provides the status of RFCs submitted to resolve incidents and the Projected Service Availability (PSAs) to determine impact on incidents. Incident Management provides validation that incidents have not recurred for Known Errors that have been resolved via Change Management.
- Release and Deployment Management provides the link of releases to incidents being impacted/solved and training for new incident handling skills and processes related to new or changed releases impacting implementation. INC provides incident history and detail to be used as input for determining development solutions, incident history and detail for incidents related to implementation of releases and identification of incidents caused by Release and Deployment Management activities if they occur.
- Configuration Management provides information about CIs related to an incident. During resolution of an incident, information about related CIs are updated by Configuration Management.

Incidents may be reported by a variety of processes, including:

- Access Management
- Change Management
- Data Management

- Event Management
- Facilities Management
- Configuration Management
- IT Asset Management
- Release and Deployment Management
- Request Fulfillment
- Information Security Management
- Service Validation and Testing
- Transition Planning and Support

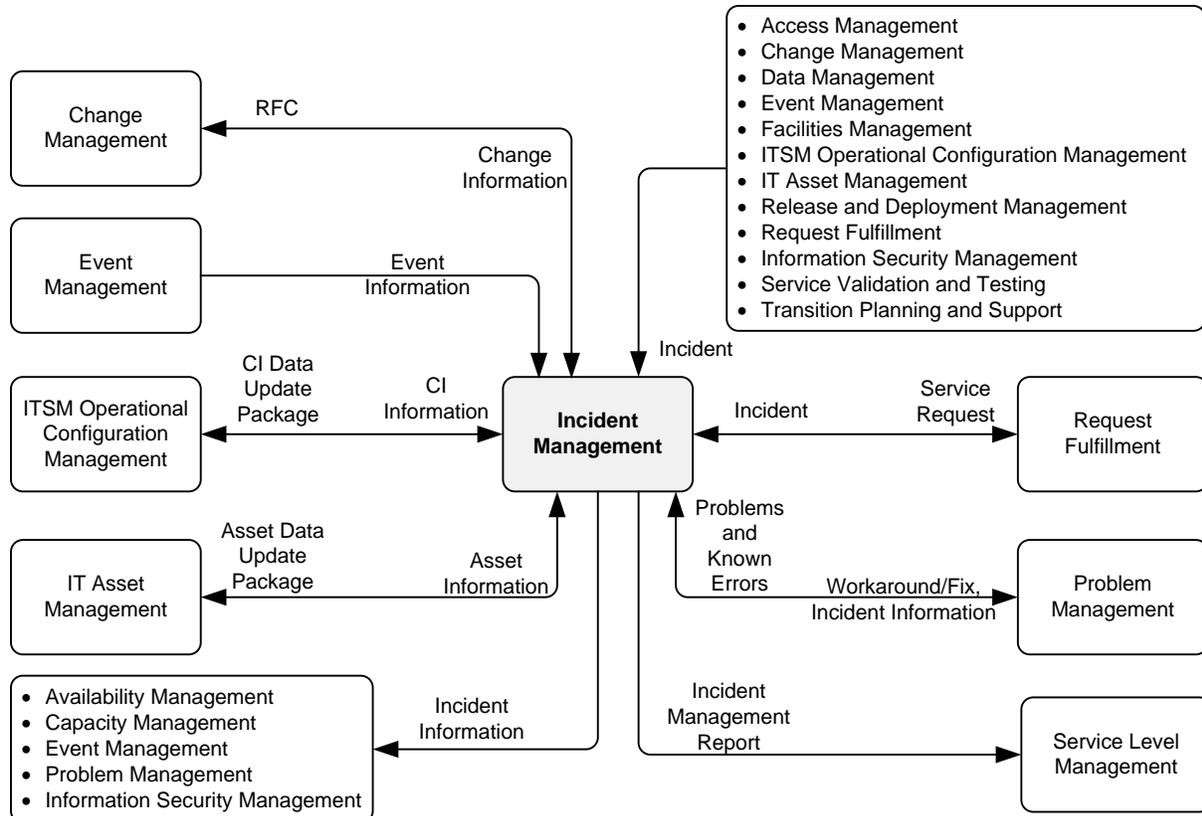
Incident information is used by a variety of processes, including:

- Availability Management – INC provides incident history and detail when requested; metrics on Mean Time To Response (MTTR) actions; actions taken to restore service to customers when requested; and satisfaction feedback from customers on incidents and overall service quality
- Capacity Management – INC provides incident history and detail when requested; satisfaction feedback from customers on capacity related incidents and overall satisfaction with performance and throughput quality
- Financial Management – INC provides cost impacts for restoring services and actions taken and assessment as to frequency that incidents will occur to identify longer term cost impacts
- Service Level Management uses INC reports to determine if SLA's fell within scope

This process is affected by the strategic direction described in the IT Strategy, generated by the Strategy Generation process.

This process provides content in the form of Knowledge Items to the Knowledge Management process. In addition, Knowledge Management organizes and processes that content into Knowledge Assets.

Compliance Management identifies specific Compliance Plans and Controls that should be adhered to by this process to meet standards and regulations that should be complied with. In return, this process provides an evaluation of how those standards and regulations were complied with.



Note: This diagram does not show the following interfaces to all processes:

- IT Strategy sent from Strategy Generation process
- Compliance Plans and Controls from Compliance Management process
- Knowledge Assets from Knowledge Management process

In addition, this diagram does not show the following interface to Knowledge Management from all processes:

- Knowledge Items sent to the Knowledge Management process

Figure 17 - Incident Management Interfaces

4.6 Activity-Level Workflow

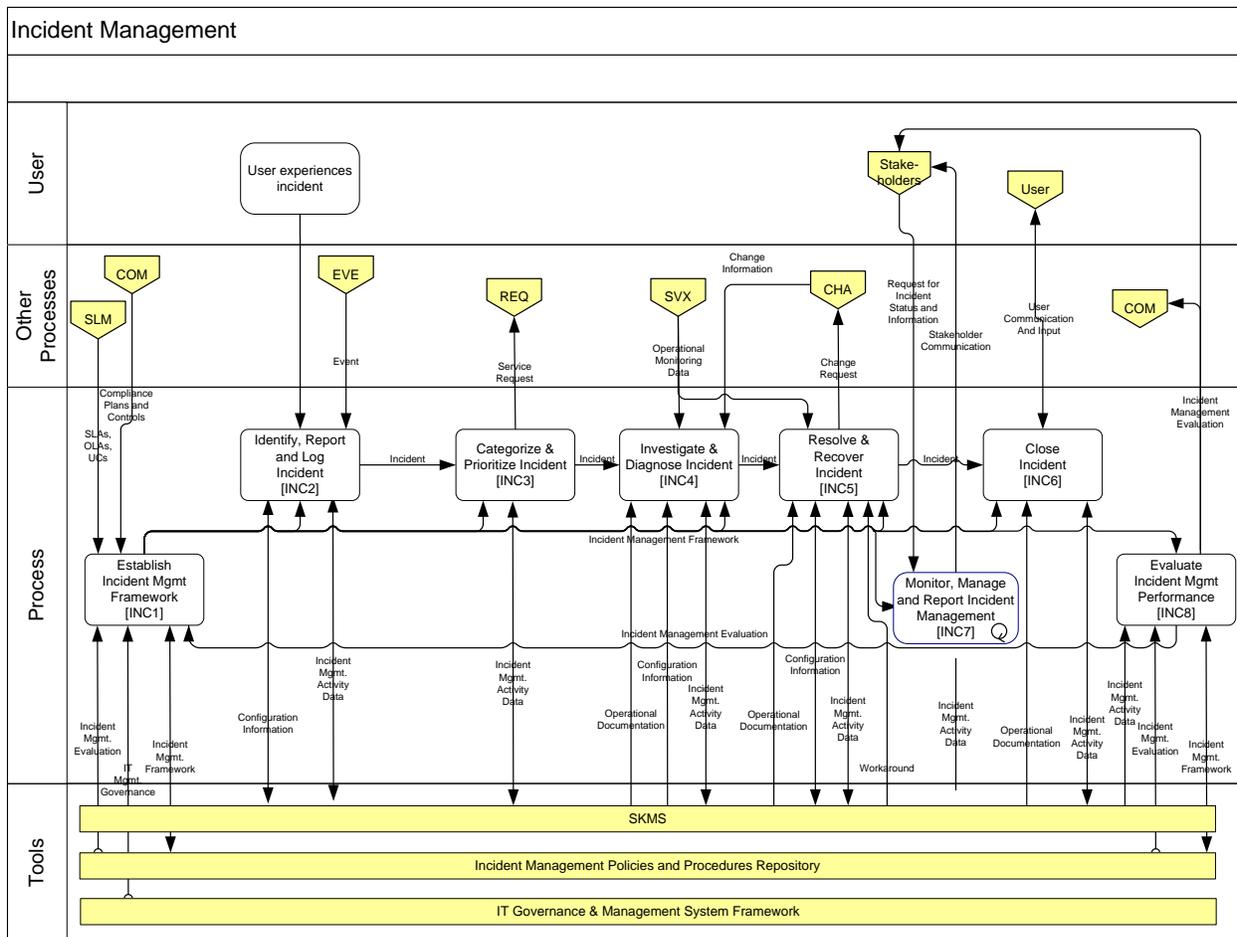


Figure 18 - Incident Management Workflow

4.7 Activities

4.7.1 [INC1] Establish Incident Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the “process framework” and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for making changes and improvements to the process framework. The process framework is a collection of information, not necessarily a single document, which includes:

- Process purpose, scope, goals, and capabilities
- Process policies, standards, and conceptual models
- Process data requirements
- Role responsibilities
- Organizational responsibilities
- Detailed procedures and best practices, including, but not limited to:

- Incident classification scheme
- Incident prioritization scheme
- Incident resolution procedures
- Incident handling scripts
- Standard practices for contacting users
- Interfaces with other processes and programs
- Measurements and controls
- Tool requirements

4.7.1.1 TASKS

- Review Process Evaluation Recommendations
- Specify Process Purpose, Scope, Goals, and Capabilities
- Define Process Policies, Standards, and Conceptual Models
- Determine Process Data Requirements
- Identify Process Roles and Responsibilities
- Assign Process Responsibilities to Organizations
- Determine Process Procedures
- Determine Process Relationships to Other Processes
- Define Measurements and Controls
- Determine Technology Needs
- Create Project Proposals
- Communicate and Deploy Framework

4.7.2 *[INC2] Identify, Report and Log Incident*

In this activity, an incident is identified and reported by the Requestor and is logged by the Service Desk. The incident is logged into the Incident Management System resulting in creation of an incident record.

4.7.2.1 TASKS

- Detect or Acknowledge Incident
- Create Incident Record
- Update Existing Record
- Record Basic Incident Information
- Send Outage Notification

4.7.2.2 DECISION TIMELINES

The headings in these tables are described in more detail in Appendix A.

Process Points	Decision	Timeline	Authority	Tools
	HP makes decision to elevate to Govt.	RtOP at 20 minutes (no associated KPP) with follow up every 90 minutes.	CCIRs and CoSC,	SM7; email; phone
	HP makes decision to elevate to Govt.	Remediation report/advisory every 30 minutes	Best practice	Email; SM7

4.7.2.3 GAPS

Process Points	Description	Severity	Mitigation	Tools
Incidents meeting CCIR/Severity 1 criteria achieved CCIR/Severity 1 timelines- Negotiate wording to specify the requirement to be acceptable to both HP and govt.	Time of receipt spreadsheet	BWC	Monthly	CCIR Tracker on portal; SM7 (?)

4.7.2.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools
Incident Management	NCDOC Ticketing System, ENMS Ticketing System, CCIR, Verbal Report	Information Security Management feeds Incident Management		Remedy, CCIR

Process Points	Process	Interface	Return/Terminate	Tools
Event Management	Occurs with HP to HP's internal event mgmt team (internal HP process)	Events may be escalated to incidents		NetCool handshake to SM7; SSIM
Event Management	Occurs internal to Government event mgmt team (internal Government process)	Coordination point		NetCool handshake to SM7
Event Management	Naval message to NetOps to Remedy as a change ticket	Investigate and remediate		Remedy, Naval Message, Phone, email

4.7.2.5 LOCATION

N/A

4.7.2.6 MEETINGS

N/A

4.7.2.7 METRICS

Process Points	Metric	Format	Access Point(s)	Tools
Incidents meeting CCIR/Severity 1 criteria achieved CCIR/Severity 1 timelines	Time of receipt spreadsheet	BWC	Monthly	CCIR Tracker on portal; SM7 (?)

CND incidents 1, 2, 4, 7 on MAC Level 1 and 2 systems would trip OPREP 3 reporting	Time of receipt spreadsheet	NCDOC Watch Officer	Monthly	SM7
Percentage of Incidents reported appropriately (CCIR incidents that are actually reported)	Occurrence spreadsheet	BWC	Monthly	Local tracker

4.7.2.8 ORGANIZATIONS

- Operations Control (HPES)
- Battle Watch Captain (BWC) [NNWC]
- Regional Network Operations and Security Center (RNOSC) JFTOC
- NCDOC

4.7.2.9 POLICIES

- GNOSC Incident Management SOP
- CJCSM 6510.01a
- SECNAVINST 5239.19
- CoSC

4.7.2.10 WORK PRODUCTS

The Response to Operational Problems (RtOP) Report is created once, within 20 minutes of incident logging. It is distributed to the RtOP distribution using email/SM7.

The Remediation Advisory is created every 30 minutes for severity 1 RtOP reports. It is distributed to the Advisory Distribution using email/SM7.

4.7.3 [INC3] Categorize and Prioritize Incident

In this activity, an incident is categorized and prioritized. An incident is categorized based on the systems, applications, service / segment affected or the requestor’s mission supporting role. An incident is prioritized based on urgency and impact. The record is assigned to an analyst for diagnosis and investigation. If the incident is categorized as a request for service, it is transferred to the Request Fulfillment process as a Service Request. Incidents exceeding a defined threshold

of impact and urgency are categorized as Major Incidents and the appropriate procedure is invoked.

4.7.3.1 TASKS

- Assign Incident Owner
- Search for Matching Incidents
- Categorize Incident
- Define Incident Impact
- Assign Incident Priority
- Initiate Major Incident Response
- Reconcile Duplicate Incidents
- Pass Non-Incident Records to Request Fulfillment

4.7.4 [INC4] Investigate and Diagnose Incident

In this activity, incidents and all data associated are accessed to identify appropriate responses and actions, and to formulate Incident Resolution Plans. Actions may include identifying workarounds, reclassifying the incident based on further analysis, and updating Incident records.

4.7.4.1 TYPICAL TASKS

- Create Incident Resolution Plan
- Reclassify and Escalate Incident
- Gather Additional Information and Investigate
- Obtain Workarounds or Fixes
- Create Workaround or Fix
- Apply Workaround or Fix

4.7.4.2 DECISION TIMELINES

N/A

4.7.4.3 GAPS

Process Points	Description	Severity	Mitigation	Tools	Tool Requirements
	ENMS ticket interface into SM7	Minor	Phone and email	long term	ENMS, SM7

4.7.4.4 INTERFACES

N/A

4.7.4.5 LOCATION

N/A

4.7.4.6 MEETINGS

N/A

4.7.4.7 METRICS

Process Points	Metric	Format	Access Point(s)	Frequency	Tools
	# times the incident ticket needs to be is reprioritized	Occurrence spreadsheet	BWC	Monthly	Local tracker

4.7.4.8 ORGANIZATIONS

Position	Organization	Name	Contact Data	Tools	Tool Requirements
BWC	NNWC	n/a		email; phone	
RNOSC BWC	RNOSCs			email; phone	
	NCDOC				

4.7.4.9 POLICIES

N/A

4.7.5 [INC5] Resolve and Recover Incident

In this activity, the actions necessary to resolve the incident and restore service are executed. Resolution and restorations may be in the form of existing workaround solutions or alternatively, raising a Change Request to affect a new solution. It also prompts any action necessary to

recover the service to agreed Service Level Agreements (SLA), Operational Level Agreements (OLA) and Underpinning Contracts (UC).

4.7.5.1 TYPICAL TASKS

- Monitor Resolution Through Closure
- Define Resolution Implementation Approach
- Perform Incident Resolution
- Provide Resolution Status Information
- Submit Change Request
- Communicate Resolution to Requestor
- Validate Service Recovery

4.7.6 [INC6] Close Incident

In this activity, ‘resolved’ incidents case histories are examined. This activity ensures that all required incident documentation is complete, including details of cause, expended effort for resolution and outcome. A review of the incident’s original classification against available root cause information is used to determine classification accuracy. In accordance with DON and related policy, this is the activity where INC obtains stakeholder agreement with resolution activity and status.

4.7.6.1 TYPICAL TASKS

- Complete and Validate Incident Information
- Reclassify Incident
- Close Incident Record
- Close Related Incidents
- Communicate Incident Closure to Requestor

4.7.6.2 DECISION TIMELINES

Process Points	Decision	Timeline	Authority	Tools	Tool Requirements
not specified	Significant change in status under the RtOP			SM7; email; phone	

4.7.6.3 GAPS

TBD

4.7.6.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools	Tool Requirements
	Event Management	Ticketing system, CCIR	Terminates an event	SM7, CCIR portal	
	Problem Management	Ticketing system, CCIR	May return incident resolution	SM7, CCIR portal	

4.7.6.5 LOCATION

Process points	Location	Seats	Seat Requirements	Timeline	Tools
	same as MMR above				

4.7.6.6 MEETINGS

N/A

4.7.6.7 METRICS

N/A

4.7.6.8 ORGANIZATIONS

Position	Organization	Name	Contact Data	Tools	Tool Requirements
GNOSC Watch Officer	GNOSC			email; phone	
BWC	NNWC			SM7; email; phone	
HP Operations	HPES			SM7; email; phone	
	NCDOC				

4.7.6.9 POLICIES

N/A

4.7.7 [INC7] Monitor, Manage and Report Incident Management

This activity involves the overall monitoring of work within the process and reporting on specific items or general status to stakeholders. The work in this activity involves the following:

- All process work is monitored to determine if incidents are being processed in an effective and timely manner
- If monitoring indicates issues with incident processing, actions may be carried out to resolve those issues
- Reports are generated, either upon request or at scheduled intervals, for stakeholders interested in specific work items or in the process as a whole

4.7.7.1 TYPICAL TASKS

- Scan and Identify Items of Interest
- Review Progress
- Verify Current Status
- Record and Perform Action
- Notify Concerning Action
- Analyze Request for Information
- Define and Build Report
- Generate and Communicate Report

4.7.7.2 DECISION TIMELINES

Process Points	Decision	Timeline	Authority	Tools	Tool Requirements
	not specified	when significant change as stated in CoSC	not specified	SM7; email; phone	

4.7.7.3 GAPS

Process Points	Description	Severity	Mitigation	Timeline	Tools
	Lack of sufficient licenses for tools	Critical	Phone and email	1-2 months	SM7

4.7.7.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools	Tool Requirements
	Problem Management	Reports as made available	Follow and coordinate	email, SM7	

4.7.7.5 LOCATION

Process points	Location	Seats	Seat Requirements	Timeline	Tools
	Co-Located	3 seats in secure area at Pearl NOC	NIPR, SIPR, same set-up as current watch	3/24/2011	ENMS, SM7,
	Co-Located	5 seats in secure area at Norfolk NOC	NIPR, SIPR, same set-up as current watch	3/25/2011	ENMS, SM7,
	Co-Located	2 seats at GNOSC Jeb Little Creek	NIPR, SIPR, same set-up as current watch	already available	SM7

4.7.7.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Lifespan	Tools
	Major incident coordination and SA	Combined	NetOps leadership leads, HP operations control, TYCOM leadership, program office, RNOSC	as-needed	DCO, phone bridge, VTC

4.7.7.7 METRICS

N/A

4.7.7.8 ORGANIZATIONS

Position	Org	Name	Contact Data	Tools	Tool Requirements
Operations Control	HPES			SM7; email; phone	
RNOSC BWC	RNOSCs			SM7; email; phone	
BWC	NNWC			SM7; email; phone	
RNOSC BWC	RNOSCs			SM7; email; phone	
	NCDOC				

4.7.7.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
KCS		KCS		KCS portal	
CCIR, CoSC		Microsoft SharePoint portal		Microsoft SharePoint portal	

4.7.8 [INC8] Evaluate Incident Management Performance

The purpose of this activity is to evaluate the performance of the Incident Management process activities against defined performance criteria and measures, and to provide input to the IT Management System. All analysis is used to create an Incident Management Evaluation. This will be a key input when updating the Incident Management Framework.

4.7.8.1 TYPICAL TASKS

- Collect Feedback
- Produce Process Measurements
- Research Trends and Best Practices
- Review Existing Documentation
- Assess Process Execution
- Audit Process
- Assess Process Framework
- Collect Evaluation Results
- Produce Gap Analysis
- Recommend Initiatives
- Complete Evaluation
 - Communicate to Stakeholders

4.7.8.2 DECISION TIMELINES

N/A

4.7.8.3 GAPS

N/A

4.7.8.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools	Tool Requirements
Major incidents lessons learned	Report	Incident Management Process Owner and Manager		SM7 (to reconstruct history)	

4.7.8.5 LOCATION

N/A

4.7.8.6 MEETINGS

N/A

4.7.8.7 METRICS

N/A

4.7.8.8 ORGANIZATIONS

N/A

4.7.8.9 POLICIES

N/A

4.8 Roles

Role Name	Brief Role Description and Responsibilities
Incident Management Process Owner	<p>The Incident Management Process Owner is the sponsor of the process, and holds the responsibility and executive authority for the overall process results across the enterprise. This authority spans across all internal and external organizations who participate in the process.</p> <p>The Incident Management Process Owner is responsible for ensuring that the Incident Management process is fit-for-purpose and that all activities defined within the process are undertaken. This responsibility includes oversight of process quality, continual improvement, and compliance with organizational mandates and performance targets.</p> <p>The Incident Management Process Owner is vested with ultimate authority over all aspects of Incident Management process design, change management, performance metrics, policies, and process automation technologies to ensure compliance with organizational objectives.</p> <p>Carries out the Process Owner responsibilities for the INC process</p>

Role Name	Brief Role Description and Responsibilities
Incident Manager	<p>The Incident Manager is responsible for the quality and integrity of the Incident Management process. The Incident Manager is the interface to the other process managers. The Incident Manager is responsible for all aspects of the day-to-day operational management of the process. This includes planning and coordinating all the activities required to perform, monitor, and report on incident resolution. The Incident Manager enables communication of preventative actions and best practices to improve service levels.</p> <p>The Incident Manager may delegate authority to other managers or to process administrators, for example assigning regional Queue Managers or IT Service Continuity Managers. However, the Incident Manager is the single authority and point of accountability for all issues relating to the operational management of the process across the enterprise. The Incident Manager's responsibilities include ensuring post-review of critical priority incidents; chairing the incident and problem review meetings, following defined escalation path when needed, as defined in the escalation policy, notifying the participants in the INC process when standards and procedures are not being followed. The Incident Manager is also responsible for re-routing misdirected incidents that have not been handled in a timely manner, responding to the Incident Analysts regarding escalation issues in a timely and appropriate fashion, identifying incidents which need special attention or escalation; managing major incidents and executes the Incident Manager responsibilities for the Incident Management process.</p> <p>Responsibilities include:</p> <ul style="list-style-type: none"> Ensuring post-review of priority 1 incidents Chairing the incident and problem review meetings Following defined escalation path when needed, as defined in the escalation policy Notifying the participants in the Incident Management process when standards and procedures are not being followed Rerouting misdirected incidents that have not been handled in a timely manner Responding to the Incident Analysts regarding escalation issues in a timely and appropriate fashion Identifying incidents which need special attention or escalation Managing major incidents Carries out the Process Manager responsibilities for the INC process
Incident Management Administrator	<p>The Incident Management Administrator supports the Incident Manager by managing new and existing incidents in the INC queue. This role is also responsible for analyzing incidents for correlation and status tracking. Incidents requiring action are identified and communicated accordingly; this may include escalation and user communications. The Incident Management Administrator is also responsible for generating and communicating process-related reports and identifying CSI opportunities within the Incident Management process.</p> <p>Carries out Process Administrator responsibilities for Incident Management</p>

Role Name	Brief Role Description and Responsibilities
Incident Analyst	<p>The Incident Analyst, being in most instances the second line (or higher) support professional, is the subject matter expert of one or more competency domain(s). This role is responsible for quickly providing an accurate analysis of an incident and/or a solution to it in order to restore the disturbed service as soon as possible. Request Fulfillment typically assigns incidents to the Incident Analyst. The Incident analyst will determine what is required to restore the service and initiate the appropriate action. The Incident Analyst's responsibilities include performing incident determination; creating a workaround and Executing a workaround, if applicable; initiating a change request; installing a permanent fix for the incident and executing a resolution, if applicable. Additional responsibilities are updating the incident reporting system with resolution information, providing effective resolution to the incident in accordance with the priority service level, updating the closure portion of the ticket and identifying resolved incidents as candidates for inclusion in the operational documentation.</p> <p>Responsibilities include:</p> <ul style="list-style-type: none">Performing incident determinationCreating a workaroundInitiating a change requestExecuting a workaround, if applicableInstalling a permanent fix for the incidentExecuting a resolution, if applicableUpdating the incident reporting system with resolution informationProviding effective resolution to the incident in accordance with the priority service levelUpdating the closure portion of the ticketIdentifying resolved incidents as candidates for inclusion in the operational documentation

Role Name	Brief Role Description and Responsibilities
Requestor (also end user or other process technical staff)	<p>The Requestor submits requests to the IT organization. These requests may come in the form of an incident, a service request, a Change Request, a request for information, or some other type of request. The Requestor responsibilities includes utilizing IT services to perform business tasks, contacting the Service Desk for requests for Information, service requests, incidents and change requests. The Requestor provides information, as needed, for incidents submitted, problems related to incidents opened by the Requestor and change requests submitted. The Requestor ensures that a change request is complete with accurate information at a sufficient level of detail to implement the change. The Requestor works with the Change Manager to resolve any data inconsistencies with the request. The Requestor responds to all issues/concerns raised by the Approvers. The Requestor ensures all issues/concerns with each submitted request are resolved.</p> <p>Responsibilities include:</p> <ul style="list-style-type: none"> Utilizes IT services to perform business tasks Contacts the Service Desk for Requests for Information Service Requests Incidents change requests Provides information, as needed, for Incidents submitted Problems related to incidents opened by the Requestor Change requests submitted Ensures that a change request is complete with accurate information at a sufficient level of detail to implement the change Works with the Change Manager to resolve any data inconsistencies with the request Responds to all issues/concerns raised by the Approvers Ensures all issues/concerns with each submitted request are resolved
Service Provider	<p>Responsible for delivery of individual service.</p> <p>Responsibilities include:</p> <ul style="list-style-type: none"> Represents service as needed. Understands high level workings of service. Provides input to Major Incident reviews.
Supplier	<p>Responsible for delivery of third party services.</p> <p>Responsibilities include:</p> <ul style="list-style-type: none"> Supports service as needed. Understands high level workings of service. Provides input to Major Incident reviews

Table 5 - Incident Management Roles

Process Activity	Incident Management Process	Incident Manager	Incident Owner	Incident Management Analyst	Incident Analyst	Service Provider	Supplier	User
[INC1] Establish Incident Management Framework	A/C/I	R/C/I	C/I	C/I	C/I			
[INC2] Identify, Report and Log Incident	A/C/I	R/C/I	R/C/I	R/C/I	R/C/I			C/I
[INC3] Categorize and Prioritize Incident	A/C/I	R/C/I	R/C/I	R/C/I	R/C/I			
[INC4] Investigate and Diagnose Incident	A/C/I	R/C/I	R/C/I	R/C/I	R/C/I	C/I	C/I	
[INC5] Resolve and Recover Incident	A/C/I	R/C/I	R/C/I	R/C/I	R/C/I		C/I	C/I
[INC6] Close Incident	A/C/I	R/C/I	R/C/I	R/C/I	R/C/I			C/I
[INC7] Monitor, Manage and Report Incident Management	A/C/I	R/C/I	C/I	C/I	C/I			
[INC8] Evaluate Incident Management Performance	A/C/I	R/C/I	C/I	C/I	C/I		C/I	

Table 6 - Incident Management RACI

4.9 Information Work Products

TBD

4.10 Performance Metrics

- Incidents meeting CCIR/Sev 1 criteria achieved CCIR/Sev 1 timelines
- CND incidents 1, 2, 4, 7 on MAC Level 1 and 2 systems would trip OPREP 3 reporting
- Percentage of Incidents reported appropriately (CCIR incidents that are actually reported)
- Number of times the incident ticket needs to be is reprioritized

4.11 Organizational RACI

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
INC	Incident Management		NNWC			A					

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT	Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
INC1	Establish Incident Management Framework	Escalation to Government RtOP at 20 Minutes, no KPP, 90 Min follow-up Escalation to Government Remediation Report, Advisory every 30 Minutes Meetings: CCIR/SEV 1 Criteria, Timelines, Tracking Mechanism NCDOC Ticket System, ENMS, CCIR, Verbal, Remedy HP Event to HP Incident System, Government Event to Government Incident System	NNWC				R	R	I	I		
		System Naval Message to NetOps to	72									

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT	Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPA WAR	Tech Authority
INC2	Identify, Report and Log Incident	INC, NCDOC Ticketing System, ENMS Ticketing System, CCIR, Verbal Report, ISM feeds INC; EVE, Occurs with HP to HP's internal event mgt team, events may be escalated to incidents, NetCool to handshake to SM7/SSIM;	NNWC				R		R	R		
INC3	Categorize and Prioritize Incident		NNWC				R		R			
INC4	Investigate and Diagnose Incident	ENMS to SM7 Interface Metrics: # times incident ticket needs to be re prioritized per occurrence spreadsheet	NNWC						R	R		

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT	Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
INC5	Resolve and Recover Incident		NNWC					R	R			
INC6	Close Incident	Change in Status under RtOP, SM7, email, Phone	NNWC			R		R	R			

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT	Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
INC7	Monitor, Manage, and Report Incident Management	When significant change as stated in COSC. SM7, email, phone SM7 Tool Licenses SM7 Reports 3 Seats in secure location in Pearl Harbor NOC, NIPR, SIPR 5 Seats in secure location in Norfolk NOC, NIPR, SIPR 2 Seats at GNOSC JEB Little Creek, NIPR, SIPR Meetings: Major Incident Coordination SA, DCO, Phone Bridge,	NNWC				R	I	R	R		
		VTC KCS Portal and SharePoint	75									

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
INC8	Evaluate Incident Management Performance	Major Incidents lessons Learned	NNWC			R	R	R			

Table 7 – Incident Management RACI Chart

5. INFORMATION SECURITY MANAGEMENT [ISM]

5.1 Purpose

The purpose of the Information Security Management process, or interchangeably described as “ISM,” is to manage and operate security controls and protections over all related IT assets and services to ensure the Confidentiality, Integrity and Availability (CIA) of IT assets, data, information, and services. It includes activities to mitigate the risk posed by malicious threats, and to decrease vulnerabilities in the DON and IT services, systems and processes that would make it easier for such malicious threats to succeed. Furthermore, the Information Security Management process will manage and operate security protections over all related IT assets and services, and its scope expands the entire ITIL Version 3 lifecycle. ISM seeks to ensure that information security is effectively managed in all service management activities related to the CIA of data, as well as the security of hardware and software components, documentation and procedures as specifically defined in Department of Defense Directive (DoDD) 8500.1. Department of Defense Instruction (DoDI) 8500.2, the IA Implementation Directive, specifically addresses important topics such as:

- Common Criteria Certification
- Audit Data and Logging
- Computer Network Defense (CND)
- Vulnerability Mitigation
- Investigative Levels for Users
- Mission Assurance Categories (MAC (I, II, or III and tolerance/threshold))
- Confidentiality Levels (Classified, Sensitive, Public)
- Information Assurance Controls
- IA Control Mechanisms

- IA Control Number and Robustness Levels
- Information Assurance Training
- Future Applicable DoD Instructions and Directives

5.2 Policies

- Continuity of Service Contract (CoSC) Section 3.0

5.3 Outcomes

The outcome of a successful Information Security Management process includes:

- Ensuring the CIA of IT assets, data, information, and services, while remaining compliant with DoD, DON, Public Law, and other non-negotiable controls
- Ensuring the agreed availability of the infrastructure and the IT services, as well as the mission functions, are not compromised

5.4 Scope

The process covers the life cycle of information security concerns, including planning, operational measures, evaluation, and audit. It will identify IT security threats, vulnerabilities, and risks in order to develop an overall approach to counter and handle activities aligned with business information security requirements. It will operate information security protections and mechanisms which meet the desired level of confidentiality, integrity and availability for applicable DON information and IT services.

5.4.1 Includes

- Information security policy
- Specification of information security controls including asset use, access, documentation, and information controls and overseeing their establishment
- Operation of controls and measures such as:
 - Credential operations
 - Perimeter defense/Intrusion detection
- Secure coding standards
- Common Criteria (CC) certification
- Audit Computer Network Defense (CND)
- Vulnerability mitigation
- Investigative levels for users
- IA Controls
- Mission Assurance Categories (MAC)
- MAC Levels for Confidentiality

- Applicable MAC levels for Integrity & Availability and Confidentiality
- IA Control Mechanism
- IA Control Number and Robustness level
- Information Assurance (IA) training
- Key and encryption management
- Separation of duties
- Application isolation
- Identification of IT security incidents
- Management of supplier and partner access to services and systems
- Compliance enforcement measures (related to information security)

5.4.2 Excludes

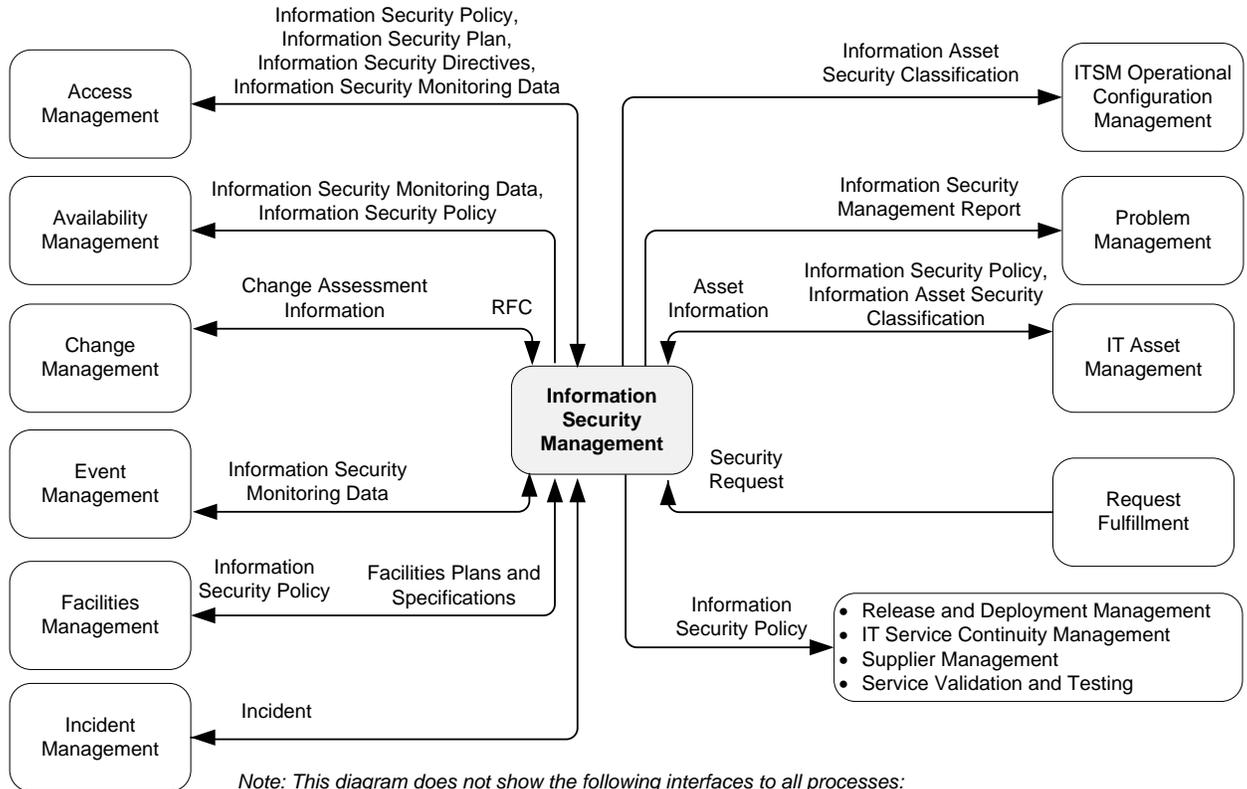
- Establishment and maintenance of identities and access rights (Access Management)
- Health and safety (Command responsibility, with contribution from Facilities Management)
- Identification of privacy requirements (within the scope of Compliance Management)

5.5 Process Interfaces

Primary interfaces with other processes include the following:

- Proposed RFCs from Change Management may be assessed by Information Security Management to determine their impact on IT security. In addition, Information Security Management may submit an RFC to Change Management to resolve a security-related issue.
- Assets (IT Asset Management) and CIs (Configuration Management) are assigned security classifications from Information Security Management.
- All CIs in Configuration Management that are assigned an information security classification.
- Information Security Management assists Request Fulfillment by handling information security-related service requests.
- Information security violations detected by Information Security Management resulting in an incident (Incident Management).
- Information security monitoring data is provided to Event Management, Access Management, and Availability Management for analysis.
- Information Security Management Reports are provided to Problem Management to help proactively identify problems.
- The Information Security Policy and Information Security Directives provide guidance to many processes, including, but not restricted to:

- Access Management
- Availability Management
- Facilities Management
- IT Service Continuity Management
- Release and Deployment Management
- Service Validation and Testing
- Supplier Management
- Facilities Management provides facilities plans and specifications to Information Security Management for planning purposes.
- This process is affected by the strategic direction described in the IT Strategy, generated by the Strategy Generation process.
- This process provides content in the form of Knowledge Items to the Knowledge Management process. In addition, Knowledge Management organizes and processes that content into Knowledge Assets.
- Compliance Management identifies specific Compliance Plans and Controls that should be adhered to by this process to meet standards and regulations that should be complied with. In return, this process provides an evaluation of how those standards and regulations were complied with.



Note: This diagram does not show the following interfaces to all processes:

- IT Strategy sent from Strategy Generation process
- Compliance Plans and Controls from Compliance Management process
- Knowledge Assets from Knowledge Management process

In addition, this diagram does not show the following interface to Knowledge Management from all processes:

- Knowledge Items sent to the Knowledge Management process

Figure 19 - Information Security Management Interfaces

5.6 Activity-Level Workflow

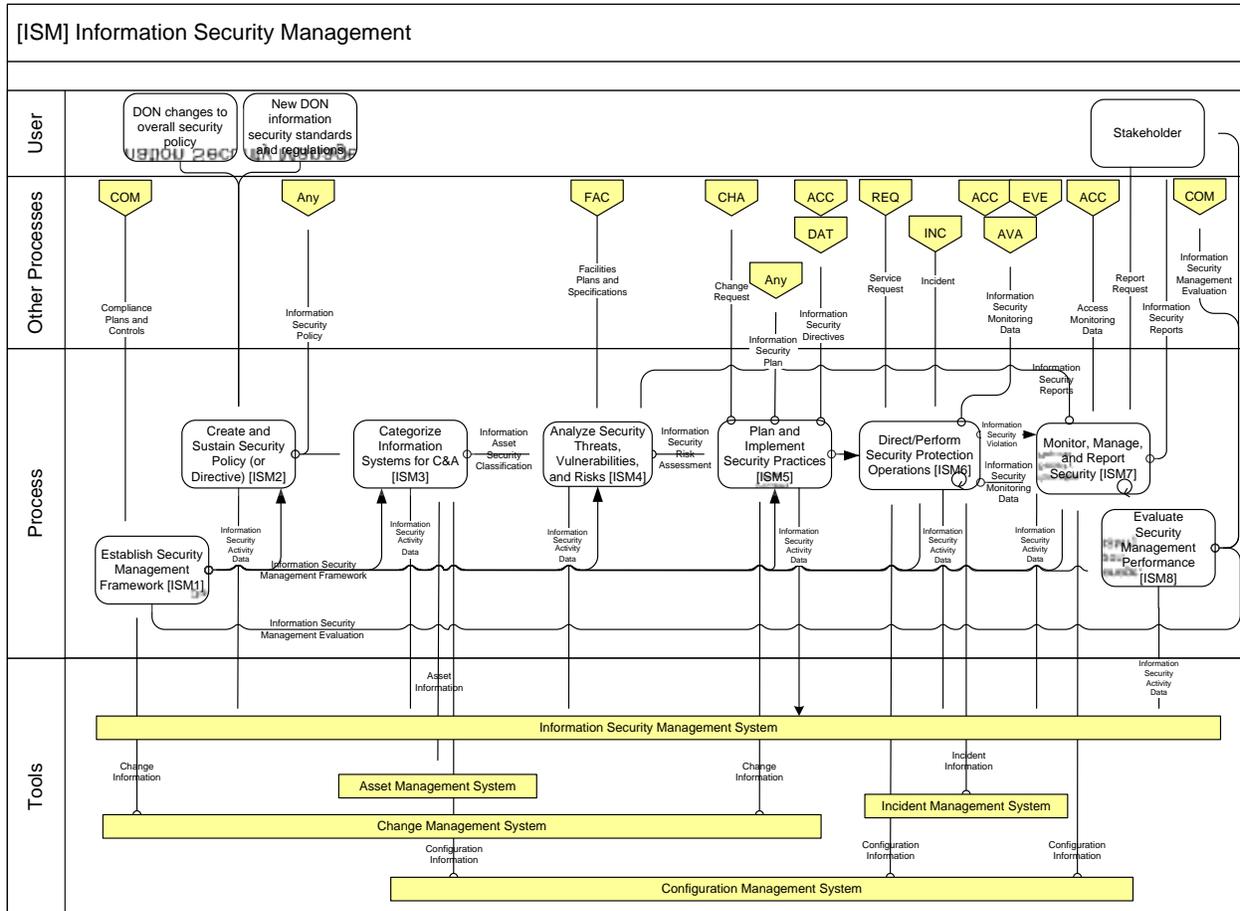


Figure 20 - Information Security Management Workflow

5.7 Activities

5.7.1 [ISM1] Establish Security Management Framework

This activity defines all direction, guidance, policies, and procedures for how the process will be performed. All of this is collectively referred to as the “process framework” and is used as reference information for all other activities. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for making changes and improvements to the process framework. The process framework is a collection of information, not necessarily a single document, which includes:

- Process purpose, scope, goals, and capabilities
- Process policies, standards, and conceptual models
- Process data requirements
- Role responsibilities
- Organizational responsibilities
- Detailed procedures and best practices, including, but not limited to:

- Standard security schemes
- Asset security classification scheme
- Classification scheme for threats, vulnerabilities, and risks
- Interfaces with other processes and programs
- Measurements and controls
- Tool requirements

In the diagram for this activity, note that the USN symbol indicates a touch point with the vendor.

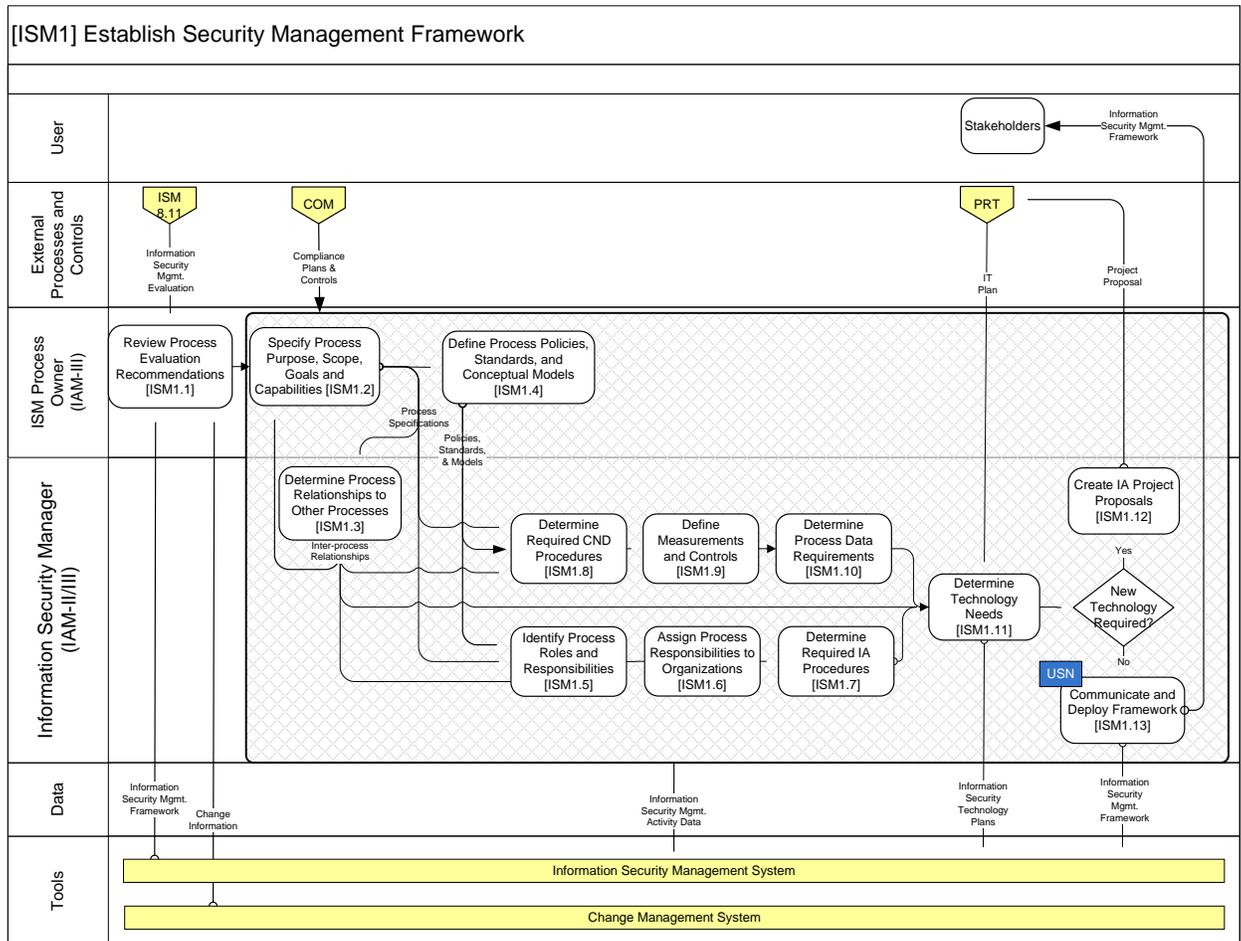


Figure 21 - ISM1 Workflow

5.7.1.1 TASKS

- Review Process Evaluation Recommendations
- Specify Process Purpose, Scope, Goals, and Capabilities
- Define Process Policies, Standards, and Conceptual Models
- Determine Process Data Requirements
- Identify Process Roles and Responsibilities
- Assign Process Responsibilities to Organizations

- Determine Process Procedures
- Determine Process Relationships to Other Processes
- Define Measurements and Controls
- Determine Technology Needs
- Create Project Proposals
- Communicate and Deploy Framework

5.7.1.2 DECISION TIMELINES

N/A

5.7.1.3 GAPS

N/A

5.7.1.4 INTERFACES

The headings in these tables are described in more detail in Appendix A.

Process Points	Process	Interface	Return/Terminate	Tools
ISM 1.13 Communicate and Deploy Framework to HPES 9.1	Change Management	RFC	Return	Remedy/SM7, RAPT/NEIRP
ISM 1.13 Communicate and Deploy Framework to HPES 9.1	Incident Management	Email, Message	Terminate	Remedy/SM7, RAPT/NEIRP
ISM 1.13 Communicate and Deploy Framework to HPES 9.1	Event Management	Email, Message	Terminate	Remedy/SM7, RAPT/NEIRP
ISM 1.13 Communicate and Deploy Framework to HPES 9.1	Release and Deploy	Email, Message	Terminate	Remedy/SM7, RAPT/NEIRP
ISM 1.13 Communicate and Deploy Framework to HPES 9.1	Problem Management	Email, Message	Terminate	Remedy/SM7, RAPT/NEIRP
ISM 1.13 Communicate and Deploy Framework to HPES 9.1	Access Management	Email, Message	Terminate	Remedy/SM7, RAPT/NEIRP

5.7.1.5 LOCATION

N/A

5.7.1.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Lifespan	Tools
ISM 1.13; 2.6; 4.1; 4.2; 4.3; 4.4; 4.5; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1a; 7.1b; 7.1d; 7.1e	IA Meeting	Virtual	Teleconference, Government leads	Weekly	portal

5.7.1.7 METRICS

N/A

5.7.1.8 ORGANIZATIONS

Process Point	Position	Org	Name	Contact Data	Tools
HPES 9.1 to ISM 1.13	HPES DoD Cyber Division	HPES	HPES DoD Cyber Director	GDA	Remedy/SM7
ISM 1.13 Communicate and Deploy Framework to HPES 9.1	NETOPS	NNWC	NetOps2	GDA, CLIN, RAPT/NEIRP	Remedy/SM7

5.7.1.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
HPES 9.1 to ISM 1.13	CoSC - Section 3.0	N/A	Portal		Portal
ISM 1.13 Communicate and Deploy Framework to HPES 9.1	CoSC - Section 3.0	N/A	Portal		Portal

5.7.1.10 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Access Point(s)	Tools
----------------	------	--------	-------------	-----------------	-------

Process Points	Type	Format	Periodicity	Access Point(s)	Tools
ISM 1.13; 2.3; 2.6; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1; 7.1a; 7.1b; 7.1d; 7.1e	Data, Information, and Reports	Electronic (RAPT, CLIN, GDA, Email, NEIRP, Messages	As Required	Pending off-site	RAPT/NEIRP, Remedy/SM7

5.7.2 [ISM2] Create and Sustain Information Security Policy

This activity creates the overall statement of the aims and objectives for the security that is to be established and operated in relation to IT services and resources. It maintains its currency as circumstances change for both the IT service provider and its customer set. It works within the limits set for the security policy of the mission as outlined in public law, applicable DoD/DON instructions and directives, modifying or extending its coverage to include aspects specific to information technology to enable compliance with existing regulations.

In the diagram for this activity, note that the USN symbol indicates a touch point with the contractor.

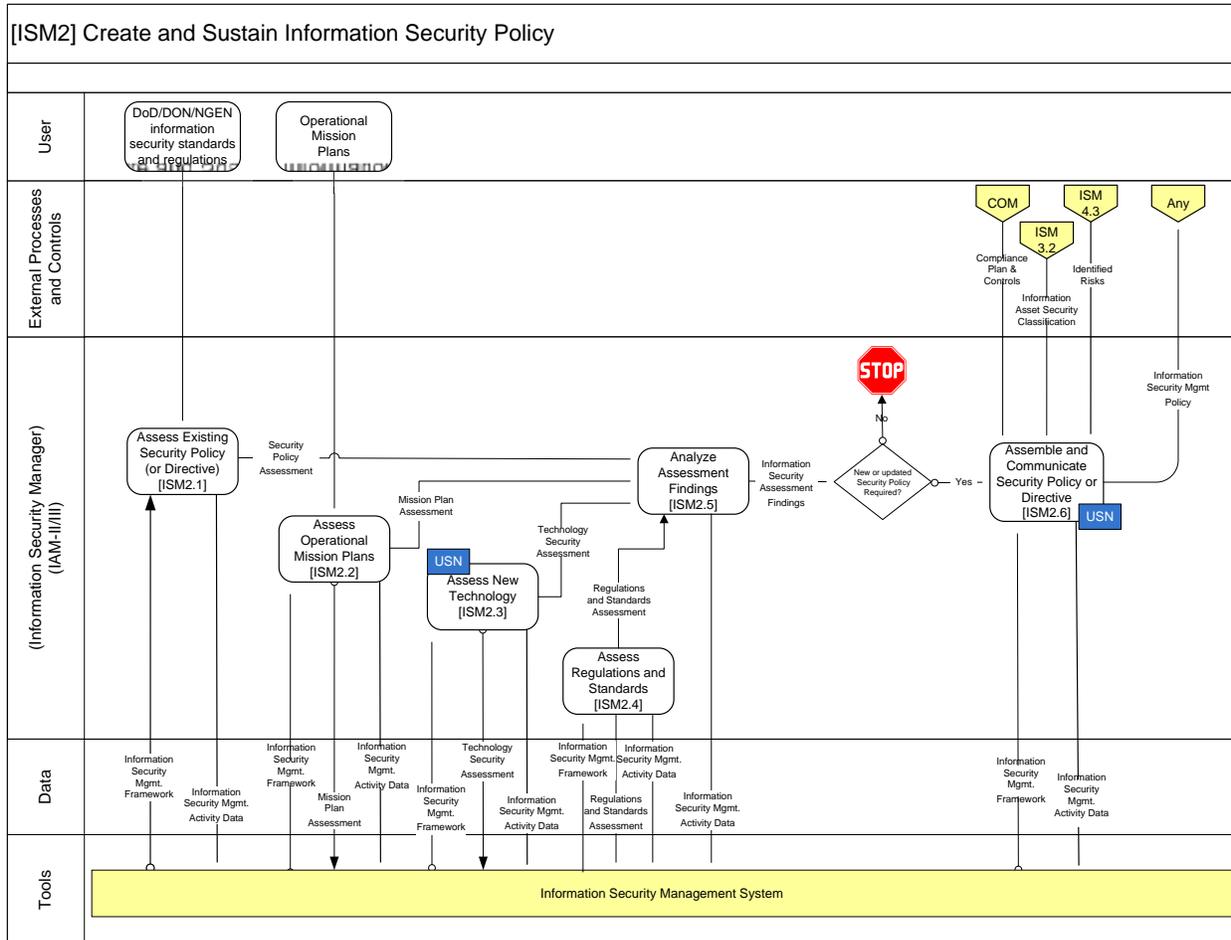


Figure 22 - ISM2 Workflow

5.7.2.1 TASKS

- Assess Existing Security Policy or Directive
- Assess Operational Mission Plans
- Assess New Technology
- Analyze Assessment Findings
- Assess Regulations and Standards
- Assemble and Communicate Security Policy or Directive

5.7.2.2 DECISION TIMELINES

Process Points	Decision	Timeline	Authority	Tools
ISM 2.6 Assemble and Communicate Security Policy or Directive to HPES 9.1	As Identified	As Directed	CoSC	GDA, Email, Remedy, SM7

5.7.2.3 GAPS

N/A

5.7.2.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools
ISM 2.6 Assemble and Communicate Security Policy or Directive	Change Management	RFC	Return	Remedy/SM7, RAPT/NEIRP
ISM 2.6 Assemble and Communicate Security Policy or Directive	Release and Deploy	Email, Message	Terminate	Remedy/SM7, RAPT/NEIRP
ISM 2.6 Assemble and Communicate Security Policy or Directive	Incident Management	Email, Message	Terminate	Remedy/SM7, RAPT/NEIRP
ISM 2.6 Assemble and Communicate Security Policy or Directive	Event Management	Email, Message	Terminate	Remedy/SM7, RAPT/NEIRP
ISM 2.6 Assemble and Communicate Security Policy or Directive	Problem Management	Email, Message	Terminate	Remedy/SM7, RAPT/NEIRP
ISM 2.6 Assemble and Communicate Security Policy or Directive	Access Management	Email, Message	Terminate	Remedy/SM7, RAPT/NEIRP

5.7.2.5 LOCATION

N/A

5.7.2.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Lifespan	Tools
ISM 1.13; 2.6; 4.1; 4.2; 4.3; 4.4; 4.5; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1a; 7.1b; 7.1d; 7.1e	IA Meeting	Virtual	Telcon, Government leads	Weekly	portal

5.7.2.7 METRICS

N/A

5.7.2.8 ORGANIZATIONS

Process Point	Position	Org	Name	Contact Data	Tools
HPES 9.1 to ISM 2.6	HPES DoD Cyber Division	HPES	HPES DoD Cyber Director	GDA	N/A
ISM 2.6 Assemble and communicate security policy or directive to HPES 9.1	NetOps	NNWC	NetOps2	GDA, CLIN, RAPT/NEIRP	N/A

5.7.2.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
ISM 2.6 Assemble and Communicate Security Policy or Directive to HPES 9.1	CoSC - Section 3.0	N/A	Portal		Portal

5.7.2.10 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Access Point(s)	Tools
ISM 1.13; 2.3; 2.6; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1; 7.1a; 7.1b; 7.1d; 7.1e	Data, Information, and Reports	Electronic (RAPT, CLIN, GDA, Email, NEIRP, Messages	As Required	Pending off-site	RAPT/NEIRP, Remedy/SM7

5.7.3 [ISM3] Categorize Information Systems for C&A

This activity examines the asset inventory, identifies security policy requirements and identifies the required security classification (MAC and Confidentiality level) for information assets.

In the diagram for this activity, note that the USN symbol indicates a touch point with the vendor.

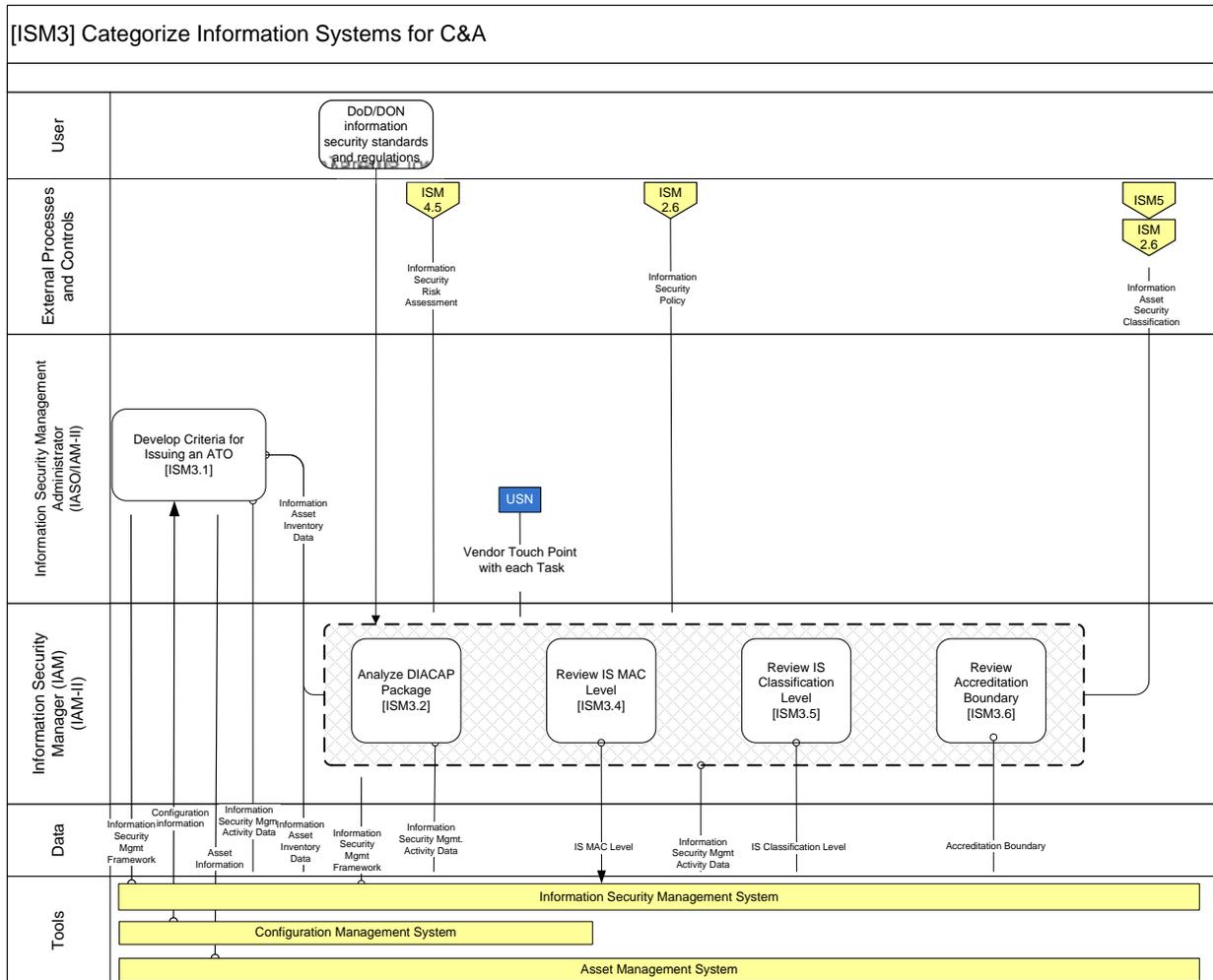


Figure 23 - ISM3 Workflow

5.7.3.1 TASKS

- Develop Criteria for Issuing an ATO
- Analyze DIACAP Package
- Review IS MAC Level
- Review IS Classification Level
- Review Accreditation Boundary

5.7.3.2 DECISION TIMELINES

Process Points	Decision	Timeline	Authority	Tools
ISM 3.2 Analyze DIACAP Package	Is DIACAP package sufficient to forward to validator	70 days prior to expiration of accreditation for site packages only not solutions	CoSC	IATS

5.7.3.3 GAPS

N/A

5.7.3.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools
ISM 3.2 Analyze DIACAP Package	Change Management	RFC	Return	Remedy/SM7, RAPT/NEIRP

5.7.3.5 LOCATION

N/A

5.7.3.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Lifespan	Tools
ISM 3.2 Analyze DIACAP Package	Package review, prioritization	Virtual	Teleconference, Government leads	Weekly at a minimum	N/A

5.7.3.7 METRICS

Process Points	Metric	Format	Access Point(s)	Frequency	Tools
ISM 3.2 Analyze DIACAP Package	Percentage of packages that meet quality requirements. 1st time 90% 2nd 100%	spreadsheet	IATS	weekly	IATS

5.7.3.8 ORGANIZATIONS

Process Point	Position	Org	Name	Contact Data	Tools
HPES 9.3 to ISM 3.2	HPES DoD Cyber Division	HPES	C&A Manager	Portal	IATS
ISM 3.2 Analyze DIACAP Package to HPES 9.3	PMW 130 C&A	SPAWAR	C&A Lead	Email/Portal	IATS

5.7.3.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
ISM 3.2 Analyze DIACAP Package	CoSC - Section 3.0	N/A	Portal		Portal

5.7.3.10 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Access Point(s)	Tools
ISM 3.2 Analyze DIACAP Package	DIACAP Package	Electronic	As required	Collaboration	IATS

5.7.4 [ISM4] Analyze Security Threats, Vulnerabilities and Risks

This activity identifies IT security threats, and determines risks and vulnerabilities to the command. It then recommends mitigating changes based on this analysis with policy guidance from DoDI 8500 series, Commander Joint Chiefs of Staff (CJCS) 6510 series, and Secretary of the Navy (SECNAV) 5239 series.

In the diagram for this activity, note that the USN symbol indicates a touch point with the contractor.

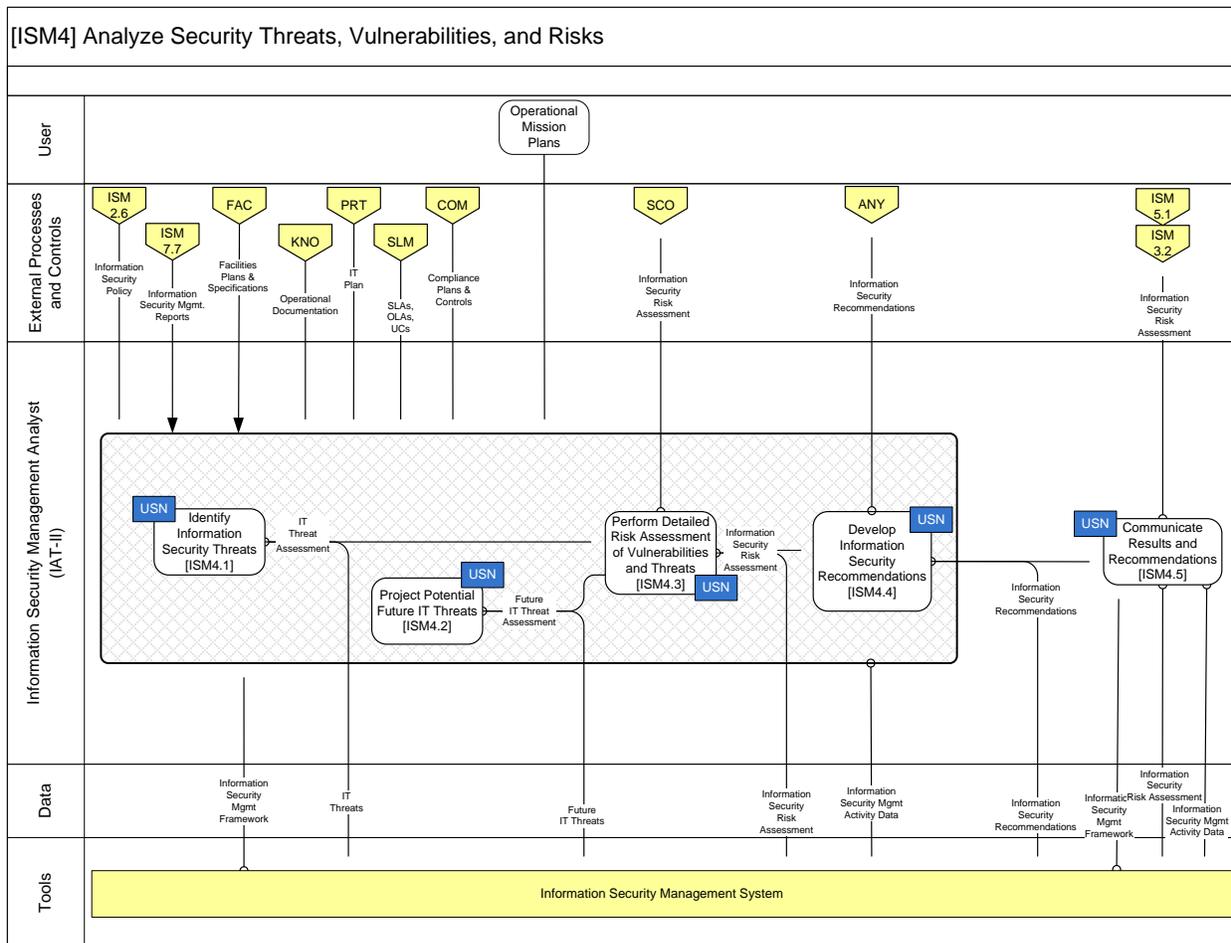


Figure 24 - ISM4 Workflow

5.7.4.1 TASKS

- Identify Information Security Threats
- Project Potential Future IT Threats
- Perform Detailed Risk Assessment of Vulnerabilities and Threats
- Develop Information Security Recommendations
- Communicate Results and Recommendations

5.7.4.2 DECISION TIMELINES

Process Points	Decision	Timeline	Authority	Tools
ISM 4.0 Analyze Security Threats, Vulnerabilities and Risks to HPES 9.6	As Identified	As Directed	CoSC	GDA, Email, Remedy, SM7

5.7.4.3 GAPS

N/A

5.7.4.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools
ISM 4.0 Analyze Security Threats, Vulnerabilities and Risks to HPES 9.6	Incident Management	Email, Message	Return/Terminate	Remedy/SM7, RAPT/NEIRP

5.7.4.5 LOCATION

N/A

5.7.4.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Lifespan	Tools
ISM 1.13; 2.6; 4.1; 4.2; 4.3; 4.4; 4.5; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1a; 7.1b; 7.1d; 7.1e	IA Meeting	Virtual	Telcon, Government leads	Weekly	portal

5.7.4.7 METRICS

Process Points	Metric	Format	Access Point(s)	Frequency	Tools
ISM 4.0 Analyze Security Threats, Vulnerabilities and Risks to HPES 9.6	Percentage of Incidents that fail to meet CoSC reporting requirements	spreadsheet	portal	quarterly	N/A

5.7.4.8 ORGANIZATIONS

Process Point	Position	Org	Name	Contact Data	Tools
HPES 9.6 to ISM 4.0	Operations Control	HPES	Watch	Phone, TMS	Remedy/SM7
ISM 4.0 Analyze Security Threats, Vulnerabilities and Risks to HPES 9.6	CNDSP	NCDOC	Watch	Phone, TMS, GDA	Remedy/SM7

5.7.4.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
ISM 4.0 Analyze Security Threats, Vulnerabilities and Risks to HPES 9.6	CoSC - Section 3.0	N/A	Portal		Portal

5.7.4.10 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Access Point(s)	Tools
ISM 4.0 Analyze Security Threats, Vulnerabilities and Risks to HPES 9.6	Data, Information, and Reports	Electronic	quarterly	portal	N/A

5.7.5 [ISM5] Plan and Implement Security Practices

This activity establishes the Security plan in compliance with DoDI 8500 series, CJCS 6510 series, and SECNAV 5239 series. It defines and creates an appropriate security infrastructure and procedures, translates actions in the plan to security directives, and communicates them. It also makes change requests in the environment to realize the Security Plan.

In the diagram for this activity, note that the USN symbol indicates a touch point with the contractor.

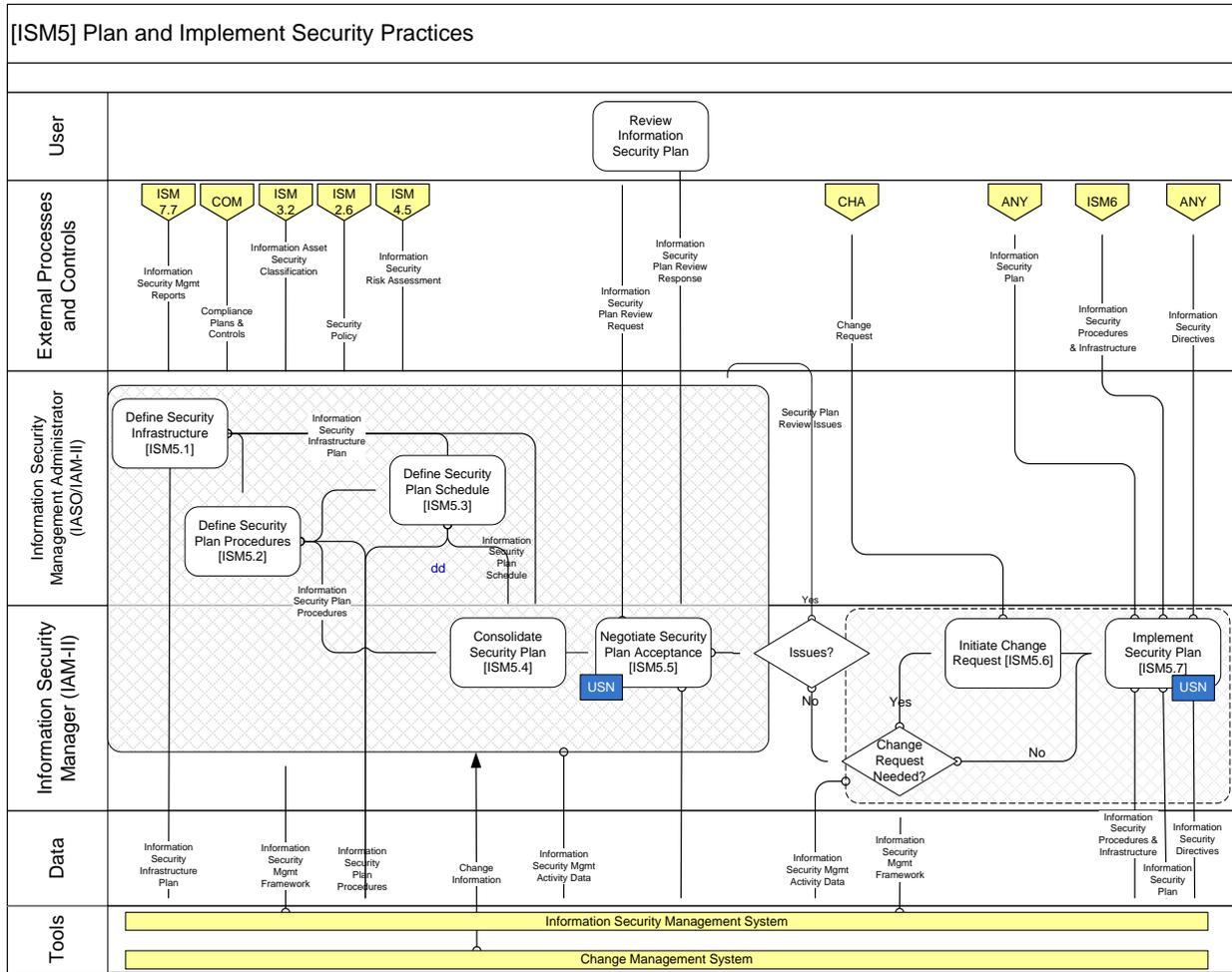


Figure 25 - ISM5 Workflow

5.7.5.1 TASKS

- Define Security Infrastructure
- Define Security Plan Procedures
- Define Security Plan Schedule
- Consolidate Security Plan
- Negotiate Security Plan Acceptance
- Initiate Change Request
- Implement Security Plan

5.7.5.2 DECISION TIMELINES

Process Points	Decision	Timeline	Authority	Tools
ISM 5.5 Negotiate Security Plan Acceptance	Implementation of ISM Framework	As Directed	CoSC	GDA

Process Points	Decision	Timeline	Authority	Tools
ISM 5.7 Implement Security Plan to HPES 9.7	Implementation of ISM Framework	As Directed	CoSC	GDA, Email, Remedy, SM7

5.7.5.3 GAPS

N/A

5.7.5.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools
ISM 5.7 Implement Security Plan	All	Email, Message	Return/Terminate	

5.7.5.5 LOCATION

N/A

5.7.5.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Lifespan	Tools
ISM 1.13; 2.6; 4.1; 4.2; 4.3; 4.4; 4.5; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1a; 7.1b; 7.1d; 7.1e	IA Meeting	Virtual	Telcon, Government leads	Weekly	portal

5.7.5.7 METRICS

Process Points	Metric	Format	Access Point(s)	Frequency	Tools
ISM 5.7 Implement Security Plan	Percentage of GDA implementations that failed to meet CoSC requirement	spreadsheet	portal	biweekly	Remedy/SM7

5.7.5.8 ORGANIZATIONS

Process Point	Position	Organization	Name	Contact Data	Tools
---------------	----------	--------------	------	--------------	-------

Process Point	Position	Organization	Name	Contact Data	Tools
HPES 9.7 to ISM 5.5	HPES DoD Cyber Division	HPES	Cyber Compliance	TMS	Remedy/SM7
HPES 9.7 to ISM 5.7	Operations Control	HPES	Watch	TMS	Remedy
ISM 5.5 Negotiate Security Plan Acceptance to HPES 9.7	NETOPS	NNWC	NetOps2	GDA, TMS	Remedy/SM7
ISM 5.7 Implement Security Plan to HPES 9.7	NETOPS	NNWC	NetOps2	GDA, Email	Remedy

5.7.5.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools
ISM 5.5 Negotiate Security Plan Acceptance	CoSC - Section 3.0	N/A	Portal	Portal
ISM 5.7 Implement Security Plan	CoSC - Section 3.0	N/A	Portal	Portal

5.7.5.10 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Access Point(s)	Tools
ISM 1.13; 2.3; 2.6; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1; 7.1a; 7.1b; 7.1d; 7.1e	Data, Information, and Reports	Electronic (RAPT, CLIN, GDA, Email, NEIRP, Messages	As Required	Pending off-site	RAPT/NEIRP, Remedy/SM7
ISM 5.5 Negotiate Security Plan	Data, Information, and Reports	Electronic	weekly/monthly	portal	N/A

5.7.6 [ISM6] Direct/Perform Security Protection Operations

This activity puts in place established security regulations, directives, controls and procedures throughout all aspects of IT, both in terms of the IT command and by activating the security protections within IT solutions and services. It also applies the mechanisms involving the full

range of education and training, installing new systems, and testing to make sure that security controls and procedures work properly. This activity actuates and monitors the full range of security measures and capabilities, responding to service or resource access authorization requests in addition to noting security violations and initiating incidents when necessary. Real-time intrusion detection sensing and immediate responses are an important part of the function of this activity.

In the diagram for this activity, note that the USN symbol indicates a touch point with the contractor.

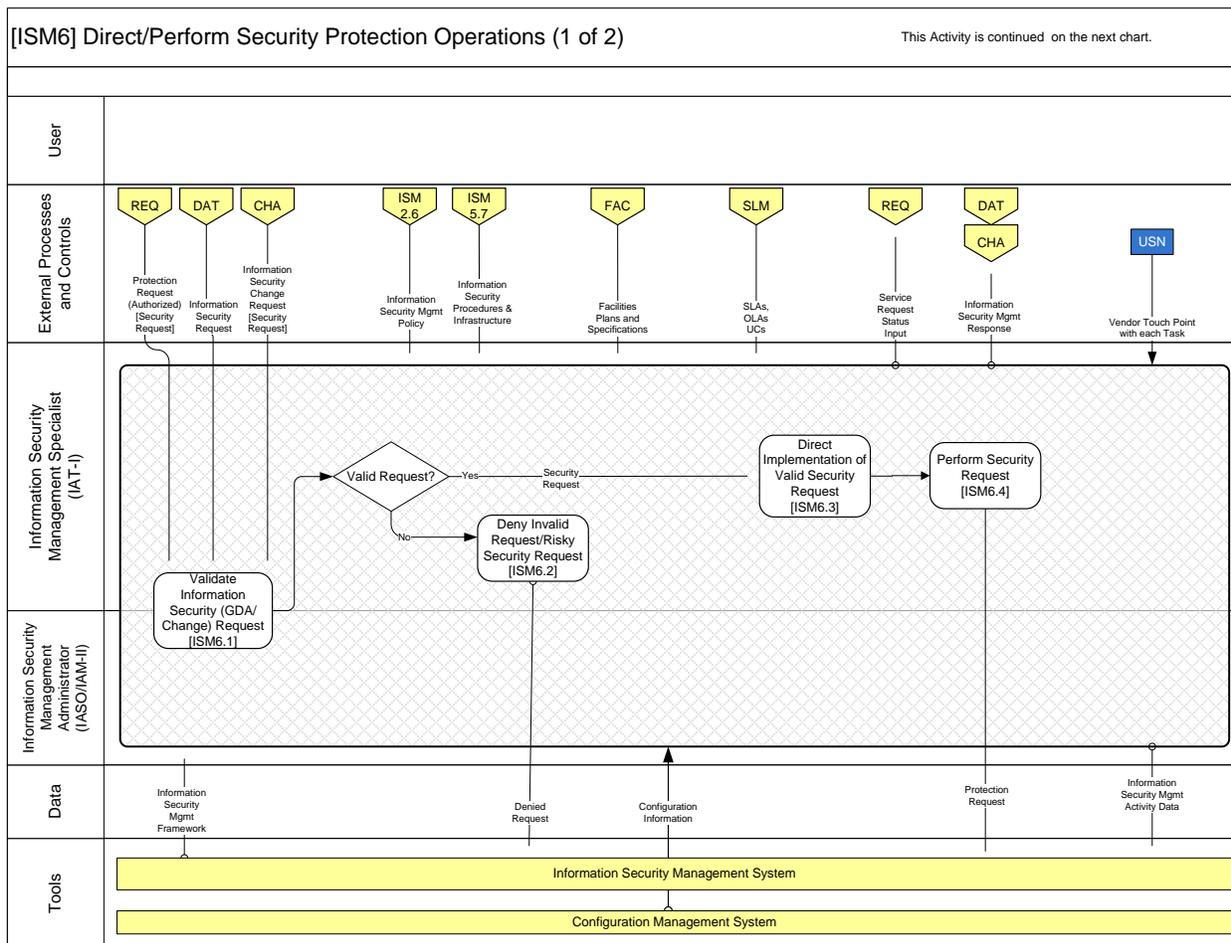


Figure 26 - ISM6 Workflow, part 1

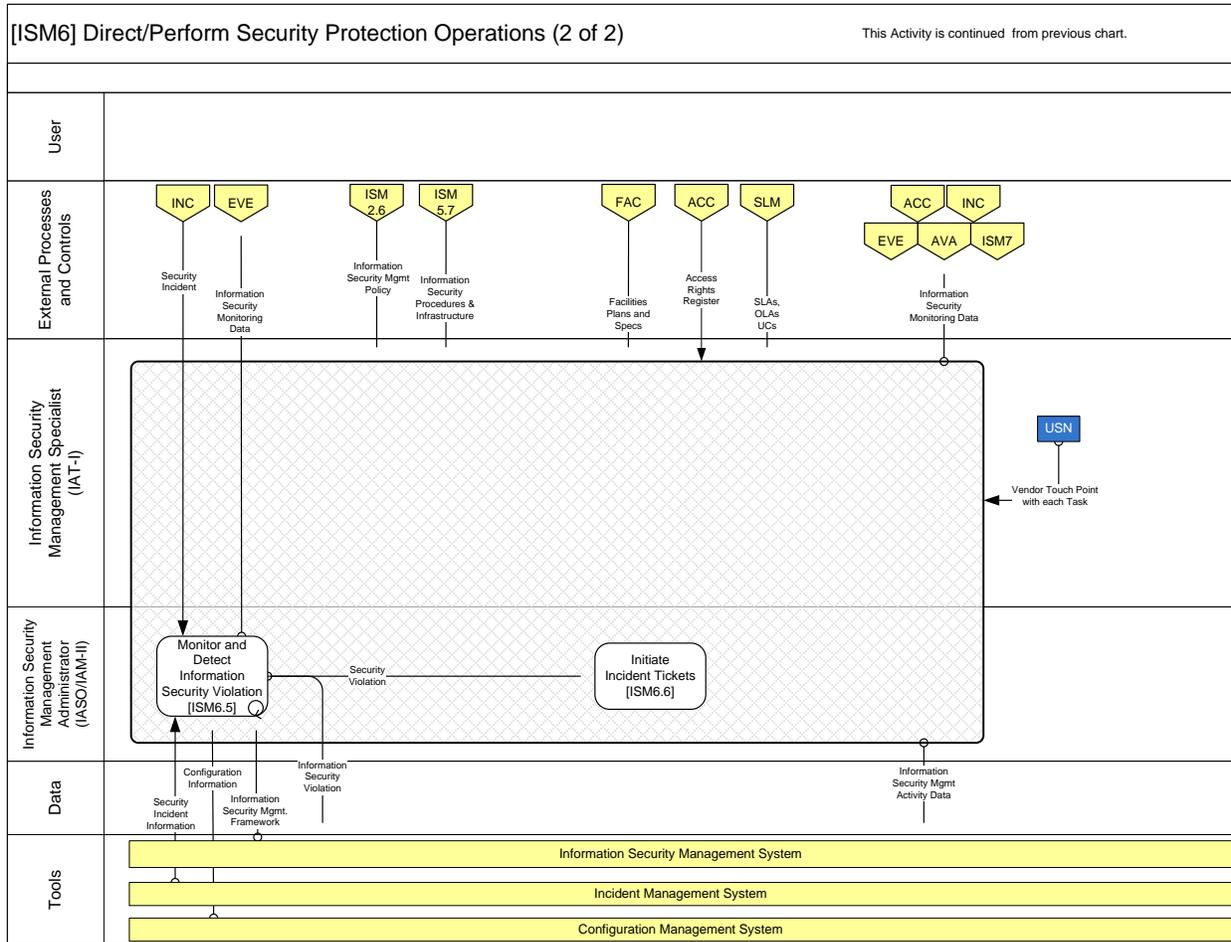


Figure 27 - RDM6 Workflow, part 2

5.7.6.1 TASKS

- Validate Information Security Request
- Deny Invalid Request/Risky Security Request
- Direct Implementation of Valid Security Request
- Perform Security Request
- Monitor and Detect Information Security Violation
- Initiate Incident Tickets

5.7.6.2 DECISION TIMELINES

Process Points	Decision	Timeline	Authority	Tools
ISM 6.1-6.4 to HPES 9.5	As Identified	As Directed	CoSC	GDA, Email, Remedy, SM7

5.7.6.3 GAPS

N/A

5.7.6.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools
ISM 6.1 -6.4	All	Email, Message	Return/Terminate	

5.7.6.5 LOCATION

N/A

5.7.6.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Lifespan	Tools
ISM 1.13; 2.6; 4.1; 4.2; 4.3; 4.4; 4.5; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1a; 7.1b; 7.1d; 7.1e	IA Meeting	Virtual	Teleconference, Government leads	Weekly	portal

5.7.6.7 METRICS

Process Points	Metric	Format	Access Point(s)	Frequency	Tools
ISM 6.1-6.4	Percentage of GDA implementations that require additional information from government	spreadsheet	portal	biweekly	Remedy/SM7

Process Points	Metric	Format	Access Point(s)	Frequency	Tools
ISM 6.1-6.4	Percentage of Government Directed Action (GDA) implementations based on Cryptologic Technician (Interpretive) [CTI] that failed to meet CoSC requirement	spreadsheet	portal	biweekly	Remedy/SM7

5.7.6.8 ORGANIZATIONS

Process Point	Position	Organization	Name	Contact Data	Tools
HPES 9.5 to ISM 6.1-6.4	Operations Control	HPES	Watch	TMS	
ISM 6.1-6.4 to HPES 9.5	NETOPS	NNWC	Watch	GDA, Email	Remedy/SM7

5.7.6.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
ISM 6.1-6.4 to HPES 9.5	CoSC - Section 3.0	N/a	Portal		Portal
ISM 6.5 - ISM6.6 Monitor and Detect Information Security Violation	CoSC - Section 3.0	N/a	Portal		Portal

5.7.6.10 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Access Point(s)	Tools
----------------	------	--------	-------------	-----------------	-------

Process Points	Type	Format	Periodicity	Access Point(s)	Tools
ISM 1.13; 2.3; 2.6; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1; 7.1a; 7.1b; 7.1d; 7.1e	Data, Information, and Reports	Electronic (RAPT, CLIN, GDA, Email, NEIRP, Messages	As Required	Pending off-site	RAPT/NEIRP, Remedy/SM7

5.7.7 [ISM7] Monitor, Manage and Report Information Security Management

This activity addresses reviewing security controls and mechanisms and determines whether they appropriately and effectively implement security policies and procedures as described in DoD 8500 Series, SECNAV 5239 Series, CJCS 6510 Series (CND Volume 1 Incident Handling Program), Security Management Framework and the Security plan.

In the diagram for this activity, note that the USN symbol indicates a touch point with the contractor.

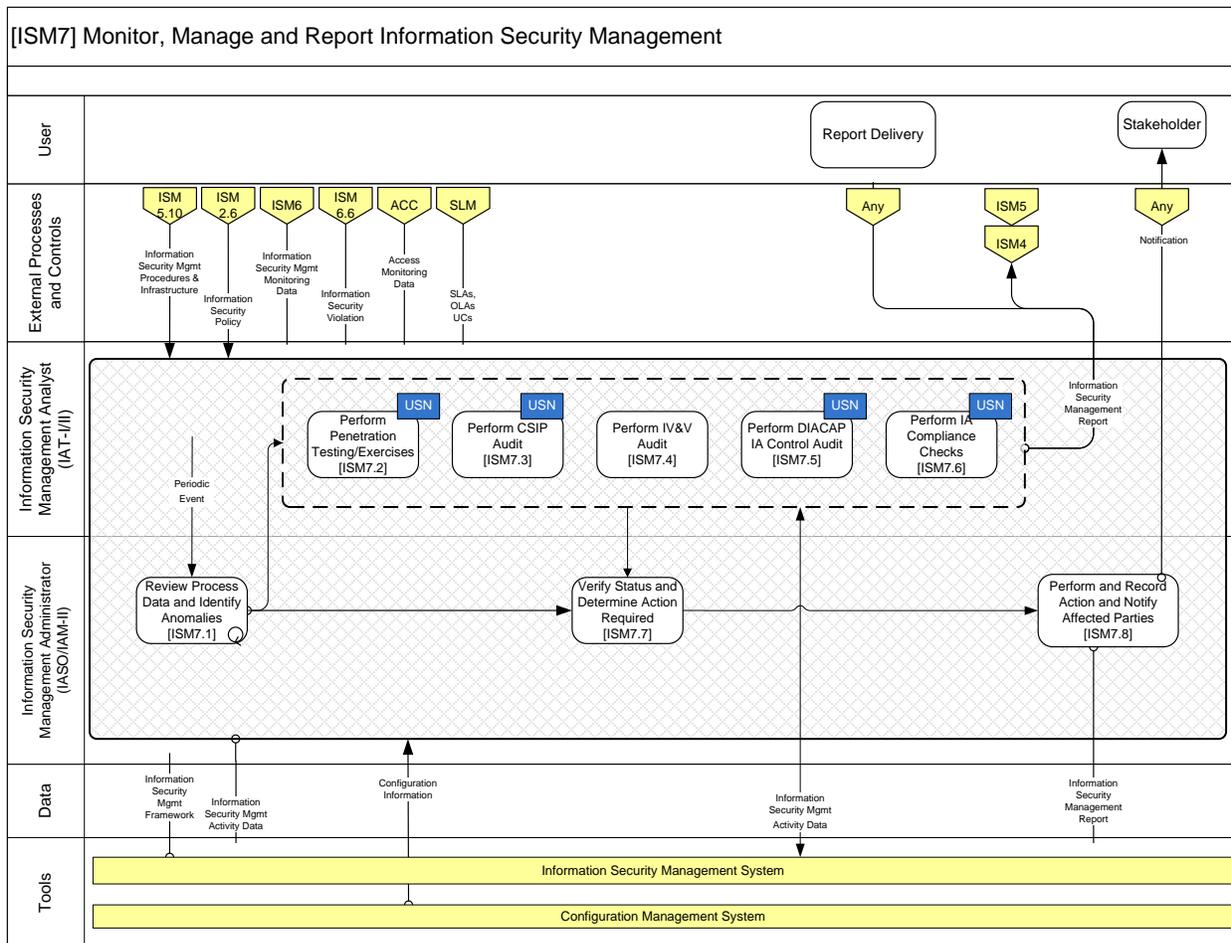


Figure 28 - ISM7 Workflow

5.7.7.1 TASKS

- Review Process Data and Identity Anomalies
- Perform Penetration Testing/Exercises
- Perform CSIP Audit
- Perform IV&V Audit
- Perform DIACAP IA Control Audit
- Perform IA Compliance Checks
- Verify Status and Determine Action Required
- Perform and Record Action and Notify Affected Parties

5.7.7.2 DECISION TIMELINES

Process Points	Decision	Timeline	Authority	Tools
----------------	----------	----------	-----------	-------

Process Points	Decision	Timeline	Authority	Tools
ISM 7.1 Review Process Data and Identify Anomalies to HPES 9.2	As Identified	As Directed	Cosc	GDA, Email, Remedy, SM7

5.7.7.3 GAPS

Process Points	Description	Severity	Mitigation	Timeline	Tools
ISM 7.1 Review Process Data and Identify Anomalies to HPES 9.2	Exercise after action reports, <u>provided to</u> <u>vendors</u> , to work towards CSI	Moderate	Regional Network Operations Security Centers will coordinate	1 year	N/A

5.7.7.4 INTERFACES

Process Points	Process	Interface	Return/Terminate		Tools
ISM 7.1 Review Process Data and Identify Anomalies to HPES 9.2	Incident, Event, Problem Management	Email, Message	Return		

5.7.7.5 LOCATION

N/A

5.7.7.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Lifespan	Tools
ISM 1.13; 2.6; 4.1; 4.2; 4.3; 4.4; 4.5; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1a; 7.1b; 7.1d; 7.1e	IA Meeting	Virtual	Telcon, Government leads	Weekly	portal

5.7.7.7 METRICS

N/A

5.7.7.8 ORGANIZATIONS

Process Point	Position	Organization	Name	Contact Data	Tools
HPES 9.2 to ISM 7.1	HPES DOD Cyber Division	HPES	HPES DoD Cyber Director	GDA	Remedy/SM7
ISM 7.1 Review Process Data and Identify Anomalies to HPES 9.2	NETOPS	NNWC	NetOps 2	GDA, Email	Remedy

5.7.7.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
ISM 7.1 Review Process Data and Identify Anomalies to HPES 9.2	CoSC - Section 3.0	N/a	Portal		Portal

5.7.7.10 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Access Point(s)	Tools
ISM 1.13; 2.3; 2.6; 5.5; 5.7; 6.1; 6.2; 6.3; 6.4; 6.5; 6.6; 7.1; 7.1a; 7.1b; 7.1d; 7.1e	Data, Information, and Reports	Electronic (RAPT, CLIN, GDA, Email, NEIRP, Messages)	As Required	Pending off-site	RAPT/NEIRP, Remedy/SM7

5.7.8 [ISM8] Evaluate Security Management Performance

In this activity, the Information Security Management process performance identifies areas that need improvement, such as the foundation and interfaces of the process, activity definitions, key performance metrics, the state of supporting automation, as well as the roles and responsibilities and skills required as stipulated in DoD 8500 Series, SECNAV 5239 Series, and CJCS 6510 Series (CND Volume 1 Incident Handling Program). This activity identifies security controls that are inconsistent with the Information Security Management Framework and Security Plan. Insights and lessons learned from direct observation and data collected on process performance is the basis for improvement recommendations.

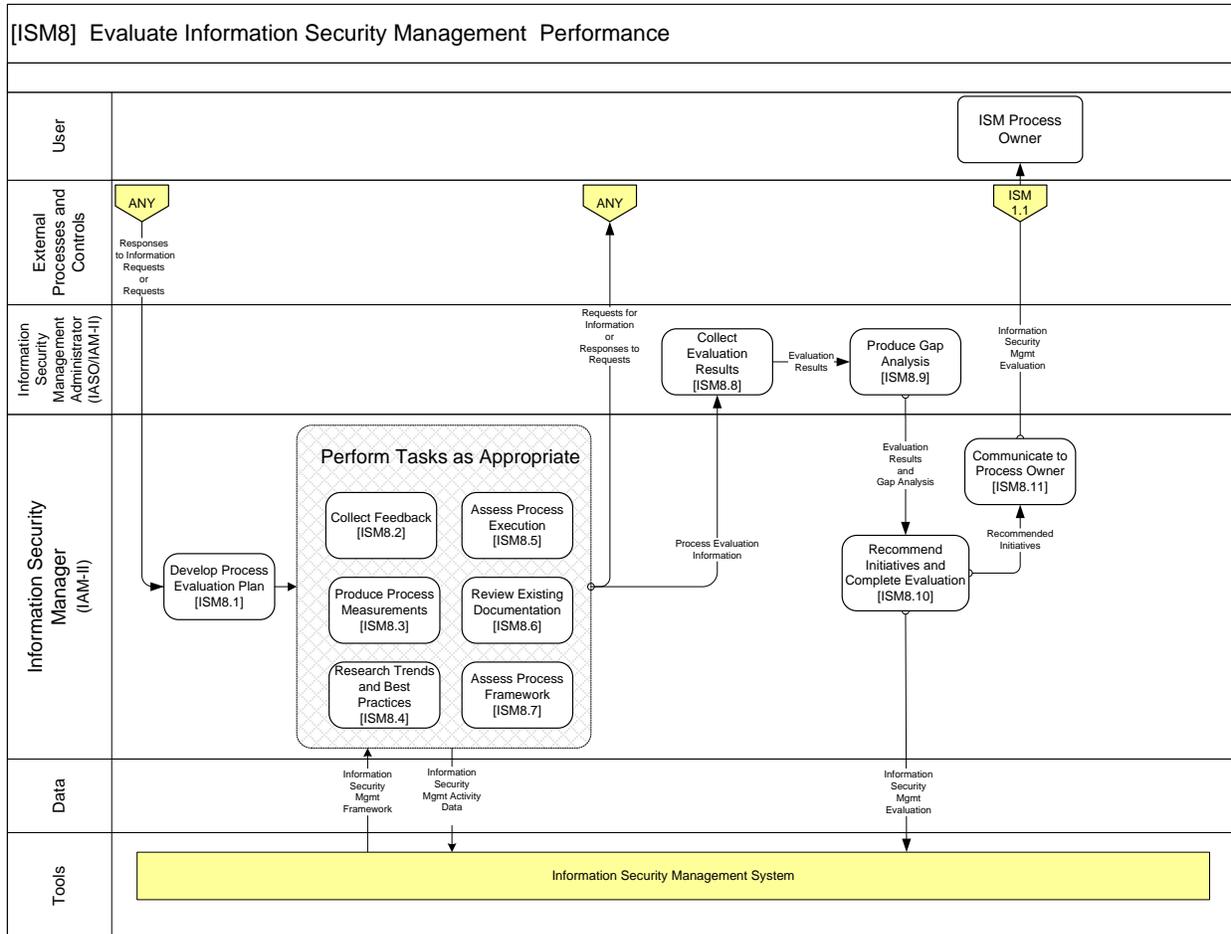


Figure 29 - ISM8 Workflow

5.7.8.1 TASKS

- Collect Feedback
- Produce Process Measurements
- Research Trends and Best Practices
- Review Existing Documentation
- Assess Process Execution
- Audit Process
- Assess Process Framework
- Collect Evaluation Results
- Produce Gap Analysis
- Recommend Initiatives
- Complete Evaluation
- Communicate to Process Owner

5.7.8.2 DECISION TIMELINES

N/A

5.7.8.3 GAPS

N/A

5.7.8.4 INTERFACES

N/A

5.7.8.5 LOCATION

N/A

5.7.8.6 MEETINGS

N/A

5.7.8.7 METRICS

N/A

5.7.8.8 ORGANIZATIONS

N/A

5.7.8.9 POLICIES

N/A

5.7.8.10 WORK PRODUCTS

N/A

5.8 Roles

Role Name	Brief Role Description and Responsibilities
Information Security Management Process Owner	Accountable for proper process design, execution, and continual improvement. Ensures that the process is being carried out, but does not run the day-to-day operation of the process. The Information Security Management Process Owner receives regular updates concerning the performance of the process and represents this process concerning all decisions.

Role Name	Brief Role Description and Responsibilities
Information Security Manager	Responsible for coordination across processes, primarily responsible for the overall quality of the ISM process. The Information Security Manager is the main coordinator within this process and is the focal point regarding changes for the command. It is recommended that all managers in the command, as well as other processes, must support this role.
Information Security Analyst	Uses technical knowledge and subject matter expertise to understand and resolve security issues, analyze security risks, and recommend changes to operational security. Analysis involves the understanding of causes and effects. An individual in the Information Security Analyst role uses the knowledge gained from their analysis to make recommendations or to provide resolutions. The Information Security Analyst also supports other ITSM process roles and activities.
Information Security Specialist	Performs the hands-on work to secure the environment and implement security controls. An Information Security Specialist's primary responsibility is to focus on the operational aspects of security.
Information Security Administrator	Supports the Information Security Manager by monitoring security systems, supporting security plan development, and providing process-related reports. Also assists with analyzing overall ISM process performance.
Service Provider	Contractually responsible and accountable for the operational activities described in the statement of work and service level agreements.
User	Supports the overall ISM process and includes higher-authority stakeholders.

Process Activity	Information Security Management Process Owner	Information Security Manager	Information Security Analyst	Information Security Specialist	Information Security Administrator	Service Provider
[ISM1] Establish Security Management Framework	A	R	I	I	I	I
[ISM2] Create and Sustain Information Security Policy	A	R	C	C	I	I
[ISM3] Analyze Security Threats, Vulnerabilities and Risks	C/I	R	A/R	C	I	I
[ISM4] Classify Information Asset Security	I	A	R	R	C/I	I
[ISM5] Plan and Implement Security Practices	I/C	A	R	R	I	I
[ISM6] Operate Security Protection Mechanisms	I	A/C/I	C	R	R	R
[ISM7] Monitor, Assess, Audit and Report Security	I	A	C	C	R	I
[ISM8] Evaluate Security Management Performance	I	A/R	R	C	C	I

5.9 Information Work Products

The work products indicated in the process workflows include:

- Access Monitoring Data
- Access Rights Register
- Accreditation Boundary
- Asset Information
- Change Information
- Change Request
- Compliance Plans and Controls
- Configuration Information
- Denied Request
- Evaluation Results
- Facilities Plans and Specifications
- Future IT Threats
- Identified Risks
- Incident
- Incident Information
- Information Asset Inventory Data
- Information Asset Security Classification
- Information Security Activity Data
- Information Security Assessment Findings
- Information Security Change Request
- Information Security Directives
- Information Security Infrastructure Plan
- Information Security Management Activity Data
- Information Security Management Evaluation
- Information Security Management Framework
- Information Security Management Policy
- Information Security Management Practices
- Information Security Management Report
- Information Security Management Reports
- Information Security Management Response
- Information Security Monitoring Data
- Information Security Plan
- Information Security Plan Procedures
- Information Security Plan Review Request

- Information Security Plan Review Response
- Information Security Plan Schedule
- Information Security Policy
- Information Security Procedures and Infrastructure
- Information Security Recommendations
- Information Security Reports
- Information Security Request
- Information Security Risk Assessment
- Information Security Technology Plans
- Information Security Violation
- IS Classification Level
- IS MAC Level
- IT Plan
- IT Plan
- IT Threat Assessment
- IT Threats
- Mission Plan Assessment
- Operational Documentation
- Operational Mission Plans
- Process Evaluation Information
- Project Proposal
- Protection Request
- Recommended Initiatives
- Regulations and Standards Assessment
- Report Request
- Requests for Information or Responses to Requests
- Responses to Information Requests or Requests
- Security Incident
- Security Plan Review Issues
- Security Policy
- Security Policy Assessment
- Security Request
- Security Violation
- Service Request
- Service Request Status Input
- SLAs, OLAs, US
- Technology Security Assessment

5.10 Performance Metrics

- Percentage of packages that meet quality requirements. 1st time 90% 2nd 100%
- Percentage of Incidents that fail to meet CoSC reporting requirements
- Percentage of GDA implementations that failed to meet CoSC requirement
- Percentage of GDA implementations that require additional information from government
- Percentage of GDA implementations based on CTI that failed to meet CoSC requirement

5.11 Organizational RACI

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
ISM	Information Security Management		NNWC	C	C	A					
ISM1	Establish Security Management Framework	Meetings: IA Meeting Policies: COSC Section 3.0 Data, Information and Reports, Electronic Format (RAPT, CLIN, GDA, Email, NEIRP, Messages, Remedy, SM7	NNWC	C	C	R	R	I	I		C

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
ISM2	Create and Sustain Information Security Policy	Directive Communications, GDA, Email, Remedy, SM7 Meetings: IA Meeting, Weekly, Leverage Portal Polices, COSC Section 3.0 Data, Information and reports: Electronic (RAPT, CLIN, GDA, Email, NEIRP, Messages, Remedy, SM7)	NNWC	C	C	R	C	R	R		I

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
ISM3	Categorize Information Systems for C&A	DIACAP Packages, electronic, IATS tool Analyze DIACAP Package 70 days prior to expiration of accreditation for site packages only, not for solutions Meetings: Package review and prioritization, weekly at a minimum Policies: COSC Section 3.0 Metrics: % of packages that meet quality requirements, 1st time 90%, 2nd 100%	NNWC		C	R	R	R			

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
ISM4	Analyze Security Threats, Vulnerabilities and Risks	Security Threat, Vulnerability, Risk Analysis Reports, DGA, Email, Remedy, SM7 Incident Ticket, Email, SM7, Remedy, RAPT, NEIRP Meetings: IA Meeting Polices maintained on Portal Metrics: % Incidents that fail to meet reporting requirements (spreadsheet, maintained on portal)	NNWC	C	C	R	R	R			

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
ISM5	Plan and Implement Security Practices	IA Meetings, Weekly Portal Polices in COSC Section 3.0 Metrics: % of GDA implementations that failed to met requirements, spreadsheet maintained on portal, biweekly, Remedy and SM7 Security Information in RAPT, NEIRP, Remedy and SM7	NNWC	C	C	R	R	R	R	I	I

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
ISM6	Direct/Performance Security Protection Mechanisms	GDA, email, Remedy, SM7 IA Meeting, Weekly Polices in COSC 3.0 Metrics: % GDA Implementations that require additional information from government, spreadsheet, maintained on portal, biweekly, Reedy, SM7 % GDA implementations based on Cryptologic Technician (Interpretative) (CTI) that failed to meet requirement	NNWC			R	R	R	R		

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
ISM7	Monitor, Manage and Report Information Security Management	Security Reviews, GDA, Email, Remedy, SM7 Exercise After Action Reports provided to vendors to support CSI, RNOSCS coordinate IA Meetings, Weekly Policies: COSC 3.0 Security Information: Electronic Messages, RAPT, CLIN, GDA, Email, NEIRP, Message, SM7, Remedy	NNWC		C	R	I	R	R		

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
ISM8	Evaluate Security Management Performance		NNWC		C	R	C	R	R		

Table 8 – Information Security Management RACI Chart

6. IT ASSET MANAGEMENT [ITAM]

6.1 Process Purpose

The purpose of IT Asset Management is to identify, track and control all hardware, software and IT related equipment necessary to deliver services throughout the asset lifecycle, including their characteristics/attributes. An asset can be any resource or capability that must be tracked for regulatory or financial purposes.

6.2 Process Policies

6.2.1 DoD and DON Policies

This section defines the key Federal, DoD and DON policies that govern the process.

Policy #	Policy Name	Requirement
CCA	Clinger-Cohen Act	The Clinger-Cohen Act supplements the information resources management policies by establishing a comprehensive approach for executive agencies to improve the acquisition and management of their information resources, by: <ul style="list-style-type: none"> • focusing information resource planning to support their strategic missions • implementing a capital planning and investment control process that links to budget formulation and execution • rethinking and restructuring the way they do their work before investing in information systems.
FAR 45	Federal Acquisition Regulation, Government Property	This part prescribes policies and procedures for providing Government property to contractors, contractors' management and use of Government property, and reporting, redistributing, and disposing of contractor inventory. It does not apply to property under any statutory leasing authority, (except as to non-Government use of property under 45.301(f)); to property to which the Government has acquired a lien or title solely because of partial, advance, progress, or performance-based payments; to disposal of real property; or to software and intellectual property.
FAR 46	Federal Acquisition Regulation, Quality Assurance	This part prescribes policies and procedures to ensure that supplies and services acquired under Government contract conform to the contract's quality and quantity requirements. Included are inspection, acceptance, warranty, and other measures associated with quality requirements.
FAR 52	Federal Acquisition Regulation, Government Property	This part gives instructions for using provisions and clauses in solicitations and/or contracts, sets forth the solicitation provisions and contract clauses prescribed by this regulation, and presents a matrix listing the FAR provisions and clauses applicable to each principal contract type and/or purpose (e.g., fixed-price supply, cost-reimbursement research and development).

OMB Circular A-136	Financial Reporting Requirements	This circular establishes a central point of reference for all Federal financial reporting guidance for Executive Branch departments, agencies, and entities required to submit audited financial statements, interim financial statements, and Performance and Accountability Reports (PAR) under the Chief Financial Officers Act of 1990 (“CFO Act”) (Pub. L. No. 101 – 576), the Accountability of Tax Dollars Act of 2002 (“ATDA”) (Pub. L. No. 107 – 289), and Annual Management Reports under the Government Corporations Control Act (31 U.S.C. § 9101 et seq.).
DFARS	Defense Federal Acquisition Regulation Supplement (DFARS) and Procedures, Guidance, and Information (PGI)	<ul style="list-style-type: none"> • Requirements of law • DoD-wide policies • Delegations of FAR authorities • Deviations from FAR requirements • Policies/procedures that have a significant effect beyond the internal operating procedures of DoD or a significant cost or administrative impact on contractors or offerors
DoD Instruction 4100.39-M	FLIS Procedures Manual	The policies outlined in this manual are published under the authority of the DoD Materiel Management Regulation, DoD 4140.1-R, and are mandatory for use by all participants in the Federal Catalog Program. The procedures contained in this manual which implement this policy are also mandatory for use by all participants in the Federal Catalog System. The Federal Catalog Program (FCP) is a Government-wide program established by public law 82-436 in 1952 to provide a uniform system of item identification; preclude/eliminate different identifications of like items; reveal interchangeability among items; aid in parts standardization; facilitate intra- and interdepartmental logistics support; and improve materiel management and military effectiveness by promoting efficiency and economy in logistics operations.
DoD Directive 4140.1-R	Supply Chain Materiel Management Policy	<ul style="list-style-type: none"> • Developing materiel requirements based on customer expectations while minimizing the DoD investment in inventories • Selecting support providers on the basis of best value • Determining how best to position and deliver materiel to satisfy highly variable readiness and combat sustainment needs in a variety of unique and demanding environments • Executing other supply chain functions and programs, some of which are unique to the Department <p>To provide for effective and efficient end-to-end materiel support, the Regulation:</p> <ul style="list-style-type: none"> • Establishes the customer as the foundation driving all materiel management decision-making • Promulgates best business practices in the area of materiel management • Institutes procedures that meet all materiel management statutory requirements
DoD 4160.21-M	Property Requiring Special Processing	Some property, because of its peculiar nature, its potential influence on public health, safety, the environment, security, or private industry, must be disposed of in other than a normal fashion. This

		chapter sets forth those items or categories of property, explains their peculiarities and provides guidance for their disposal. This includes Automated Resources (AR), which refers to any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. The term "AR" includes computers, ancillary equipment, and COTS software.
DoD Instruction 5000.64	Accountability and Management of DoD-Owned Equipment and Other Accountable Property	This Instruction reissues DoD Instruction 5000.64 dated August 13, 2002 to establish accountability and management policy for tangible DoD-owned equipment and other accountable property, in accordance with the authority outlined in DoD Directive 5134.01, dated December 9, 2005. It establishes policy and procedures to comply with Title 40, United States Code, Public Buildings, Property, and Works and Section 901 et seq. of title 31, United States Code; outlines requirements that reflect both the accounting perspective, which supports the documentation of life-cycle events and transactions, and the accountability perspective, which supports the life cycle management of assets. It provides policy and procedures for DoD-owned equipment and other accountable property; assists DoD property managers, accounting and financial managers, and other officials in understanding their roles and responsibilities. It complements the accounting and financial reporting requirements contained in DoD 7000.14-R.
DoD Regulation 7000.14-R Volume 4 Chapter 4	Inventory and Related Property	This chapter prescribes the accounting policy and related requirements necessary to establish financial control over DoD inventory, materials and supplies including stockpile materials.
DoD 8115.01	IT Portfolio Management	This Directive establishes policy and assigns responsibilities for the management of DoD IT investments as portfolios that focus on improving DoD capabilities and mission outcomes.
DoD Instruction 8320.04	IUID Standards for Tangible Personal Property	Establishes the IUID Registry as: <ul style="list-style-type: none"> • The authoritative source of Government unit acquisition cost for items with UII acquired after January 1, 2004, and for UII pedigree data established at delivery • The master data source for Government Furnished Property (GFP) • An authoritative source for establishing the full cost of end-item equipment Establishes the functional framework for IUID as it relates to associated DoD policy and guidance.
DoD Memorandum	Update to policy for Unique Identification (UID) of Tangible Items - New Equipment, Major Modifications, and Re-procurements of Equipment and Spares	This update to the "Policy for Unique Identification (UID) of Tangible Items - New Equipment, Major Modifications, and Re-procurements of Equipment and Spares" dated July 29, 2003, will address clarifications including approval of specific DoD UID equivalents.

MIL STD 130N	DoD Standard Practice Identification Marking Of U.S. Military Property	This standard provides the criteria by which product designers develop specific item identification marking requirements. Product designers must include in product definition data the specific requirements as to marking content, size, location, application process, and any required marking materials that will be part of the deliverable item. Simply stating in the product definition data that the marking be in accordance with this standard is not sufficient for initial design, development and manufacture or subsequent production and procurement of replenishment spare items.
SFFAC	Statement of Federal Accounting Concepts (SFFAC) and Standards	This SFFAC is the fifth in a series of concepts statements intended to set forth objectives and fundamentals on which financial accounting and reporting standards will be based. The objectives identify the goals and purposes of financial reporting. The fundamentals are the underlying concepts of financial accounting-concepts that guide the selection of transactions, events, and circumstances to be accounted for; their recognition and measurement; and the means of summarizing and communicating them to interested parties.
N/A	NSA/CSS Storage Device Declassification Manual	This manual provides instructions and guidance for declassification and disposal of Government media.
SECNAV Instruction 4440.33	Sponsor-Owned Material, Government-Owned Material and Plant and Project Stock Management	Establish USN Sponsor-Owned Material, Government-Owned Material and plant and project stock management policy in accordance with references (a) through (p). This instruction is issued in coordination with the Office of the Deputy Chief of Naval Operations for Fleet Readiness and Logistics (CNO (N4)).
SECNAV Instruction 4440.34	Implementation of Item Unique Identification (IUID) within DON	This instruction promulgates DON policy regarding the UID of tangible items of personal property, equipment, and materiel. This instruction establishes policy and responsibility necessary for implementation and management of IUID within DON.
SECNAV Instruction 5000.36A	DON IT Applications And Data Management	This instruction establishes policy for DON applications and data management and describes the responsibilities of the FAMs, Functional Data Managers and Functional Namespace Coordinators. It also establishes responsibilities for DON IT processes and tools to transform applications and data into net-centric naval capabilities consistent with DoD policy for interoperability and data sharing. Additionally, it describes the relationships between the DON Chief Information Officer, the Assistant Secretaries of the Navy, the Chief of Naval Operations and the Commandant of the Marine Corps for DON applications and data management.
SECNAV Instruction 5230.14	IT Portfolio Management Implementation	This instruction establishes DON policies and procedures for the management of IT and national security systems investments as portfolios across the DON enterprise that focuses on improving DON capabilities and mission outcomes. It also establishes standard operating procedures that leverage the existing decisional processes of Planning, Programming, Budgeting, and Execution (PPBE); Joint Capabilities Integration and Development System, and Defense Acquisition System; to ensure that IT investments are managed collectively as capabilities that yield economies of scope and scale;

		are integrated with the full complement of investment programs in the PPBE process; and, support current strategic guidance and policies.
SECNAV Instruction 5230.15	Information Management/IT Policy For Fielding Of Commercial Off The Shelf (COTS) Software	This instruction provides policy on the fielding and vendor support of COTS software. It is the policy of DON that all COTS software in use across the Department will be vendor supported.
SECNAV Instruction 7320.10A	DON Personal Property Policies and Procedures	Establishes DON policies and procedures for General Fund and Working Capital Fund (WCF) personal property management as delineated in enclosure (1) that meet financial accounting and accountability requirements establishment by DoD Financial Management Regulation (FMR) DoD 7000.14-R, Volume 4, Chapter 6 of Jan 01 and DoD Instruction 5000.64, the Chief Financial Officer's Act of 1990, Statements of Federal Financial Accounting Standards, and applicable DoD guidance.
SECNAV Memorandum	Designation of DADMS as an Authoritative Data Source and DADMS Configuration Control Board Charter	This memo establishes DADMS as the Authoritative Data Source for DON IT and National Security Systems applications and database inventory and IT systems registration. Further, this memo establishes the charter for the DADMS Configuration Control Board to address and prioritize USN and Marine Corps requirements for DADMS.
SECNAV Memorandum	Department of the Navy Strategy for Green Information Technology Electronic Stewardship and Energy Savings Strategy	On January 24, 2007, the President signed reference (a), which established federal goals in the areas of energy efficiency, acquisition, renewable, energy, toxic and hazardous chemical reduction, recycling, sustainable buildings, electronic equipment stewardship, vehicle fuel consumption and water conservation. In addition, reference (a) requires Federal agencies to lead by example in advancing our Nation's energy and sustainability practices. This includes the following provisions: <ul style="list-style-type: none"> • The DON needs to maintain an accurate and up-to-date inventory of information technology devices and the energy specifications of those devices. Accordingly, DON will take all necessary measures to ensure a DON-wide IT automated asset identification process and tools are deployed to maintain an accurate and up-to-date inventory of IT devices, their configurations, and authoritative data • Give preference to acquiring laptops that can be secured and encrypted, which use less than one quarter of the energy of an equivalent computing power desktop computer, when a cost analysis demonstrates no significant increased cost over the four-year life cycle compared to a desktop computer.
DON CIO Message DTG 021419Z FEB 99	DON IT Enterprise-Wide Investment Policy	The purpose of this policy is to ensure that DON speaks with one coordinated voice to suppliers when negotiating for most favorable terms and prices on products and services. The policies in this message apply to any proposed acquisition vehicle or orders under any existing vehicle which provide it products or services including

		NSS, that support and can be used by more than a single claimant (i.e., multi-claimant). Acquisition vehicles and orders under existing vehicles which are negotiated solely in support of a single acquisition category (ACAT) Program are not considered multi-claimant.
DON CIO 221633Z AUG 10	Processing of Magnetic Hard Drive Storage Media for Disposal	This Naval message applies to all DON commands and organizations using classified (collateral only) and unclassified internal and removable magnetic hard drives. This includes, but is not limited to, storage area network devices, servers, workstations, laptops/notebooks, printers, copiers, scanners, and multi-function devices with internal hard drives, removable hard drives and external hard drives. This policy is also applicable to all IT resources with magnetic hard drives, whether it is DON-owned, leased or purchased as a service by DON commands and organizations.
NAVSUP Instruction 4400.100	Stock Readiness	Prescribes instructions for the uniform care of supplies, including the inspection and reporting of condition and serviceability of materiel, and the scheduling, controlling, and reporting of packaging and other cost reimbursable actions in support of depot receiving operations, and uniform care of supplies in storage (COSIS).
NAVSUP P-723	Navy Inventory Integrity Procedures	Navy Inventory Integrity Procedures provide policy, procedure, and performance objectives for maintaining controls over material inventories at USN shore activities and the accuracy of associated inventory item and financial records. The impact of inventory accuracy covers a broad spectrum ranging from readiness to DoD budget credibility. Whenever material on an accountable record cannot be found, readiness is impacted. If the accountable record is overstated, nonexistent assets are applied to requirements. The opportunity for undetected theft is also increased when accountable records do not agree with material in storage. This publication reflects recommendations and changes to streamline and simplify the physical inventory process to better employ physical inventory resources in maintaining higher levels of inventory accuracy.
MCO P10150.1	Garrison Property Policy Manual	This Manual prescribes the policy and procedures governing the acquisition, management, and control of garrison property used at Marine Corps bases, air stations, districts, and other independent commands. The information contained in this Manual reflects the current policy in effect to achieve the DoD objective to improve property management. This Manual does not supersede but complements policy in supply and fiscal matters related to garrison property. This document incorporates all applicable Public Laws and Federal Property Management Regulations and consolidates the policy and procedures for Marine Corps garrison property management into a single document. Garrison property is all Government personal property used to support the operation of a Marine Corps installation and its tenant activities.
DON CIO 221633Z AUG 10	Processing of Magnetic Hard Drive Storage Media for Disposal	This Naval message applies to all DON commands and organizations using classified (collateral only) and unclassified internal and removable magnetic hard drives. This includes, but is not limited to,

		storage area network devices, servers, workstations, laptops/notebooks, printers, copiers, scanners, and multi-function devices with internal hard drives, removable hard drives and external hard drives. This policy is also applicable to all IT resources with magnetic hard drives, whether it is DON-owned, leased or purchased as a service by DON commands and organizations.
NAVSUP Instruction 4400.100	Stock Readiness	Prescribes instructions for the uniform care of supplies, including the inspection and reporting of condition and serviceability of materiel, and the scheduling, controlling, and reporting of packaging and other cost reimbursable actions in support of depot receiving operations, and uniform care of supplies in storage (COSIS).
NAVSUP P-723	Navy Inventory Integrity Procedures	Navy Inventory Integrity Procedures provide policy, procedure, and performance objectives for maintaining controls over material inventories at USN shore activities and the accuracy of associated inventory item and financial records. The impact of inventory accuracy covers a broad spectrum ranging from readiness to DoD budget credibility. Whenever material on an accountable record cannot be found, readiness is impacted. If the accountable record is overstated, nonexistent assets are applied to requirements. The opportunity for undetected theft is also increased when accountable records do not agree with material in storage. This publication reflects recommendations and changes to streamline and simplify the physical inventory process to better employ physical inventory resources in maintaining higher levels of inventory accuracy.
MCO P10150.1	Garrison Property Policy Manual	This Manual prescribes the policy and procedures governing the acquisition, management, and control of garrison property used at Marine Corps bases, air stations, districts, and other independent commands. The information contained in this Manual reflects the current policy in effect to achieve the DoD objective to improve property management. This Manual does not supersede but complements policy in supply and fiscal matters related to garrison property. This document incorporates all applicable Public Laws and Federal Property Management Regulations and consolidates the policy and procedures for Marine Corps garrison property management into a single document. Garrison property is all Government personal property used to support the operation of a Marine Corps installation and its tenant activities.

6.2.2 Process-Specific Policies

This section defines the specific policies developed to govern the ITAM process for NGEN.

Policy #	Policy Name	Requirement
----------	-------------	-------------

N/A	DON ITAM Implementation Plan	The purpose of this document is to provide the requirements, concept of operations, and plan of action to implement objective 5.4 of Goal 5 of the DON Information Management/ Information Technology (IM/IT) Strategic Plan (Mid-cycle update to the plan for 2009). Goal 5 of the DON IM/IT Strategic Plan is to “Ensure naval IM/IT investments are selected, resourced, and acquired to deliver affordable enhancements to warfighter effectiveness.” Objective 5.4 is to “Implement a DON-wide ITAM process that builds on the FAM governance structure, meets the ITAM requirements of DON and President’s Management Agenda, and efficiently utilizes the IM/IT Enterprise Agreements to acquire products and services.”
N/A	NGEN AMP	The NGEN Asset Management Plan (AMP)defines and provides guidance for establishing NGEN ITAM program, as directed by under the NEN Program Office. This document provides the ITAM Process Framework, high level NGEN goals and objectives and describes the overall structure for managing USN and Marine Corps assets.
N/A	NGEN Block 1, Increment 1 System Design Specification	This version of the NGEN SDS provides high-level, system functional requirements and performance characteristics for NGEN Block 1, Increment 1. This document is, in fact, a snapshot in time of the program's specifications for services, IF, and architecture to include a description of NGEN's intended service delivery model which is based upon an IT IF Library (ITIL) / ITSM framework. This snapshot does not propose or describe either acquisition or contracting methods for provisioning or resourcing the NGEN services. Future iterations of this System Design Specification will document detailed design efforts as well as alignment of NGEN's services, IF and service delivery model with a maturing acquisition strategy. The NGEN IT Services described in this document represent NGEN's Functional Baseline, while the IF described represents the framework for NGEN's Allocated Baseline. Remaining engineering work supporting NGEN's Systems Engineering process entails the further development of the Allocated Baseline and the mapping and/or development of NGEN's Product Baseline.

6.3 Process Outcomes

The key qualitative and quantitative outcomes (objectives) of the Process are:

- Existing investments in hardware, software and licenses are utilized
- Ensured compliance with DoD and DON standards, requirements and enterprise architecture
- Full control of all NGEN assets throughout their life cycle
- Accurate financial information for NGEN assets
- Reduction in unnecessary or duplicate spending

NGEN assets are available at the right time for deployment

Transparency into Total Cost of Ownership and Return on Investment

6.4 Process Scope

This document includes the high level asset management process activities performed by the current service provider - Hewlett Packard Enterprise Services within CoSC. Government touch points with HP Enterprise Services are identified within the asset management process activities. These touch points are interfaces between Government and HP Enterprise Services operational staff and provide the Government with an increased level of command and control (C2). The information provided was gathered from multiple C2 summit meetings with the HP Enterprise Services' Asset Management and Configuration Management Teams. Additional information and details will be obtained from HP Enterprise Services during follow up C2 sessions. This document will be updated as new asset management information is obtained.

6.4.1 Includes

- Management of end user IT assets such as desktops, laptops and printers
- Management of all IT infrastructure related software & hardware such as data storage, enterprise messaging, application hosting, directory, and electronic SW distribution. This also includes IT assets used in support of the local area network (LAN), base area network (BAN), wide area network (WAN), point of presence, pier side connectivity, security boundaries.
- Management of licenses, to include software license and end user agreement compliance
- Management of asset leasing and maintenance (includes maintenance price and renewal dates)
- Management of physical inventory and attribute specifications
- Management of asset availability to fulfill approved requests
- Management of logistical data, to include physical location, transportation information and storage of assets
- Asset retirement/disposal
- Track ownership of assets by means of an IUID Tag
- Financial history of assets, to include amounts for purchase, depreciation and disposal
- Management of IT Asset warranty information

6.4.2 Excludes

- Risk Management

- Procurement
- Relations between assets -included within the Configuration Management process
- Physical security of assets
- Real Property (building and land)
- Site Improvements – building related materials (e.g. partition walls, raised flooring, dropped ceilings, interior finishes, lighting, mechanical and electrical systems and components, server farm support equipment, computer room cooling units, condensers, Heating, Ventilation, & Air Conditioning units, Power Distribution Units , Uninterruptible Power Supplies, fire protection systems, and security systems).
- Inside Cable Plant (ISP) – cabling and associated patch panels and pathway materials that connect intelligent network devices within a building or server farm. ISP may be fiber-optic or copper cable. There are three major categories of ISP assets: Seat Drops, Fiber Ties, and Server Farm Cabling.
- Outside Cable Plant (OSP) – fiber-optic and copper cabling that connects intelligent network devices between different buildings, including server farms.
- Access security of assets
- Change Management – included within the Change Management process
- Financial Management

6.5 Process Interfaces

This section summarizes the interfaces between the HP Enterprise Services Asset Management Process and other ITSM processes. A direct interface occurs when a process provides a work product (input or output) to another process.

The following diagram graphically depicts notional process interface relationships and work products with the HP Enterprise Services Asset Management Process. These process interfaces will need to be validated with HP Enterprise Services. Once validated, the following format is to be used:

- <Name of Interfacing Process> + additional description of the interface if required
 - Detailed description of work product(s) if required

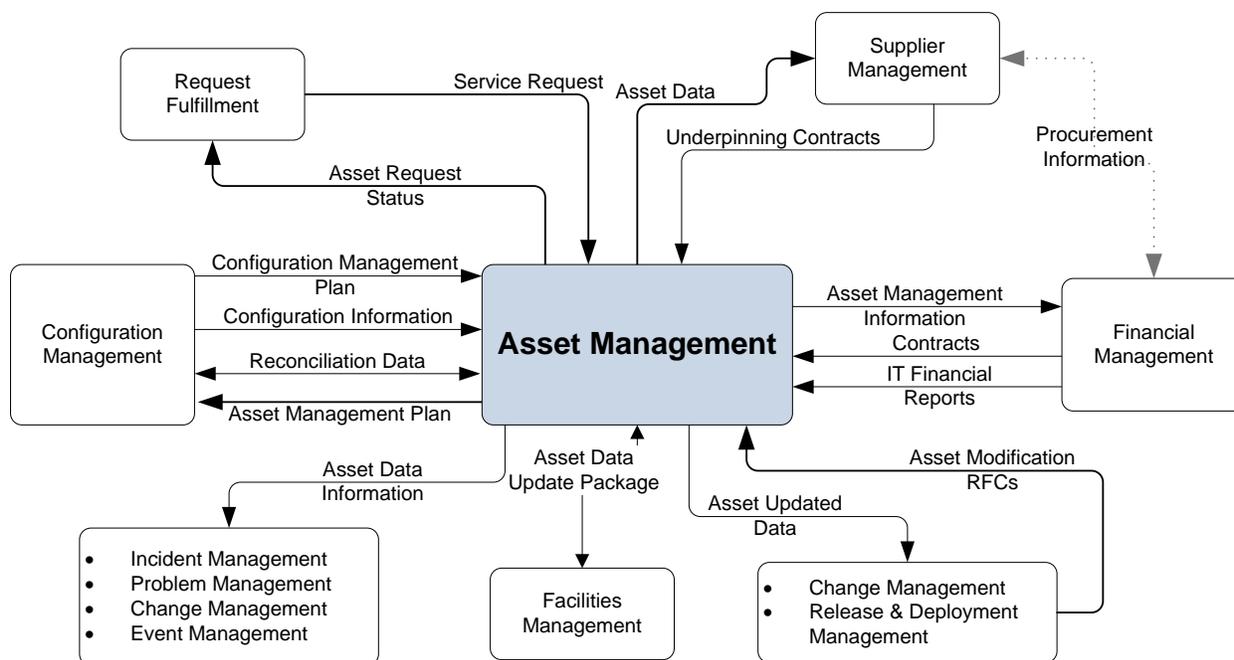


Figure 1: IT Asset Management Process Interface Diagram

6.6 Process Functional Requirements

Technical ITAM functions will be guided by the NGEN Service Delivery Strategy (SDS) and Capability Production Document, and as a component of a larger, integrated COTS ITSM tool or suite of tools. The AM System must include the following minimum core capabilities: automated asset discovery, life cycle status and refresh tracking, asset relationship mapping, asset cost tracking and management (to include actual IT assets, maintenance and warranties), SW license and compliance management, and auditing/alerting – all of which share data across a common, normalized CMS that enables robust reporting (to include dashboards, analytical drilldown and ad-hoc capabilities).

The following table outlines the high-level categories of requirements for the AM System capability, which include Asset Tracking, Discovery Operations, SW License Management, Financial Management, Policy, Program Management, Integration Reporting and Security. Each category is further defined into specific, measurable capability requirements within the NGEN ITAM Functional System Requirements – Appendix E.

ID	Date Recorded	Functional Area	Requirement
1.0	03/22/2011	Logistics	Category: IT Asset Tracking IT Asset Tracking accounts for all IT HW and SW assets (online and offline) within the NGEN environment, throughout the asset life cycle – this includes situational awareness of assets and accountability per DoD and SECNAV instruction. Accordingly, the AM System must track assets via a CMS that

			provides integration with other ITSM tool modules and enterprise IT management tools. The CMS must enable physical inventory and UII tracking and also provide visibility of asset statuses and asset relationships (such as showing SW that is installed on a particular asset or CI). All asset tracking data in the CMS must be reconciled and made available to report on asset inventory and distribution, license allocation and IT asset utilization, enabling DON IT decision-makers to form better resource and security related business decisions. Additionally, asset tracking must include a bar coding capability, enabling proper receiving processes, adherence to DoD policy and physical inventory scanning.
2.0	03/22/2011	DA/TA	<p>Category: Discovery Operations</p> <p>Discovery Operations establishes rules for automating the collection of data for online IT assets and establishes a baseline that will be used to discover additions, deletions and use of IT assets. Dynamic updates from the discovery tool to the CMS supports minimized human administration associated with ITAM. The discovery tool must transmit all asset data to the CMS, where it will then be reconciled and linked to other asset data (such as data that is entered manually). The tool must poll all devices on a regular basis to maintain accuracy. Examples of the types of data include:</p> <ul style="list-style-type: none"> • Machine identification (such as serial number, media access control [MAC] address, internet protocol [IP], physical location) • Device OSs and types (such as servers, desktops, printers, routers, IP-enabled devices) • System configuration data (such as central processing unit [CPU], memory, disk capacity) • Installed SW • Identification of rogue devices
3.0	03/22/2011	Logistics	<p>Category: Software License Management</p> <p>SW License Management describes rules and standards for COTS and GOTS application management. This includes differentiating between COTS and GOTS applications, license contract terms, usage, available license inventory, provisioning to HW and/or users and entitlements within the AM System. Additionally, the system should capitalize on Discovery Operations to identify the exact number of SW instances on the network, as reconciled against authorized entitlements and available inventory.</p>
4.0	03/22/2011	PM	<p>Category: Financial Management</p> <p>Financial Management includes the processes, standards and business rules for recording network investment, operations and support costs. Specific to ITAM, the system must enable recording of HW and SW asset cost and budgetary data in the system at the time of procurement, with standardized depreciation calculation over the asset life cycle. Additionally, the AM system should have the capability to track maintenance and warranty contract information for each asset under contract.</p>
5.0	03/22/2011	PM	<p>Category: Policy</p> <p>All ITAM-specific tool Policy requirements are aligned to the policies outlined in the NGEN Asset Management Plan Appendix B – Governing Policies.</p>

			Additionally, the ITAM tool must adhere to DoD and DON IA policies as outlined by the 8500.1 and 8500.2 IA controls.
6.0	03/22/2011	PM NetOps Logistics	Category: Reporting Reporting requirements establish automated reporting standards for all IT asset data in accordance with defined data elements and metrics as outlined in Sections 1.18. Additionally, reporting capabilities should support out-of-the-box, custom, dashboard and ad-hoc reporting that allows for analyses regarding trends, anomalies and projections.
7.0	03/22/2011	Data ITSM DA/TA	Category: Integration Integration requirements ensure future data integration and interface between the AM System and external systems in order to satisfy DoD and DON requirements are supported – such as asset accountability within DPAS, the IUID Registry and DON Functional Area Manager (FAM) compliance within DADMS and Financial Management within Navy ERP system. Additionally, integration must support an SOA model.
8.0	03/22/2011	IA	Category: Security Security requirements are necessary for planning and developing the system concept of operations and minimizing potential threats to the AM System. All DON asset data will be stored in an approved, certified, and accredited AM System, in accordance with appropriate Government security classification guidelines. The AM System must be Public Key IF enabled for Common Access Card user authentication and must support role-based access. Additionally, the system must adhere to DoD and DON IA policies as outlined by the 8500.1 and 8500.2 IA controls.

6.7 Process Activities

6.7.1 Process Diagram

This section defines the high level process activities in a standardized swim lane format (the process model should always be aligned to the current version of the NNPDM document): In the current CoSC environment, asset management activities are performed by multiple HP Enterprise Services organizations in their daily operational tasks. These asset management tasks are identified as part of the High Level CLIN Delivery process and are combined as part of other processes such as Request Fulfillment, Seat Delivery, and Acquisition. Only asset management related process activities and touch points are identified within this document.

The following diagram displays the HP Enterprise Services high level process activities, the Government’s high level IT Asset Management (ITAM) process activities, US Navy C2 touch points and the various tools used to support asset management within CoSC. The Government’s high level ITAM process activities are also known as the NGEN ITAM Process Framework. Government C2 touch points are depicted by this diagram shape:

AM 1
 USN

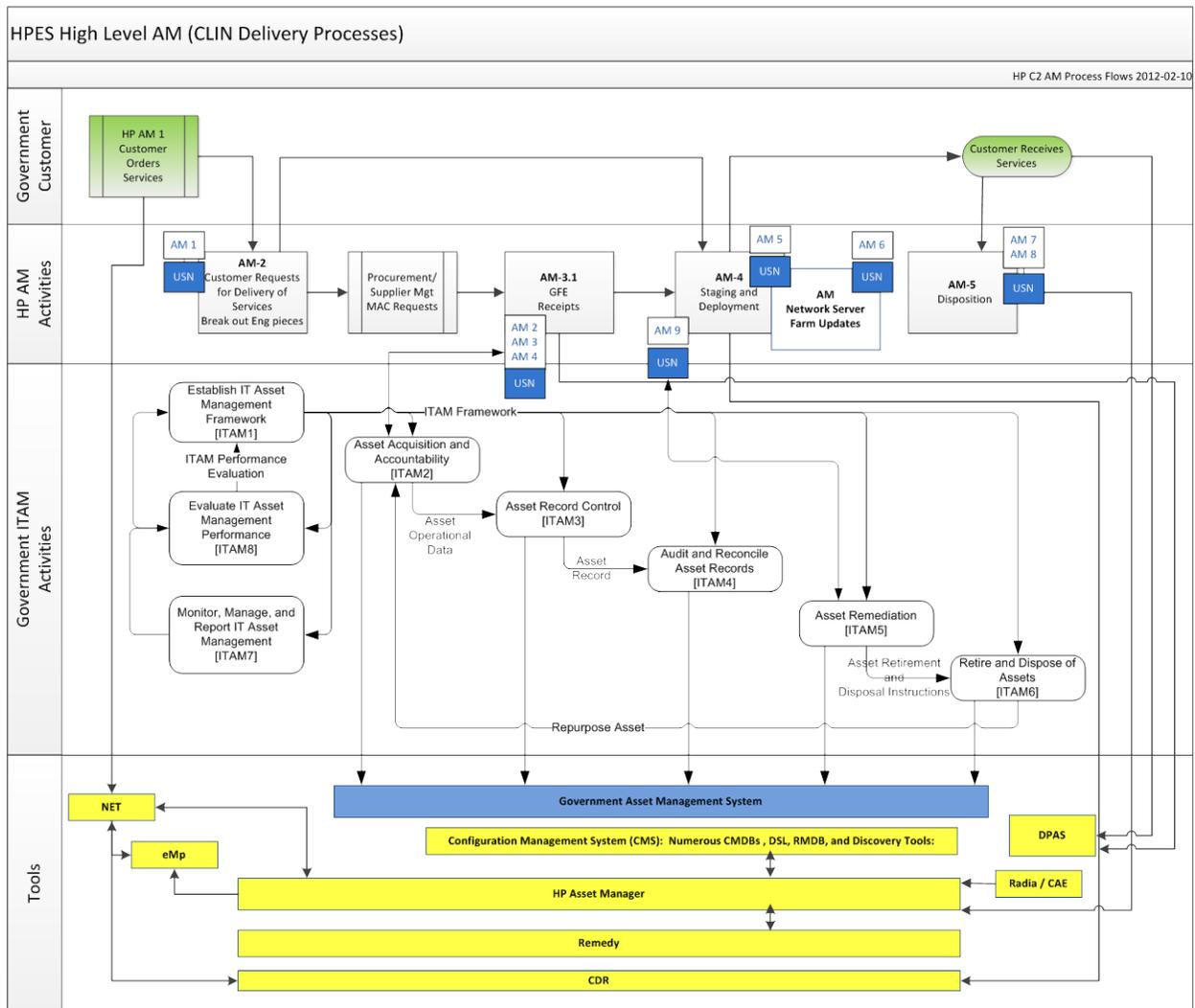


Figure 2: IT Asset Management Lifecycle

*Note: Additional guidance on creating the Process Diagram is provided in Appendix C.

6.7.2 Process Activity Descriptions

This section defines the details of each activity in the process model. Not all activity details are known at this time. Additional information on these HP Enterprise Services Asset Management Activities will be determined during further C2 process discovery sessions with HP Enterprise Services.

AM-1 Customer Orders Services	
Description:	The first HP Enterprise Services Activity, Customer Orders Services, is initiated when a customer orders a service via the Government Customer Technical Representative (CTR). A customer service order triggers asset management to add a new asset record.
Supplier:	<ul style="list-style-type: none"> • CTR • ACTR
Inputs:	<ul style="list-style-type: none"> • TBD
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? No <ul style="list-style-type: none"> • TBD
Outputs:	<ul style="list-style-type: none"> • Service Request
Customer:	<ul style="list-style-type: none"> • HP Enterprise Services Request Fulfillment Process • HP Enterprise Services Asset Management Process
Assumptions:	<ul style="list-style-type: none"> • TBD

AM-2 Customer Requests for Delivery of Services	
Description:	In this activity, HP Enterprise Services processes the Government's request for services (ITIL – Request Fulfillment process). Different processes and tools are used to support various service requests such as Seat Orders, Technology Refresh, and Move Add Change (MAC) requests. These service requests are outside the scope of the Asset Management process but trigger the start of the Asset Management

		process.
Supplier:		<ul style="list-style-type: none"> TBD
Inputs:		<ul style="list-style-type: none"> Electronic notification of an order via the Government's order placement tool – NET.
Standard Operating Procedures (SOPs):		SOPs Exist for This Activity? No <ul style="list-style-type: none"> TBD
Outputs:		<ul style="list-style-type: none">
Customer:		<ul style="list-style-type: none"> TBD
Assumptions:		<ul style="list-style-type: none"> Post delivery meeting may be held with a Government representative to ensure order accuracy.

AM-3.1	GFE Receipts	
Description:		HP Enterprise Services Delivers Government Furnished Equipment (GFE) to the Government. These GFE assets were purchased from HP Enterprise Services through the CoSC contract.
Supplier:		<ul style="list-style-type: none"> The HP Enterprise Services eMarketplace (eMp) tool HP Enterprise Services Warehouse Manager
Inputs:		<ul style="list-style-type: none"> Ordered CLIN Report
Standard Operating Procedures (SOPs):		SOPs Exist for This Activity? No <ul style="list-style-type: none"> TBD
Outputs:		<ul style="list-style-type: none"> DD250 DD1149
Customer:		<ul style="list-style-type: none"> Logistics ITAM Process Manager assisted by on-site NAVSISA support

	Assumptions:	<ul style="list-style-type: none"> TBD
AM-4	Staging and Deployment and Network Server Farm Updates	
	Description:	Within these activities assets are prepared for delivery to the Government end-user or placed into service to support network transport services or the various server farms.
	Supplier:	<ul style="list-style-type: none"> HP Enterprise Services Warehouse Manager CTR/ACTR
	Inputs:	<ul style="list-style-type: none"> “Shipping” DD1149 Asset Record Discrepancies
	Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? No <ul style="list-style-type: none"> TBD
	Outputs:	<ul style="list-style-type: none"> HP Enterprise Services Signed “shipping” DD250 Reconciliation Report
	Customer:	<ul style="list-style-type: none"> Logistics ITAM Process Manager Government ITAM Data Analyst HP Enterprise Services Asset Management SME
	Assumptions:	<ul style="list-style-type: none"> TBD

AM-5	Disposition	
	Description:	Within this activity HP Enterprise Services prepares end-of-life assets for disposal
	Supplier:	<ul style="list-style-type: none"> TBD
	Inputs:	<ul style="list-style-type: none"> Modified Service Record
	Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? No <ul style="list-style-type: none"> TBD

Outputs:	<ul style="list-style-type: none"> Updated Service Record
Customer:	<ul style="list-style-type: none"> Logistics ITAM Process Manager Government ITAM Data Analyst
Assumptions:	<ul style="list-style-type: none"> CTRs are notifying HP Enterprise Services of inaccurate asset record data. This touch point (reconciliation) is currently being refined by HP Enterprise Services

ORGANIZATION AND ROLES

6.8 Roles and Organizations

This section defines the roles (e.g. Process Owner, Process Manager, Analyst, etc.) and functional organizations (e.g. DA/TA, Logistics, NetOps, etc.) involved in executing the process.

Role	Responsibility
ITAM Process Owner	<p>The Process Owner is the sponsor of the process, and holds the responsibility and executive authority for the overall process results across the enterprise. This authority spans across all internal and external organizations across the NEN Program who participate in the process.</p> <p>The Process Owner is responsible for ensuring that the process is fit-for-purpose and that all activities defined within the process are undertaken. This responsibility includes oversight of process quality, continual improvement, and compliance with Federal, DoD, DON and NGEN organizational mandates and performance targets.</p> <p>The Process Owner is vested with ultimate authority over all aspects of process design, change management, performance metrics, policies, and process automation technologies to ensure compliance with organizational objectives. PMW 205 will staff this role.</p>

Contractor Technical Representative (CTR)	The Contractor Technical Representative (CTR) is the liaison between the network contractor and the end user, and is responsible for ordering services, accounts, and applications in the current environment. CTRs perform many additional duties such as end-user support, technical support, infrastructure and legacy network support, seat refresh, and emergent request duties. The CTR/ACTR workforce is composed of approximately 1700 military, civilian, and contractor fulltime equivalents (FTEs) that perform a myriad of duties in support of the NMCI end-users.
--	---

6.9 R/A/C/I

This section contains a process-level RACI chart that shows the relationship between the activities and roles within the organization.

Processes may span departmental boundaries; therefore, procedures and work instructions within the process need to be mapped to roles within the process. These roles are then mapped to job functions, IT staff and departments. The Process Owner is accountable for ensuring process interaction by implementing systems that allow smooth process flow.

The Responsible, Accountable, Consulted, Informed (RACI) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks. Listed below are the roles that have been identified in the process.

R (Responsible) – A Responsible organization is involved in the daily execution of process activities. There may be more than one organization responsible for a given activity. Designating an organization as “Responsible” implies that they fall under the guidance and review of the “Accountable” party. Responsible organizations may or may not be organizationally aligned under the Accountable organization.

A (Accountable) – An Accountable organization serves as the overall owner of process quality and end results. There should only be one Accountable organization per process activity.

C (Consulted) – A Consulted organization provides knowledge and/or information to an activity. These organizations function as “part-time” actors in the process by contributing to specific situations, providing insight to others, performing very clear tasks, etc.

I (Informed) – An Informed organization receives specific information about process execution, status, etc.

Process Activities	Service Provider (HP Enterprise Services)	PMW-205 (Logistics ITAM Process Owner)	Customer (Service Recipient)	Contractor Technical Representative (Approves and Orders Service)
HP AM 1: Customer Orders Services	I	I	R/C	A/R
HP AM 2: Customer Requests for Delivery of Services	R	n/a	I	A/R
HP AM 3.1: GFE Receipts	A/R	R	I	I
HP AM 4: Staging and Deployment	A/R	R	I	R
HP AM 5: Disposition	A/R	I	n/a	R

6.10 Resource Requirements

6.10.1 Resources Required to Execute the Process

This information is unknown at this time and will be determined prior to transition to the NGEN Contract.

6.10.2 Knowledge, Skills and Abilities (KSAs)

This information is unknown at this time and will be determined prior to transition to the NGEN Contract.

6.10.3 Identification and Training of Government Personnel

This information is unknown at this time and will be determined prior to transition to the NGEN Contract.

DATA AND INFORMATION

6.11 Data and Information Requirements

This section summarizes the data and information management requirements of the process, and identifies the key consumers (e.g. roles, organizations) of process information work products.

6.12 Information Work Products (IWP)

This section details the process IWPs including their usage and target audience. IWPs will be used either internally within the process which generated them, or by another process which receives the work product. IWPs will contribute to the Command and Control (C2) analysis and decisions used in managing the process:

IWP	Target Audience	Description/Usage
TBD	TBD	This information is unknown at this time and will be determined prior to transition to the NGEN Contract.

6.13 Reporting Requirements

Detailed reporting requirements can be found in Appendix E – ITAM Functional System Requirements under Category 6 – Reporting.

During CoSC HP Enterprise Services is required to provide asset reporting via CDRL 5.7-1. NGEN Asset Management CDRL 5.7-1 defines the report elements in the following table.

Report Elements	Amplifying Information
Report Name	Supplemental Asset Report
Report Description	TDB
Report Audience	PMW-205 Logistics
Report Owner	HP Enterprise Services
CSFs In Report	TDB
KPIs/Metrics Used In Report	TDB
Report Frequency	Monthly

PERFORMANCE MANAGEMENT

6.14 Current Process Metrics

This section lists the Critical Success Factors (CSFs) and Key Performance Indicators (KPIs) used to baseline and measure process transition success.

Effective day-to-day operation and long-term management of the process requires measuring the process. Reports must be defined, produced and distributed to enable the management of process-related issues and initiatives. Daily performance management occurs with the process manager. Long-term trending analysis and management of significant process activities occurs at the process owner.

A powerful vision and well-defined mission statement are critical to defining enterprise goals and objectives. Process governance starts with establishing objectives for the enterprise, and continuous performance management aids direction of activities aligned with those set objectives. The Process Owner is responsible for measuring and providing value-based reporting. Critical Success Factors (CSFs) identify the most important actions for achieving control over the process and Key Performance Indicators (KPIs) measure whether or not a control is meeting its objective.

Continual service improvement depends on accurate and timely process measurements and relies on obtaining, analyzing, and using information that is practical and meaningful to the process. Measurements of process efficiency and effectiveness enable NGEN management to track process performance and improve overall end-user satisfaction.

The following table summarizes the relationships between process CSFs and KPIs. See Appendix D for a complete list of CSFs and KPIs.

CSFs and supporting KPIs are currently not defined for HP Enterprise Services Asset Management process activities within CoSC.

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	TBD	1	TBD
		2	TBD
		3	TBD
		4	TBD
		5	TBD

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
		6	TBD
		7	TBD
2	TBD		TBD
			TBD
			TBD
			TBD

*Note: Additional metric details incl. threshold and objective values are defined in the SOPs.

6.15 Desired Metrics and Compliance Controls

This section provides a narrative description of additional metrics and compliance controls applicable to the process, but not currently in place to support Transition.

TBD

TOOLS AND TECHNOLOGY

6.16 Tool Requirements

This section defines key tool automation capability, interface, and interoperability requirements. Detailed Asset Management tool requirements can be found in Appendix E – NGEN ITAM Functional System Requirements.

Requirement	Process Activity
TBD	TBD

6.17 Tools Used to Support the Process

This section defines the requirements met by COSC tools today and documents key gaps:

Requirement	COSC Tool Used Today	Measurement	Gap	Recommendation
TBD	TBD	TBD	TBD	TBD

INTEGRATION AND VALIDATION

6.18 Interface Requirements

This section defines the key interfaces with other processes, tools, governance bodies, and resources (service owners, vendors):

Interface ID	Interface Description
--------------	-----------------------

1	TBD
----------	------------

6.19 Integration Approach

The Asset Management Process Integration Activity (PIA) has not been performed at this time. PIA for asset management will be performed as part of the Government Operational Readiness activities prior to transition to the NGEN contract.

6.19.1 Use Case Selection

Use cases have not been developed and are still TBD.

6.19.2 Workshops and Simulations

TBD

6.20 Validation Results and Remediation

TBD

Error ID	Validation Scenario	Step Description	Type of Error Found	Error Description
		TBD	TBD	TBD

7. DATA MANAGEMENT [DAT]

7.1 Purpose

The purpose of Data Management is to identify the data needed to design, build, deploy, operate and sustain the network and ensure the data is accounted for, inventoried, and effectively managed and protected from creation to final disposition. The incumbent's digital data environment is utilized to manage, maintain and grant access to all data. Data Management also provides Government objectives and requirements to be applied in establishing the processes, procedures, tools and roles that will be necessary to effectively create, capture, validate, maintain, and appropriately share information ensuring it is available when needed, where needed and that it is retained as a reusable asset to support successor contracts.

The data and information required to support the NMCI network is extensive; consisting of data feeds between systems, architectural specifications, technical configurations, drawings, diagrams, and other operational data that is dynamic in nature. The DM process currently identifies the data needed to design, build, deploy, operate and sustain the network and ensures the data is accounted for, inventoried, and shared with the Government as per the Continuity of Services Contract (CoSC) Attachment 4. CoSC Attachment 4 outlines the requirements for the incumbent to enable the Government to access, inspect, accept, direct remediation of, and eventually, accept delivery of all data developed for NMCI. Data within the scope of the NMCI IP License includes any technical data, processes, procedures, or software developed in support of the NMCI network. This license does not include incumbent contractor financial data, third party agreements, personnel information, or contractor proprietary data, such as commercial software developed at the corporate level, not in support of the NMCI network.

The Objectives of Data Management are:

- Establish authoritative data source and ensure the quality of the data within
- Inventory, protect, and control data assets
- Ensure data assets available to the appropriate audiences in a timely manner
- Accept Delivery of all NMCI TDPP to ensure it is available to enable Network operations as well as future contracts, and

- Develop standard, repeatable processes and procedures for data management.

7.2 Process Policies

7.2.1 DoD and DON Policies

This section defines the key DoD and DON Policies that govern the process. Only list the key policies that impact how a process is designed and managed, especially in regards to process control and audit requirements. For example, the MIL-HDBK describes policies that govern Configuration Management; DoD5000 does not.

Policy #	Policy Name	Requirement
DoDI 5000.02	Operation of the Defense Acquisition System	<ul style="list-style-type: none"> • Mandates that the NEN PM assess the long-term technical data needs of the program and develop a Data Management Strategy that assesses the data required to design, manufacture and sustain the system as well as support re-competition for production, sustainment or upgrades.
DoDI 8320.02	Data Sharing in a Net-Centric Department of Defense	<ul style="list-style-type: none"> • Directs the use of resources to implement data sharing among information capabilities, services, processes and personnel interconnected within the Global Information Grid (GIG)
NGEN Requirements Document v2.0 6.9.2.1	Establishment of an NGEN knowledge repository	<ul style="list-style-type: none"> • Under the section covering System Capabilities and Governance the NGEN requirements document directs that the program will have a knowledge repository where the organization's collective information can be stored, searched, used and updated.
DoD Directive 8500.1-E	Information Assurance (IA)	<ul style="list-style-type: none"> • Establishes policy and assigns responsibilities to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.
DoD Directive 8500.2	IA Implementation	<ul style="list-style-type: none"> • Implements policy, assigns responsibilities, and prescribes procedures for applying integrated,

		layered protection of the DoD information systems and networks.
252.227-7013	Rights in Technical Data-Noncommercial Items	<ul style="list-style-type: none"> Provides guidelines for rights in technical data on non-commercial items.
27.401	Rights in Data and Copyrights	<ul style="list-style-type: none"> Defines policies and procedures regarding rights in data and copyrights, and acquisition of data.
46	Quality Assurance	<ul style="list-style-type: none"> FAR 46 prescribes policies and procedures to ensure that supplies and services acquired under Government contract conform to the contract's quality and quantity requirements. Included are inspection, acceptance, warranty, and other measures associated with quality requirements.
52.227	Authorization and Consent	<ul style="list-style-type: none"> Defines patent rights in Government contracts and the conditions under which the Government may obtain title or rights.
	Discovery Metadata Specifications (DDMS)	<ul style="list-style-type: none"> The DoD Discovery Metadata Specification (DDMS) defines discovery metadata elements for resources posted to community and organizational shared spaces.

7.2.2 Process-Specific Policies

This section defines the specific policies developed to govern the process for NGEN.

Policy #	Policy Name	Requirement
CoSC Attachment 4 Delivery / Transition of NMCI IP section 1.8.4	Delivery of Intellectual Property	<ul style="list-style-type: none"> CoSC Attachment 4 defines the requirements for Government Access, virtualization, Inspection, Acceptance, and Remediation, as well as Training related to NMCI TDPP. As services transition from incumbent to successor, a copy of all licensed NMCI TDPP relating to transitioned services is delivered to the

		Government. At that point, accountability for maintaining and controlling the acquired TDPP also transfers to the Government/successor.
CoSC Section H-8 IP License Agreement		<ul style="list-style-type: none"> The IP License Agreement defines the terms, conditions, and rights the Government has to the licensed NMCI TDPP.

7.3 Process Outcomes

The key qualitative and quantitative outcomes (objectives) of the Process are:

- Appropriate access to usable data when needed and where needed
- Standard data lifecycle management policies and governance that enable data integration and sharing
- Appropriate tagging of data to enable discovery and effective use of data
- Compliance with legal, regulatory, and operational requirements for data privacy, quality, and retention
- Ensuring that accessibility, performance, cost, and value of data are established, managed and optimized throughout the full life cycle

7.4 Process Scope

The scope of the Data Management process encompasses the full life cycle of both externally acquired and enterprise generated data, as well as information about that data (metadata). Data imported into the environment from external sources is verified and validated, ensuring its usefulness and fitness for purpose, before importing into enterprise data stores. Policies and processes are implemented to ensure data integrity and accountability in the event of adverse events occurring as a result of inaccurate or untrustworthy data.

7.4.1 Includes

Data Management includes all aspects of data from creation to disposal.

- Managing data as an asset, or set of assets, and planning for its use in the enterprise
- Cataloging and controlling all data types used by the enterprise to design, build, deploy, operate and sustain IT services

- Accepting, cataloging, and controlling imported or generated data
- Processes, procedures and technology sufficient to restore data to a defined previous state
- Planning and control of data placement, retention, and disposal where applicable
- Data protection and security adhering to DoD/DON policies pertaining to data storage

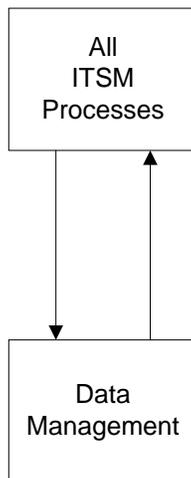
7.4.2 Excludes

- Personally Identifiable Information (PII)
- Records management
- Personnel files

7.5 Process Interfaces

This section summarizes the interfaces between the process and other ITSM processes. A direct interface occurs when a process provides a work product (input or output) to another process.

DM activities are an integral part of most if not all ITSM processes. This dependency requires ITSM processes to integrate data management principles within their processes. It also requires that DM establish standards, common practices and shared data repositories to support data inputs and outputs that result from ITSM activities.



Data Management Dependencies with Other ITSM Processes

7.6 Process Functional Requirements

This section defines all of the NGEN Functional Area Requirements applicable to the process in a requirements traceability matrix (RTM).

ID	Date	Functional Area	Requirement
----	------	-----------------	-------------

	Recorded		
			TBD

7.7 Process Activities

7.7.1 Process Diagram

This section defines the high level process activities in a standardized swim lane format (the process diagram should always be identical to the current version of the NPDM document):

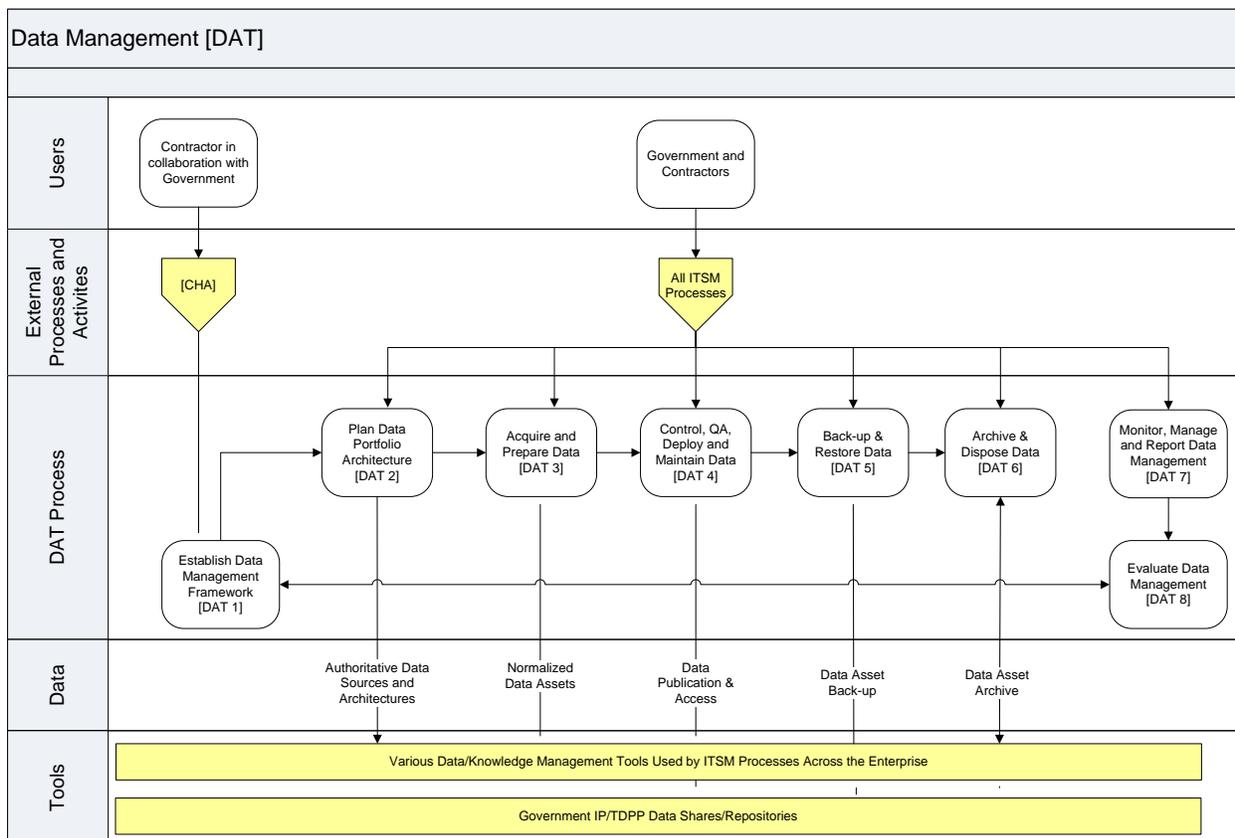


Figure 30 – DAT Data Management Life Cycle

7.7.2 Process Activity Descriptions

This section defines the details of each activity in the process model:

DAT1 Establish Data Management Framework	
Description:	Specify process purpose, goals, scope and capabilities of Data Management
Supplier:	<ul style="list-style-type: none"> • PM NEN DM Manager • PM NEN DM Owner • PM NEN Contractors and • PM NEN Stakeholders
Inputs:	<ul style="list-style-type: none"> • CoSC Attachment 4 • CDRL IP 002 • IP Inventory Business Rules • NMCI IP Access Plan • DoDI 5000.2 • DDMS • DoDI 8320.02
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • DAT_Establishing_Process_Framework_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • Scope, Objectives, Goals, Purpose, Capabilities • Roles and Responsibilities • Processes and Procedures • Measurements and Controls • Tool Requirements / Gap Analysis • Training and Communications
Customer:	All PM NEN data owners, authors, editors, users
Assumptions:	<ul style="list-style-type: none"> • Establishing the framework is a collaborative effort between the Government and Contractor • The Government will approve the final framework prior to implementation

	<ul style="list-style-type: none"> The Framework will adopted by all Government and Contractor personnel to achieve standardization and quality objectives
--	---

DAT2		Plan Data Portfolio Architecture
Description:	The data portfolio architecture includes the gathering of requirements for data repositories, structures, standards, formats and guidance that is required to achieve standard DAT process operations across the enterprise. The Government provided guidance and standards for taxonomy; metadata and quality apply to all NEN data.	
Supplier:	<ul style="list-style-type: none"> Incumbent Contractor PM NEN Data Manager 	
Inputs:	<ul style="list-style-type: none"> Data architectures, formats and standards Technology and tools managing program data Government requirements for standardization and normalization of data 	
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> DAT_Plan_Portfolio_Architecture_SOP_v1.0 	
Outputs:	<ul style="list-style-type: none"> Data Management Plan NGEN Metadata Guide IP Inventory Business Rules CoSC CDRL IP002 	
Customer:	<ul style="list-style-type: none"> Incumbent Contractor All PM NEN data owners, authors, editors, users 	
Assumptions:	<ul style="list-style-type: none"> Establishing the architecture and standards is a collaborative effort between the Government and Contractor The Government will approve the final architecture and standards prior to implementation The architecture and standards will adopted by all Government and Contractor personnel to achieve standardization and quality objectives 	

DAT3 Acquire and Prepare Data	
Description:	The Government and all contractors supporting the PM NEN are involved in acquiring and preparing data. Data is captured in many authoritative data sources where it can be managed through the Data Management lifecycle.
Supplier:	<ul style="list-style-type: none"> • Incumbent Contractor • All PM NEN data owners, authors, editors, users
Inputs:	<ul style="list-style-type: none"> • Acquisition of Government Purpose Rights (GPR) licensed data • Service Management Operations • New or Modified solutions • Process Activities • Process Development • Requirements Development • Report Development • Configured Automated Triggers within ITSM tools
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • DAT_Acquire_Prepare_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • Data assets within authoritative data sources
Customer:	<ul style="list-style-type: none"> • Incumbent Contractor • PM NEN Personnel
Assumptions:	<ul style="list-style-type: none"> • Both the Government and the contractor are producers and consumers of data within defined authoritative data sources

DAT4 Control, QA, Deploy and Maintain Data	
Description:	Two activities are performed within this process activity. The Government performs inspection and remediation of select data. It also controls access to the data through its data request access process.
Supplier:	<ul style="list-style-type: none"> • Incumbent Contractor
Inputs:	<ul style="list-style-type: none"> • FAR 46 • CoSC Attachment 4 • Data Artifacts • Requests for data access
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • DAT_Control_Access_SOP_v1.0 • DAT_IA&R_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • IA&R Reports • Requests for Remediation • Accepted Data Artifacts
Customer:	<ul style="list-style-type: none"> • PM NEN
Assumptions:	<ul style="list-style-type: none"> • Inspection, Acceptance, and Remediation (IA&R) activities will focus on a sample a data from each of the Incumbent Contractor's data sources. PM NEN will not inspect all data assets.

DAT5	Data Back-up and Restore	
Description:	Protect data assets through the effective data back-up activities for all authoritative data repositories. This includes required efforts to restore data that is lost or corrupt.	
Supplier:	<ul style="list-style-type: none"> • Incumbent Contractor • Government 	
Inputs:	<ul style="list-style-type: none"> • Data Assets held in authoritative data repositories • Data backup requirements, policies and procedures 	
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • DAT_Data_Back-up_Restore_SOP_v1.0 	
Outputs:	<ul style="list-style-type: none"> • Back-up copies of data 	
Customer:	<ul style="list-style-type: none"> • PM NEN 	
Assumptions:	<ul style="list-style-type: none"> • The incumbent contractor will establish and perform backup and recovery activities to support the data it develops and maintains. • Government is responsible for back-up and recovery of its data repositories. 	

DAT6 Data Archival and Disposal	
Description:	When a data asset has reached its effective end-of-life, the asset is archived. Data assets are not deleted but are tagged as archived within the IP Inventory. The data assets remain in the IP share drive where they can be accessed as appropriate for historical and program related needs.
Supplier:	<ul style="list-style-type: none"> • Incumbent Contractor
Inputs:	<ul style="list-style-type: none"> • Updated Data Assets • Request for Change • Data Audits
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • DAT_Archival_Disposal_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • Archival Data • Standardized NMCI IP Inventory
Customer:	<ul style="list-style-type: none"> • PM NEN
Assumptions:	<ul style="list-style-type: none"> • The incumbent contractor has been instructed not to delete licensed data as the Government licensed all NMCI TDPP. • Prior to CoSC Attachment 4, NMCI TDPP may have been deleted, and is no longer available for historical reference. • The IP Inventory data is integrated into the SearchNAVY index, enabling users to filter data based on status (e.g., active, archival).

DAT7 Monitor, Manage and Report Data Management	
Description:	This activity describes the tasks required to assess the efficiency and effectiveness of the Data Management process. It includes the capture of data, the relationships with other process areas, and the suitability of procedures and training. It is used as a basis to ensure Data Management remains fit for purpose and identifies where changes to the process might be required.
Supplier:	<ul style="list-style-type: none"> • Incumbent Contractor • PM NEN Data Management Process Manager
Inputs:	<ul style="list-style-type: none"> • Performance Management Reports
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • DAT_Monitor_Report_Manage_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • Data Management process reports that have been processed and ready for evaluation
Customer:	<ul style="list-style-type: none"> • PM NEN
Assumptions:	<ul style="list-style-type: none"> • This step is a vital contributor to Continual Process Improvement

DAT9 Evaluate Data Management	
Description:	Evaluate the Data Management process against defined objectives to determine if process improvements are required
Supplier:	<ul style="list-style-type: none"> • Incumbent Contractor • PM NEN Data Management Process Manager
Inputs:	<ul style="list-style-type: none"> • Performance Management Reports
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • DAT_Evaluatre_Data_Management_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • Data Management process information to be used for process management decisions
Customer:	<ul style="list-style-type: none"> • PM NEN
Assumptions:	<ul style="list-style-type: none"> • This step is a vital contributor to Continual Process Improvement

ORGANIZATION AND ROLES

7.8 Roles and Organizations

This section defines the roles (e.g. Process Owner, Process Manager, Analyst, etc.) and functional organizations (e.g. DA/TA, Logistics, NetOps, etc.) involved in executing the process. This can be in the form of a narrative, table(s), and/or organization chart(s).

7.9 R/A/C/I

This section contains a process-level RACI chart that shows the relationship between the activities and roles within the organization.

Processes may span departmental boundaries; therefore, procedures and work instructions within the process need to be mapped to roles within the process. These roles are then mapped to job functions, IT staff and departments. The Process Owner is accountable for ensuring process interaction by implementing systems that allow smooth process flow.

The Responsible, Accountable, Consulted, Informed (RACI) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks. Listed below are the roles that have been identified in the process.

R (Responsible) – A Responsible organization is involved in the daily execution of process activities. There may be more than one organization responsible for a given activity. Designating an organization as “Responsible” implies that they fall under the guidance and review of the “Accountable” party. Responsible organizations may or may not be organizationally aligned under the Accountable organization.

A (Accountable) – An Accountable organization serves as the overall owner of process quality and end results. There should only be one Accountable organization per process activity.

C (Consulted) – A Consulted organization provides knowledge and/or information to an activity. These organizations function as “part-time” actors in the process by contributing to specific situations, providing insight to others, performing very clear tasks, etc.

I (Informed) – An Informed organization receives specific information about process execution, status, etc.

Process Activities	Process Owner	Process Manager	Incumbent Contractor
DAT1 Establish Data Management Framework	A	R	R
DAT2 Plan Data Portfolio Architecture	C/I	R	A/R
DAT3 Acquire and Prepare Data	C/I	R	A/R
DAT4 Control, QA, Deploy and Maintain Data	A	R	R
DAT5 Back-up and Restore Data	C/I	R	A/R
DAT6 Archive and Dispose Data	C/I	R	A/R
DAT7 Monitor, Mange and Report	C/I	R	A/R
DAT8 Evaluate Data Management	C/I	R	A/R

7.10 Resource Requirements

7.10.1 Resources Required to Execute the Process

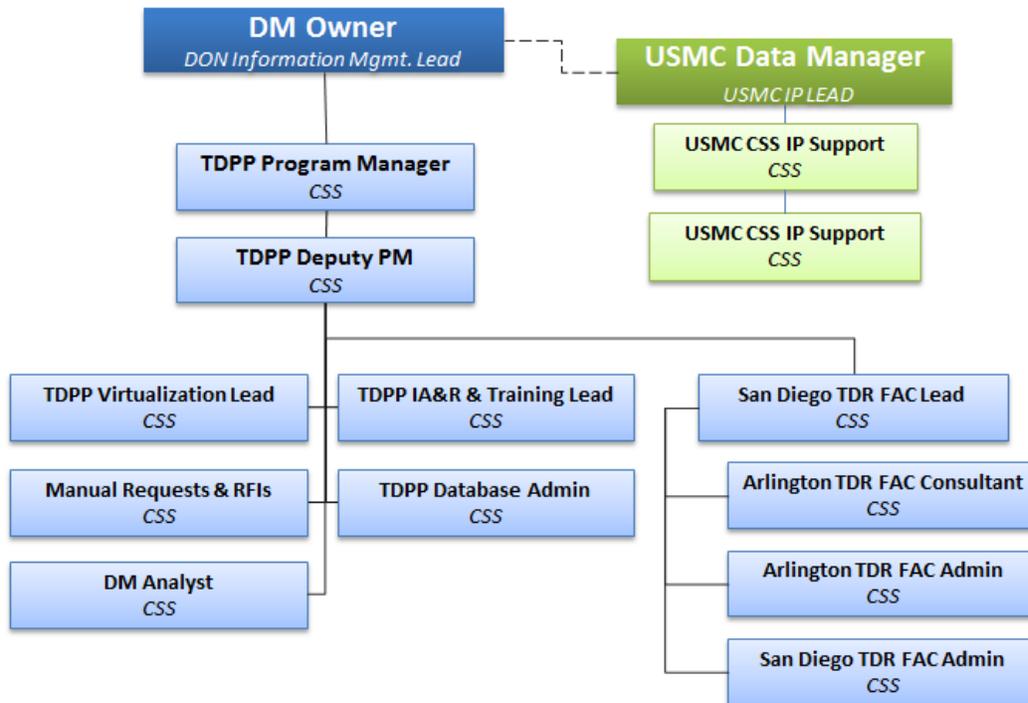


Figure 31 PM NEN Data Management Organization

7.10.2 Knowledge, Skills and Abilities (KSAs)

Each role associated with the Data Management process has specific knowledge, experience and training requirements. This will be included in the process the plan. Generally speaking, some of the general KSA considerations are as follows:

- Familiarity with PM NEN Documentation (e.g., Systems Engineering Plan (SEP), Acquisition Strategy (AS),
- Familiarity with Government Policy (e.g., FAR 46, DODI 5000.02, DDMS, etc..)
- Experience with industry recognized Knowledge Management practices
- Experience with MAIS programs
- Experience with the strategy, design, transition and operations of large Enterprise Networks
- Communication skills that include strong abilities in both verbal and written communications

7.10.3 Identification and Training of Government Personnel

Government personnel supporting the Data Management process require the standard skill set related to understanding and managing Government contracts, management and direction of contract support personnel and confidentiality requirements. In addition, the following requirements are valuable in supporting the NEN program.

- Defense Acquisition University (DAU) Acquisition 101
- DAU CLC 132 Organizational Conflicts of Interest (OCI)
- ITIL Foundations

DATA AND INFORMATION

7.11 Data and Information Requirements

This section summarizes the data and information management requirements of the process, and identifies the key consumers (e.g. roles, organizations) of process information work products.

7.12 Information Work Products (IWP)

This section details the process IWPs including their usage and target audience. IWPs will be used either internally within the process which generated them, or by another process which receives the work product. IWPs will contribute to the Command and Control (C2) analysis and decisions used in managing the process:

IWP	Target Audience	Description/Usage
Data Management Plan	All NEN Stakeholders	A program document that defines the scope, objectives and direction of the Data Management effort.
NGEN Metadata and Data Architecture Guide	All NGEN Stakeholders	The Metadata Guide provides documented standards are guidance for federated data that is leveraged and utilized across the enterprise. This is a living document that contains guidance and standards that apply to a large percentage of program data
NMCI IP Access Plan and Execution Schedule	Contractors and Government staff directly involved with Data Management operations	CoSC CDRL IP003 defines the procedures, timelines and activities for granting the Government access to NMCI IP and providing training about NMCI IP.
Inspection, Acceptance, and Remediation Strategy	Contractors and Government staff directly involved with Data Management operations	CoSC Attachment 4 outlines Acceptance criteria against which NMCI TDPP will be measured. The IA&R Strategy elaborates on this criteria and defines the strategy which PM NEN employs to inspect, accept, and direct remediation on NMCI TDPP.
NMCI IP Delivery Strategy	Contractors and Government staff directly involved with Data Management	CoSC CDRL IP001 defines the strategy and procedures for delivering a copy of all NMCI IP to PM NEN. The delivery schedule is aligned to the transition of services from incumbent to successor.

	operations	
--	-------------------	--

7.13 Reporting Requirements

This section defines process reports:

Report Elements	Amplifying Information
CoSC CDRL IP002	NMCI IP Inventory
Report Description	Listing of NMCI IP artifacts, by repository, used to report changes in the IP Baseline and apply architecture standards to the IP corpus
Report Audience	PM NEN
Report Owner	NEN Program Manager
CSFs In Report	Accurate Inventory of Data Assets
KPIs/Metrics Used In Report	Count of Artifacts on the IP Share Count of Artifacts in the IP Inventory Compare IP Share contents to IP Inventory Audit Corpus Changes
Report Frequency	Monthly

PERFORMANCE MANAGEMENT

7.14 Current Process Metrics

This section lists the Critical Success Factors (CSFs) and Key Performance Indicators (KPIs) used to baseline and measure process transition success.

Effective day-to-day operation and long-term management of the process requires measuring the process. Reports must be defined, produced and distributed to enable the management of process-related issues and initiatives. Daily performance management occurs with the process manager. Long-term trending analysis and management of significant process activities occurs at the process owner.

A powerful vision and well-defined mission statement are critical to defining enterprise goals and objectives. Process governance starts with establishing objectives for the enterprise, and continuous performance management aids direction of activities aligned with those set objectives. The Process Owner is responsible for measuring and providing value-based reporting. Critical Success Factors (CSFs) identify the most important actions for achieving control over

the process and Key Performance Indicators (KPIs) measure whether or not a control is meeting its objective.

Continual service improvement depends on accurate and timely process measurements and relies on obtaining, analyzing, and using information that is practical and meaningful to the process. Measurements of process efficiency and effectiveness enable NGEN management to track process performance and improve overall end-user satisfaction.

The following table summarizes the relationships between process CSFs and KPIs. See Appendix D for a complete list of CSFs and KPIs.

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Accurate Inventory of Data Assets	1	Count of Artifacts on the IP Share
		2	Count of Artifacts in the IP Inventory
		3	Compare IP Share contents to IP Inventory
		4	Audit Corpus Changes
2	Timely Publication of Relevant Data	5	Mean Time to Publish
3	Quality Assurance - Inspection, Acceptance & Remediation (IA&R)	6	Mean time to Remediate
		7	Percentage of Inspections Requiring Remediation
		8	Number of Artifacts Accepted
		9	Number of Artifacts Accepted with Exception
		10	Number of Artifacts Remediated
4	Data Accessibility	11	Number of Artifacts Inspected
		12	Percentage of Failed Data Inquiries
		13	Number of times user cannot locate data on the IP Share
		14	Percentage of requests requiring the DM team request Data from Incumbent

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
		15	Mean Time to Grant Access
		16	Mean Time to Restore

*Note: Additional metric details incl. threshold and objective values are defined in the SOPs.

7.15 Desired Metrics and Compliance Controls

Additional performance management reports, dashboards and other controls are desired to assist in establishing a standardized, efficient Data Management process and to support its continual improvement. Examples of additional reporting capability include:

- Data quality within authoritative data sources,
- Data usage reports that help identify information that is most frequently used,
- Reports identifying contributors who consistently provide data assets that are of greatest value to the enterprise, and
- Failed search criteria that can identify data gaps which need to be filled.

TOOLS AND TECHNOLOGY

7.16 Tool Requirements

This section defines key tool automation capability, interface, and interoperability requirements:

Requirement	Process Activity
Ability to capture many different types of data that are generated by the activities associated with delivering and supporting IT services.	3.0 Acquire and Prepare Data
Ability to audit, review, and validate data prior to publication to extended audiences	4.0 Control, QA, Deploy and Maintain Data
Ability to store, manage and publish data to designated audiences based on a need to know.	4.0 Control, QA, Deploy and Maintain Data
Ability to archive data in such a way that it is available to appropriate audiences while restricting its access by the majority of the enterprise users	6.0 Archive Data

7.17 Tools Used to Support the Process

This section defines the requirements met by COSC tools today and documents key gaps:

Requirement	COSC Tool Used Today	Measure -ment	Gap	Recommendation
Ability to publish data to a Government audience, and manage access to NMCI IP	IP Share Drives	Partially Meets	No ability to mine data, filter, organize, or manage data	Implementation of Enterprise Content Management (ECM)
Accurate Inventory of Data Assets	IP Inventory Database	Partially Meets	Inventory maintained manually, updated on a monthly basis in MS Access with	Implementation of Integrated Digital Environment (IDE)

			limited functionality	
Ability to manage PM NEN Acquisition Documents	CMPRO	Partially Meets	Ease of use / User Friendly Interface, ability to customize, Publication and collaboration capability limited, no integration with Active Directory	Implementation of Enterprise Content Management (ECM)
Ability to store, share, and manage PM NEN Team documentation	PEO EIS Portal	Partially Meets	Restrictions on data type storage, restricted ability to customize, limited search capability, limited disc space,	Implementation of Enterprise Content Management (ECM)
Ability to mine data	Search NAVY	Partially Meets	Search/filter only, not full portal functionality, cannot apply metadata at artifact level, cannot manage data	Implementation of Enterprise Content Management (ECM) using SearchNAVY for Search functionality
Track and report IA&R efforts	Inspection, Acceptance & Remediation Database	Partially Meets	Ability to host in a location that is accessible to appropriate audiences, disparate from actual data	Implementation of Enterprise Content Management (ECM)

7.18 Interface Requirements

This section defines the key interfaces with other processes, tools, governance bodies, and resources (service owners, vendors):

Interface ID	Interface Description
1	Process: Most, if not all ITSM processes rely upon data inputs to perform process activities and they develop data outputs that become inputs for other processes. The Data Management lifecycle tasks, standards, and activities must be adopted and integrated in all ITSM process activities related to the capture, validation, publication, access, storage and maintenance of data.
2	Process: ITSM processes that do not have the ability to capture, store or publish data in a federated environment will rely upon the Enterprise Content Management tools and associated processes that are established and managed by the Data Management process.

7.19 Integration Approach

7.19.1 Use Case Selection

TBD

7.19.2 Workshops and Simulations

TBD

7.20 Validation Results and Remediation

This section summarizes the key process validation results with emphasis on broken interfaces or other issues that require remediation in order to achieve process transition objectives.

Error ID	Validation Scenario	Step Description	Type of Error Found	Error Description
		TBD	TBD	TBD

8. PROBLEM MANAGEMENT [PRB]

8.1 Purpose

Problem Management is the process responsible to manage the lifecycle of all problems affecting the IT service, both reactively and proactively. Problem Management identifies trends in incidents, correlates incidents to problems, identifies the root causes of problems and initiates Requests for Change (RFCs) against those problems. Additionally, Problem Management attempts to proactively mitigate issues identified as part of the Continuous Service Improvement (CSI) plans within other Information Technology Service Management (ITSM) processes.

8.2 Policies

- Continuity of Service Contract (CoSC)

8.3 Outcomes

A successful implementation of the Problem Management process should yield:

- Reduced number of incidents and problems
- Reduced recurrence rate of incidents
- Less impact of reported incidents
- Proactive prevention of issues before they become incidents
- Efficient and effective management of incidents and problems
- Improved support staff productivity
- Problems recorded and classified
- Problems prioritized and analyzed
- Problems resolved and closed
- Problems which are not progressed according to agreed service levels are escalated
- Effect of unresolved problems minimized
- Status and progress of the resolution of problems communicated to affected parties

An effective Problem Management process maximizes system availability, improves service levels, reduces costs, and improves customer convenience and satisfaction.

8.4 Scope

The Problem Management process is primarily concerned with establishing the root cause of an incident and its subsequent resolution and prevention. Problems relating to one or more incidents are resolved reactively. Problems are the result of incidents, while performing root cause analysis additional incidents related to the original problem may occur.

Effective Problem Management requires problem identification and classification, root cause analysis and problem resolution. The Problem Management process also includes the formulation of recommendations for improvement, maintenance of problem records and review of the status of corrective actions.

8.4.1 Includes

- Root cause analysis and identification
- Solution (and workaround) definition and selection
- Submission of change requests
- Appropriate prioritization of resources required for resolution based on business need
- Contribution to the collective problem resolution knowledge base
- Maintenance of the Known Error Database

8.4.2 Excludes

- Incident identification, creation and resolution (Incident Management)
- Actual implementation of the resolution of a problem. Problem Management initiates resolution through Change Management and participates in the Post Implementation Review (PIR)
- Knowledge management methodology (Knowledge Management)

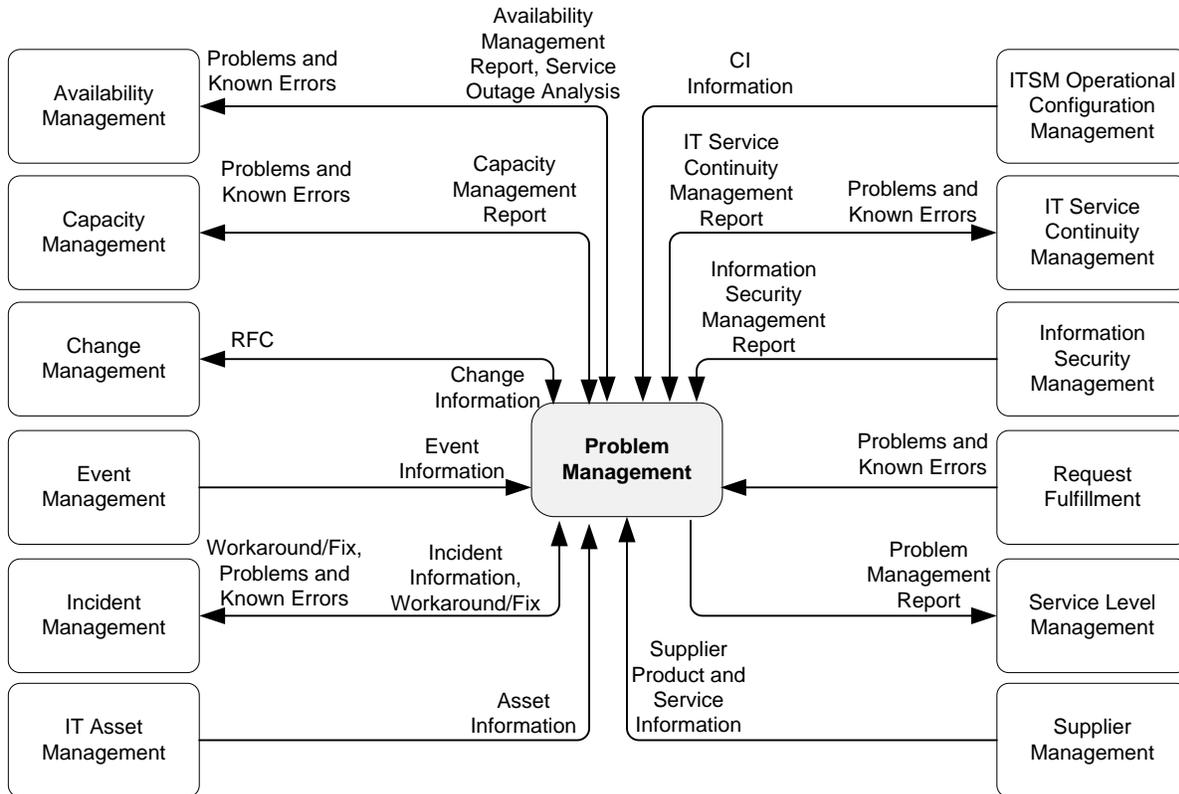
8.5 Process Interfaces

Primary interfaces with other processes include the following:

Information from a variety of sources may be used to detect and diagnose problems, including:

- Availability Management provides Availability Management Reports
- Capacity Management provides Capacity Management Reports and Service Outage Analyses
- Change Management provides Change Information
- Event Management provides Event Information
- Incident Management provides Incident Information
- Information Security Management provides Information Security Management Reports
- IT Asset Management provides Asset Information
- Configuration Management provides Configuration Information
- IT Service Continuity Management provides IT Service Continuity Management Reports
- Supplier Management provides Supplier Product and Service Information
- Reports from:

- Availability Management
- Capacity Management
- Information Security Management
- IT Service Continuity Management
- Problems and Known Errors are used by many processes for analysis, including:
 - Availability Management
 - Capacity Management
 - Incident Management
 - IT Service Continuity Management
 - Request Fulfillment
 - Service Level Management
- New workarounds and fixes created during the resolution of incidents are provided by Incident Management.
- Workarounds and fixes are created during Problem Management and provided to Incident Management.
- This process is affected by the strategic direction described in the IT Strategy, generated by the Strategy Generation process.
- This process provides content in the form of Knowledge Items to the Knowledge Management process. In addition, Knowledge Management organizes and processes that content into Knowledge Assets.
- Compliance Management identifies specific Compliance Plans and Controls that should be adhered to by this process to meet standards and regulations that should be complied with. In return, this process provides an evaluation of how those standards and regulations were complied with.



Note: This diagram does not show the following interfaces to all processes:

- IT Strategy sent from Strategy Generation process
- Compliance Plans and Controls from Compliance Management process
- Knowledge Assets from Knowledge Management process

In addition, this diagram does not show the following interface to Knowledge Management from all processes:

- Knowledge Items sent to the Knowledge Management process

Figure 32 - Problem Management Interfaces

8.6 Activity-Level Workflow

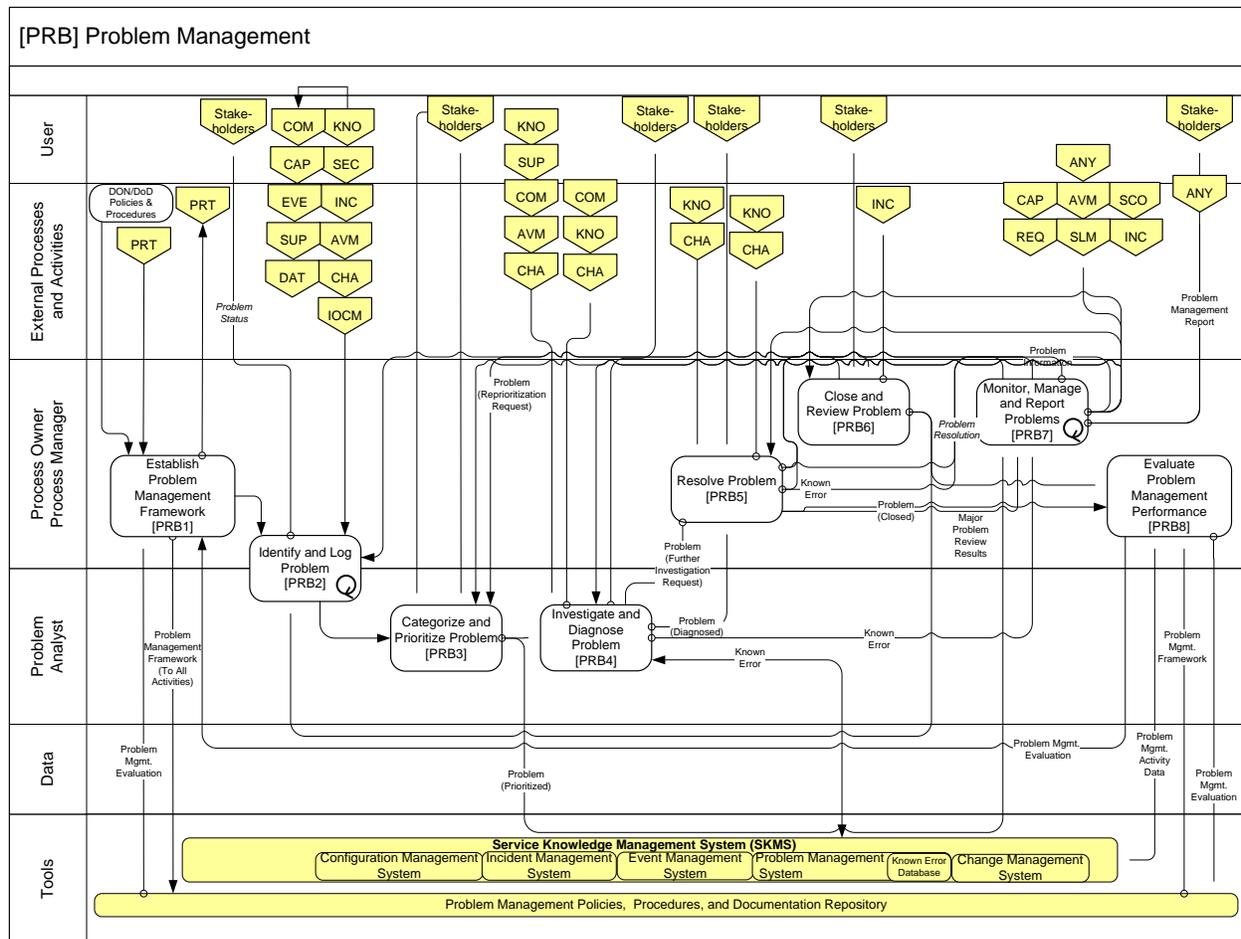


Figure 33 - Problem Management Workflow

8.7 Activities

8.7.1 [PRB1] Establish Problem Management Framework

This activity defines the relationships of other processes and interfaces, classification and prioritization guidelines are defined along with information work products inputs and outputs, including the review of process evaluation results and the implementation of recommended improvement actions. Process metrics and tool requirements are identified and updated as necessary and methods of communicating the process framework are established. During this activity the requisite service level agreements and operational level agreements are taken into account as the framework is developed and improved.

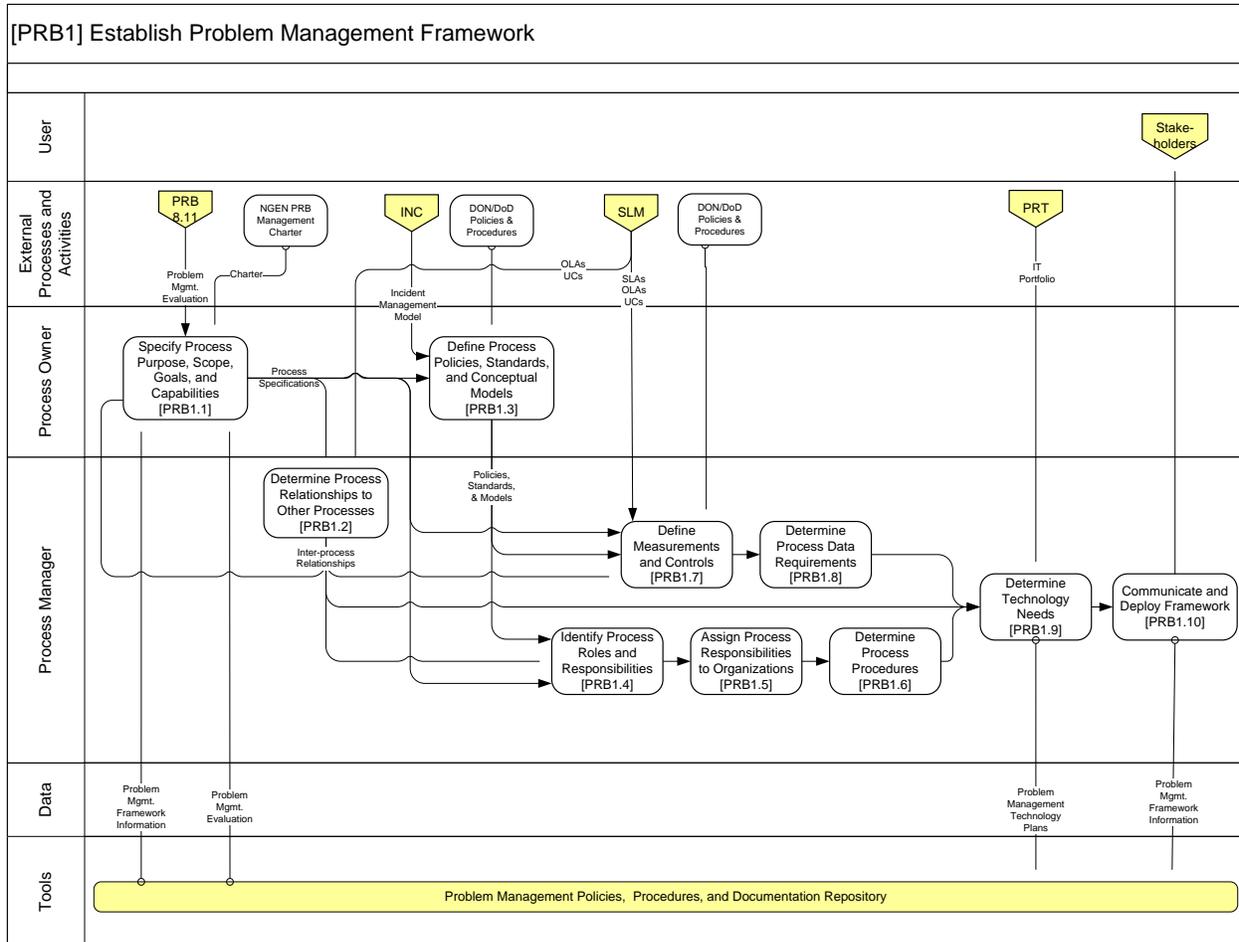


Figure 34 - PRB1 Workflow

8.7.1.1 TASKS

- Specify Process Purpose, Scope, Goals, and Capabilities
- Determine Process Relationships to Other Processes
- Define Process Policies, Standards, and Conceptual Models
- Identify Process Roles and Responsibilities
- Assign Process Responsibilities to Organizations
- Determine Process Procedures
- Define Measurements and Controls
- Determine Process Data Requirements
- Determine Technology Needs
- Communicate and Deploy Framework

8.7.1.2 DECISION TIMELINES

N/A

8.7.1.3 GAPS

N/A

8.7.1.4 INTERFACES

N/A

8.7.1.5 LOCATION

N/A

8.7.1.6 MEETINGS

N/A

8.7.1.7 METRICS

N/A

8.7.1.8 ORGANIZATIONS

The headings in these tables are described in more detail in Appendix A.

Process Point	Position	Organization	Name	Contact Data	Tools
	Incident Problem Manager	HPES			
	Process Manager	NNWC		N/A	

8.7.1.9 POLICIES

N/A

8.7.2 [PRB2] Identify and Log Problem

This activity ensures that monitoring, analysis, and notification mechanisms are implemented to identify Problems. Once identified, Problems are fully recorded and linked to the associated Incident(s). Incidents provide the primary source for Problem identification; the activity includes further ways to identify Problems:

- Notification from Suppliers
- Feedback from the GNOSC, technical support groups or customer surveys

- Change Management information
- Inputs from Event Management
- Proactive approaches like trend analysis

Problem identification and logging can include both automated and manual activities. The result of this activity is the formal creation of a Problem Record with the relevant details logged.

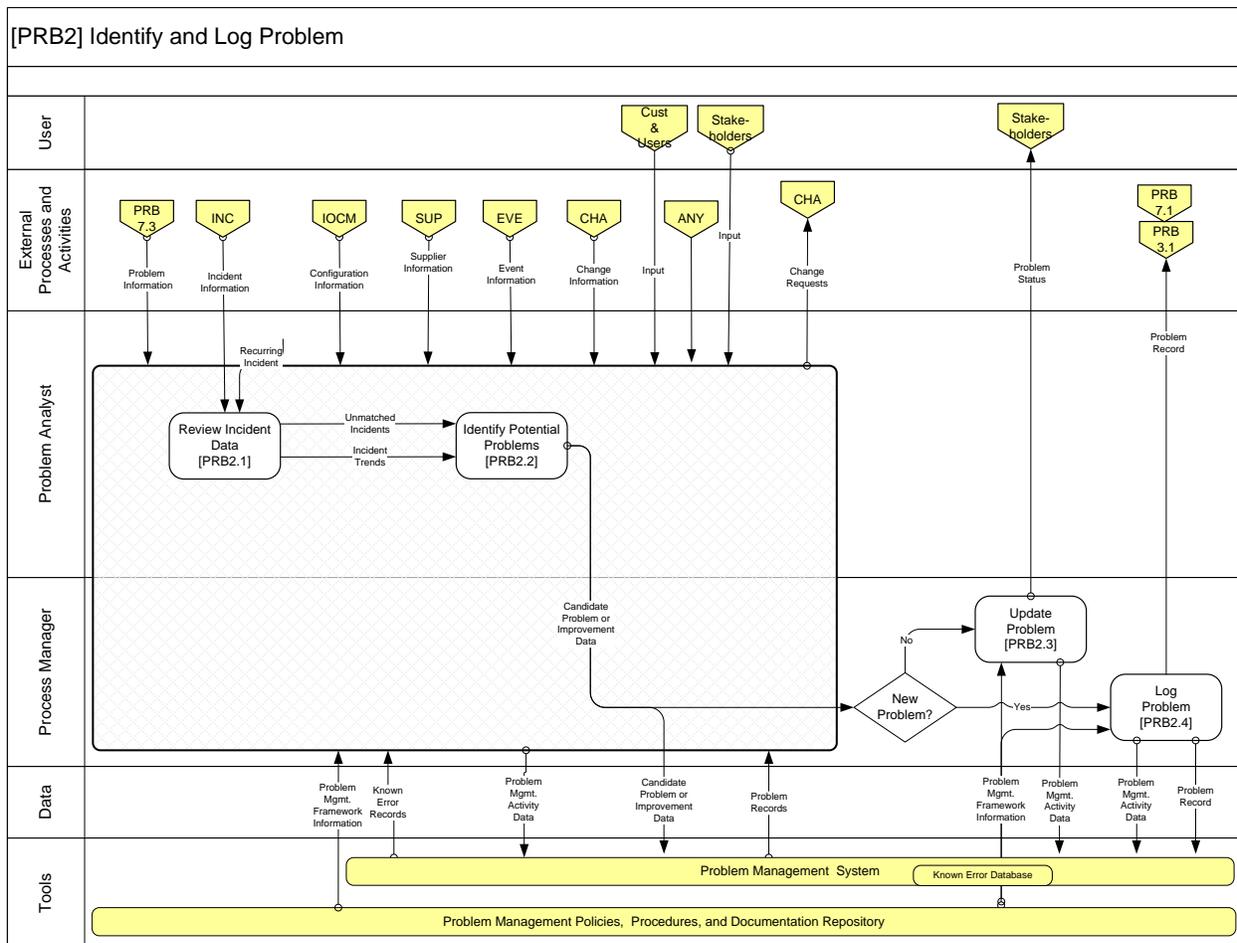


Figure 35 - PRB2 Workflow

8.7.2.1 TASKS

- Review Incident Data
- Identify Potential Problems
- Update Problem
- Log Problem

8.7.2.2 DECISION TIMELINES

N/A

8.7.2.3 GAPS

Process Points	Description	Severity	Mitigation	Tools	Tool Requirements
Availability of licenses for access to tools	Critical	Manual intervention	Same as INC	SM7	Include Ops console ACTIONS: 1) HP to provide specifics on licensing 2) Government provide billet and name listing of personnel requiring access 3) HP conducts licensing gap analysis and informs Government 4) Government pursues funding for additional licenses (if needed)
Directive on how to create a new problem ticket from Government to HP	Moderate	Manual intervention	1 month	Digitally signed Email	ACTION: 1) NetOps3 hosts meeting with HP to define problem ticket directive/artifact

8.7.2.4 INTERFACES

N/A

8.7.2.5 LOCATION

N/A

8.7.2.6 MEETINGS

N/A

8.7.2.7 METRICS

Process Points	Metric	Format	Access Point(s)	Tools	Tool Requirements
Difference between HP problem detection and Gov't problem detection	Problem tickets	SM7	Monthly	SM7	
Problem ticket creation time	See gap on problem ticket				

8.7.2.8 ORGANIZATIONS

Process Point	Position	Organization	Name	Contact Data	Tool Requirements
Problem Analysts	NNWC	NetOps3	SM7/EPMD/Net Vigil/SCIA/Email	Read and run reports	Request access to Known Error Database
Problem Analysts	RNOSC L	NetOps	SM7/EPMD/Net Vigil/SCIA/Email	Read and run reports	Government to Government Not just LANT Request access to Known Error Database
Problem Analysts	NCDOC	Incident Mgmt	SM7/EPMD/Net Vigil/SCIA/Email	Read and run reports	Government to Government Request access to Known Error Database
Problem Analysts	HPES	SMI	SM7/EPMD/Net Vigil/SCIA/Email		
Problem Manager	NNWC	NetOps 3	TBD		See gap for problem ticket

					creation
--	--	--	--	--	----------

8.7.2.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
CoSC		Portal		Portal	
CoSC		Portal		Portal	

8.7.3 [PRB3] Categorize and Prioritize Problem

This activity ensures the appropriate analysis can be performed for resolution by classifying Problems correctly according to established categorization and prioritization criteria. The impact of the Problem and its severity are also considered within this activity.

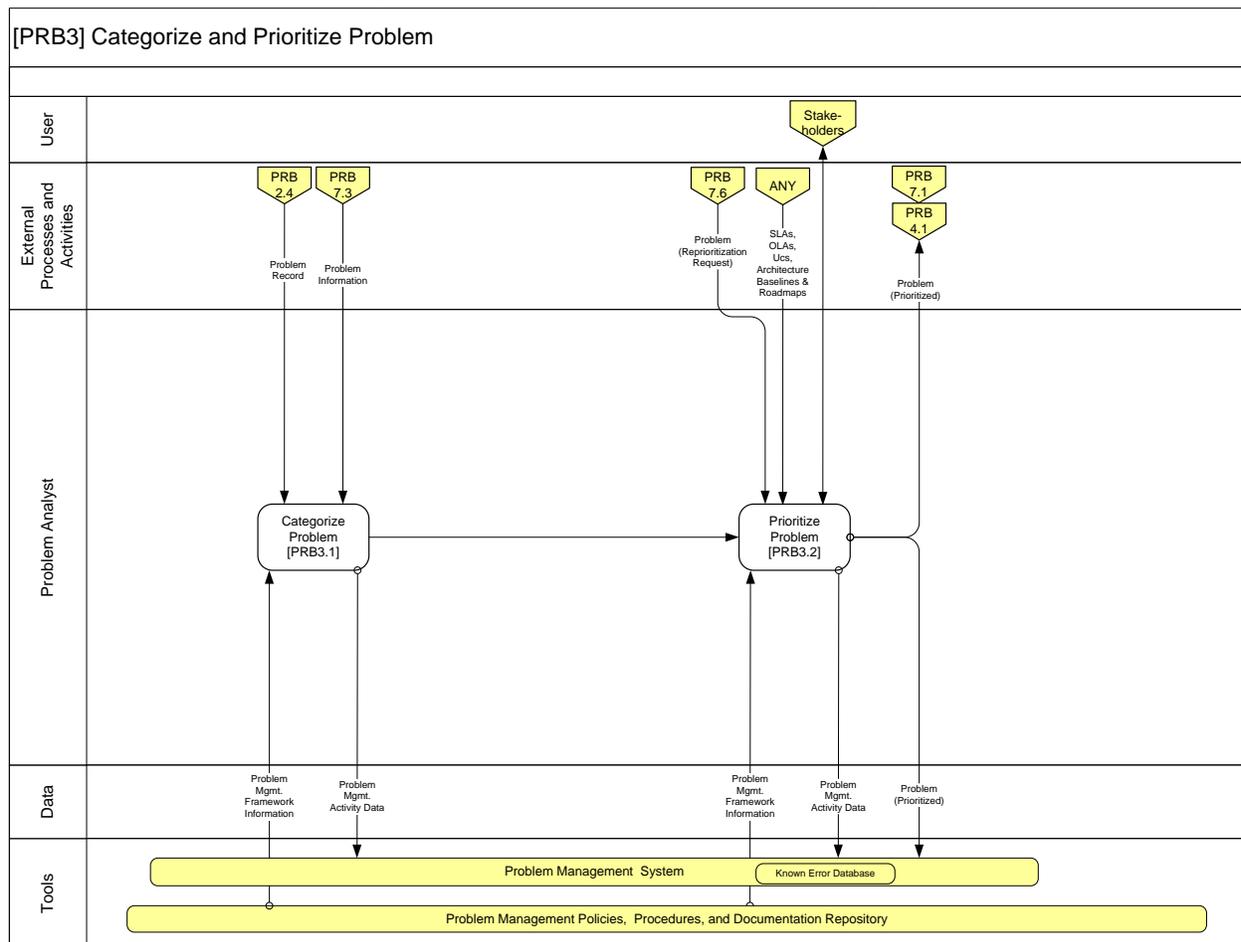


Figure 36 - PRB3 Workflow

8.7.3.1 TASKS

- Categorize Problem
- Prioritize Problem

8.7.3.2 DECISION TIMELINES

N/A

8.7.3.3 GAPS

Process Points	Description	Severity	Mitigation	Tools	Tool Requirements
Prioritization schema/methodology	Moderate	Manual intervention	1 month	PRB SOP	ACTION: 1) NetOps3 hosts meeting with HP

8.7.3.4 INTERFACES

N/A

8.7.3.5 LOCATION

N/A

8.7.3.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Tools	Tool Requirements
Drumbeat	Virtual	NetOps 3 - Lead with open forum	Perpetual	SM7	Every 2 weeks

8.7.3.7 METRICS

Process Points	Metric	Format	Access Point(s)	Tools	Tool Requirements
	Number of times priorities have changed, and reasons why	Problem record	Quarterly	SM7	

8.7.3.8 ORGANIZATIONS

Position	Organization	Name	Contact Data	Tools	Notes
HP SMI Manager	HPES			Verbal/Email	Re-prioritization
NetOps 3 DIVDIR	NNWC			Verbal/Email	Re-prioritization
Problem Analysts	NNWC	NetOps 3		SM7/EPMD/Net Vigil/SCIA/Email	Initial prioritization meeting required
Problem Analysts	HPES	SMI		SM7/EPMD/Net Vigil/SCIA/Email	

8.7.3.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
CoSC		Portal		Portal	

8.7.3.10 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Tools	Tool Requirements
	Problems in SM7 PRB module	Web-based	as required	within SM7	SM7

8.7.4 [PRB4] Investigate and Diagnose Problem

In this activity, Root Cause Analysis (RCA) is performed to determine the root cause of the problem. As a result of RCA activities, effective workarounds can be determined and the problem record updated with the workaround. This activity also provides the required analysis and diagnosis to complete RCA activities. The Problem Record, Workaround Data (Record) and Known Error Record are indicated separately however, they may be linked within the same record.

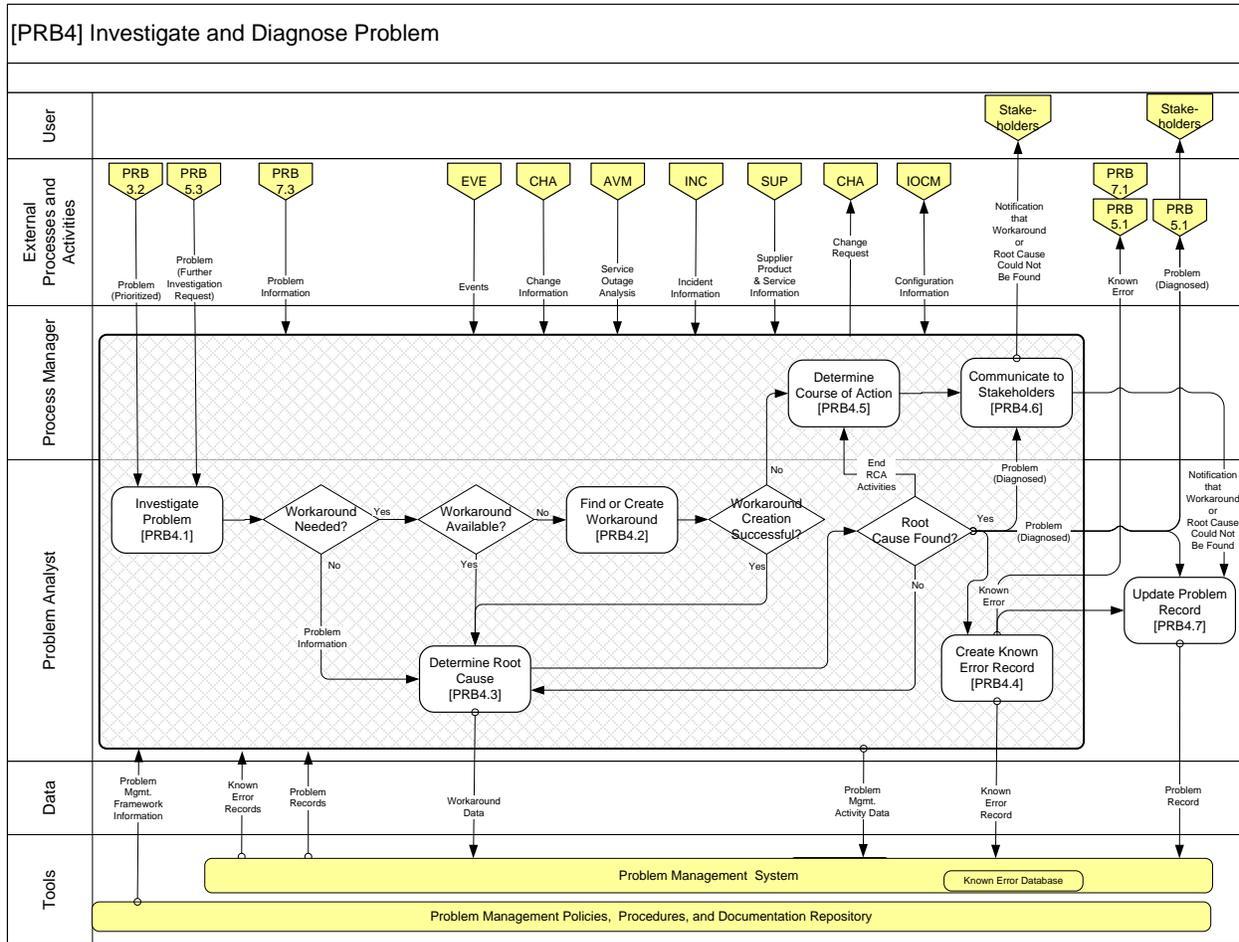


Figure 37 - PRB4 Workflow

8.7.4.1 TASKS

- Investigate Problem
- Determine Root Cause
- Find or Create Workaround
- Determine Course of Action
- Create Known Error Record
- Communicate to Stakeholders
- Update Problem Record

8.7.4.2 DECISION TIMELINES

N/A

8.7.4.3 GAPS

Process Points	Description	Severity	Mitigation	Tools	Tool Requirements
Sharing of non-NMCI known errors with NMCI	Moderate	Manual intervention	6 months	SM7	Tasked to NetOp3, incorporate KM team

8.7.4.4 INTERFACES

N/A

8.7.4.5 LOCATION

N/A

8.7.4.6 MEETINGS

N/A

8.7.4.7 METRICS

N/A

8.7.4.8 ORGANIZATIONS

N/A

8.7.4.9 POLICIES

N/A

8.7.5 [PRB5] Resolve Problem

This activity provides resolutions for Problems which a Known Error is identified and understood. Information is gathered to search for a resolution, a resolution is found, solutions are planned, implemented, tracked and confirmed. This activity may include major outputs such as a project proposal or Change Request or both. Lastly, the Problem and Known Error Records are updated.

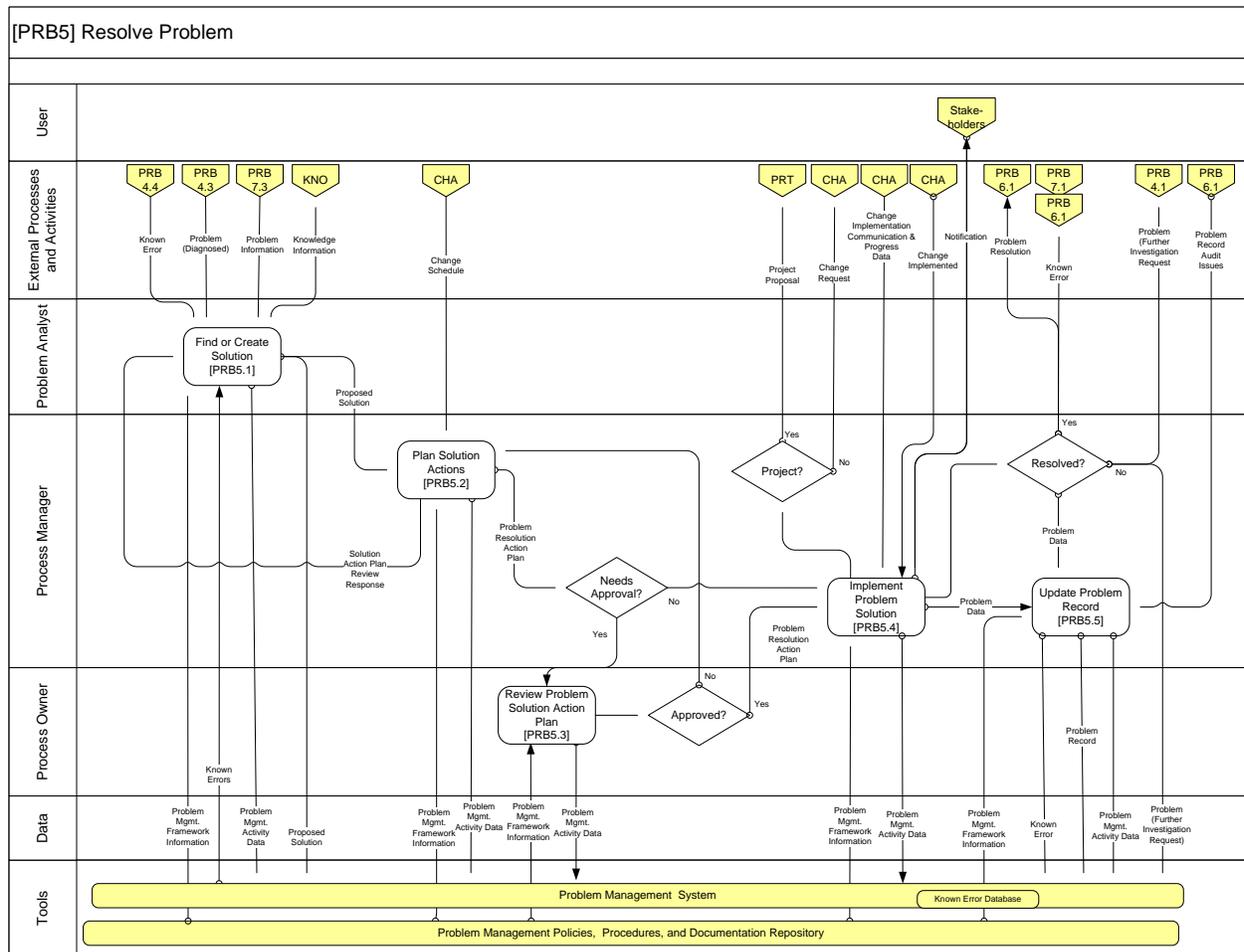


Figure 38 - PRB5 Workflow

8.7.5.1 TASKS

- Find or Create Solution
- Plan Solution Actions
- Review Problem Solution Action Plan
- Implement Problem Solution
- Update Problem Record

8.7.5.2 DECISION TIMELINES

N/A

8.7.5.3 GAPS

Process Points	Description	Severity	Mitigation	Tools	Tool Requirements
----------------	-------------	----------	------------	-------	-------------------

Process Points	Description	Severity	Mitigation	Tools	Tool Requirements
Definition of interface to external service providers (DISA, WNY ITA...)	Moderate	Manual intervention	2 months	MOA/MOU	ACTION: 1) NetOps3 to define

8.7.5.4 INTERFACES

Process Points	Process	Interface	Return/Terminate	Tools	Tool Requirements
	Change Management	Request for Change	Return to HP	Remedy ticket	
	Request Fulfillment	Recommended solution from HP to Gov't	Return to HP	Text document	

8.7.5.5 LOCATION

N/A

8.7.5.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Tools	Tool Requirements
Drumbeat	Virtual	NCF N47 and NetOps 3 - Lead with open forum	Perpetual	SM7	Concurrently with PRB3.2. Agenda item to discuss priority of C&A queue

8.7.5.7 METRICS

Process Points	Metric	Format	Access Point(s)	Tools	Tool Requirements
	First pass approval percentage	Problem record	Quarterly	SM7	

8.7.5.8 ORGANIZATIONS

Process Point	Position	Organization	Name	Tools	Tool Requirements
	NAVCYBERFOR N47	NCF		SM7	Owner
	NetOps 3 DIVDIR	NNWC		SM7	Manager

8.7.5.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
CoSC		Portal		Portal	

8.7.5.10 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Tools	Tool Requirements
	Problems in SM7 PRB module	Web-based	as required	within SM7	SM7

8.7.6 [PRB6] Close and Review Problem

This activity closes Problem Records and updates Known Error Records as appropriate. The Problem Records are checked for completeness to aid their use in support of information available to other processes. Major Problems are systematically reviewed and results incorporated in service review, training and stakeholder communication.

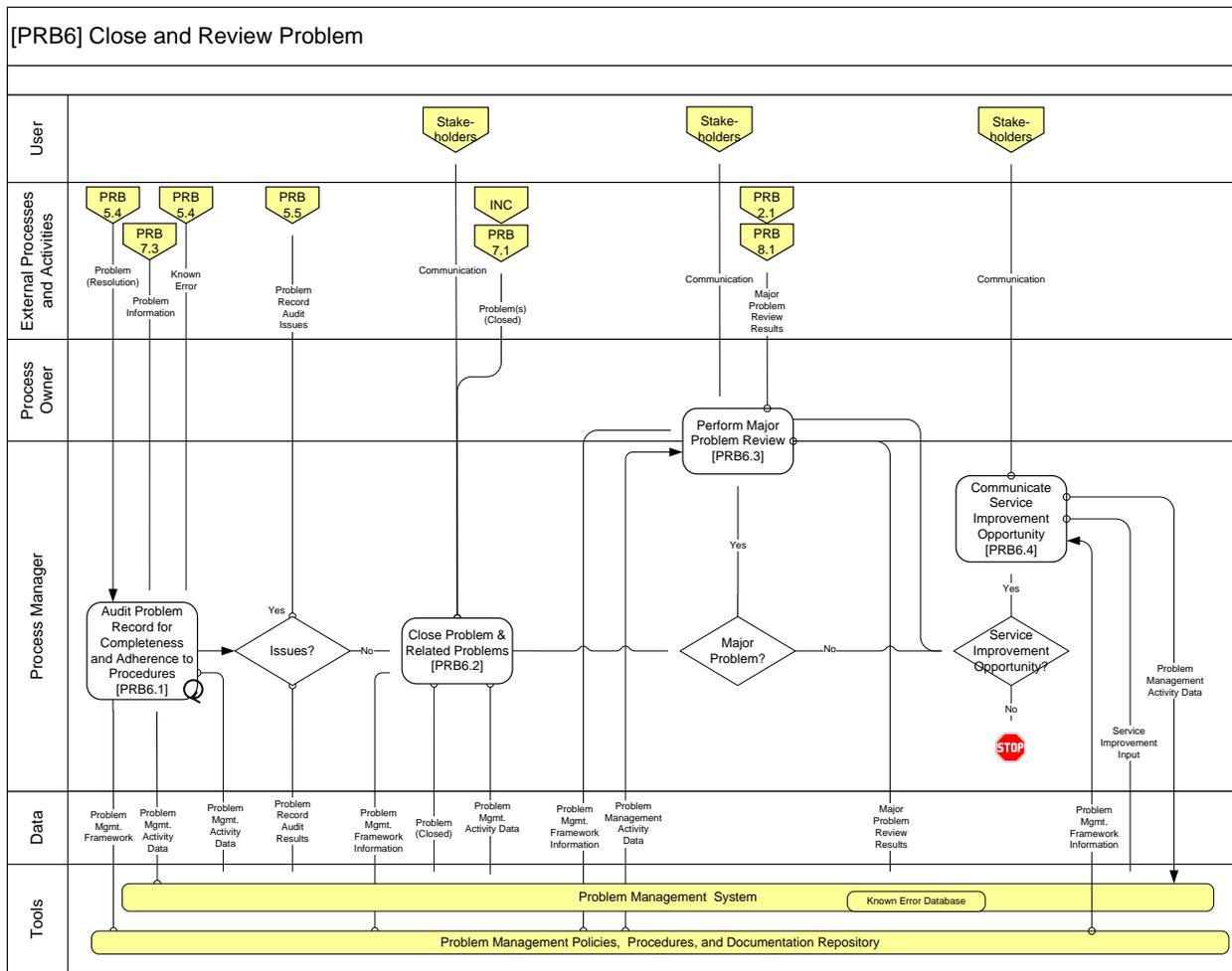


Figure 39 - PRB6 Workflow

8.7.6.1 TASKS

- Audit Problem Record for Completeness and Adherence to Procedures
- Close Problem and Related Problems
- Perform Major Problem Review
- Communicate Service Improvement Opportunity

8.7.6.2 DECISION TIMELINES

N/A

8.7.6.3 GAPS

Process Points	Description	Severity	Mitigation	Tools	Tool Requirements
----------------	-------------	----------	------------	-------	-------------------

Process Points	Description	Severity	Mitigation	Tools	Tool Requirements
Definition and extra requirements for a Major Problem	Moderate	Manual intervention	1 month	PRB SOP	ACTION: 1) NetOps3 hosts meeting with HP

8.7.6.4 INTERFACES

N/A

8.7.6.5 LOCATION

N/A

8.7.6.6 MEETINGS

Process Points	Purpose	Live/Virtual	Methodology	Tools	Tool Requirements
Major Problem review	Combined	NCF N47 and NetOps 3 - Lead with open forum	As required	SM7/PowerPoint	May become a recurring meeting in the future

8.7.6.7 METRICS

Process Points	Metric	Format	Access Point(s)	Tools	Tool Requirements
	Length of time at each step from problem resolution recommendation to problem closure	Problem record and spreadsheet	Semi-Annual	SM7	Each step
	Quantity and qualifications of Major Problems being tracked	Problem record	Quarterly	SM7	

8.7.6.8 ORGANIZATIONS

Process Point	Position	Organization	Name	Tools	Tool Requirements
	NAVCYBERFOR N47	NCF		SM7	Owner
	NetOps 3 DIVDIR	NNWC		SM7	Manager

8.7.6.9 POLICIES

Process Points	Basis	Boundaries	Current Location	Tools	Tool Requirements
CoSC		Portal		Portal	

8.7.6.10 WORK PRODUCTS

Process Points	Type	Format	Periodicity	Tools	Tool Requirements
	Problems in SM7 PRB module	Web-based	As required	within SM7	SM7

8.7.7 [PRB7] Monitor, Manage and Report Problem Management

This activity monitors, manages and provides reporting throughout the PRB lifecycle. This activity can result in Root Cause analysis, new resolution plans, and provide information to service reviews. The monitoring and reporting is recurrent on a scheduled basis, although monitoring and reporting can be initiated by special request. While most of the statistics used in the reports is based on Problem Record data, customer input is also used.

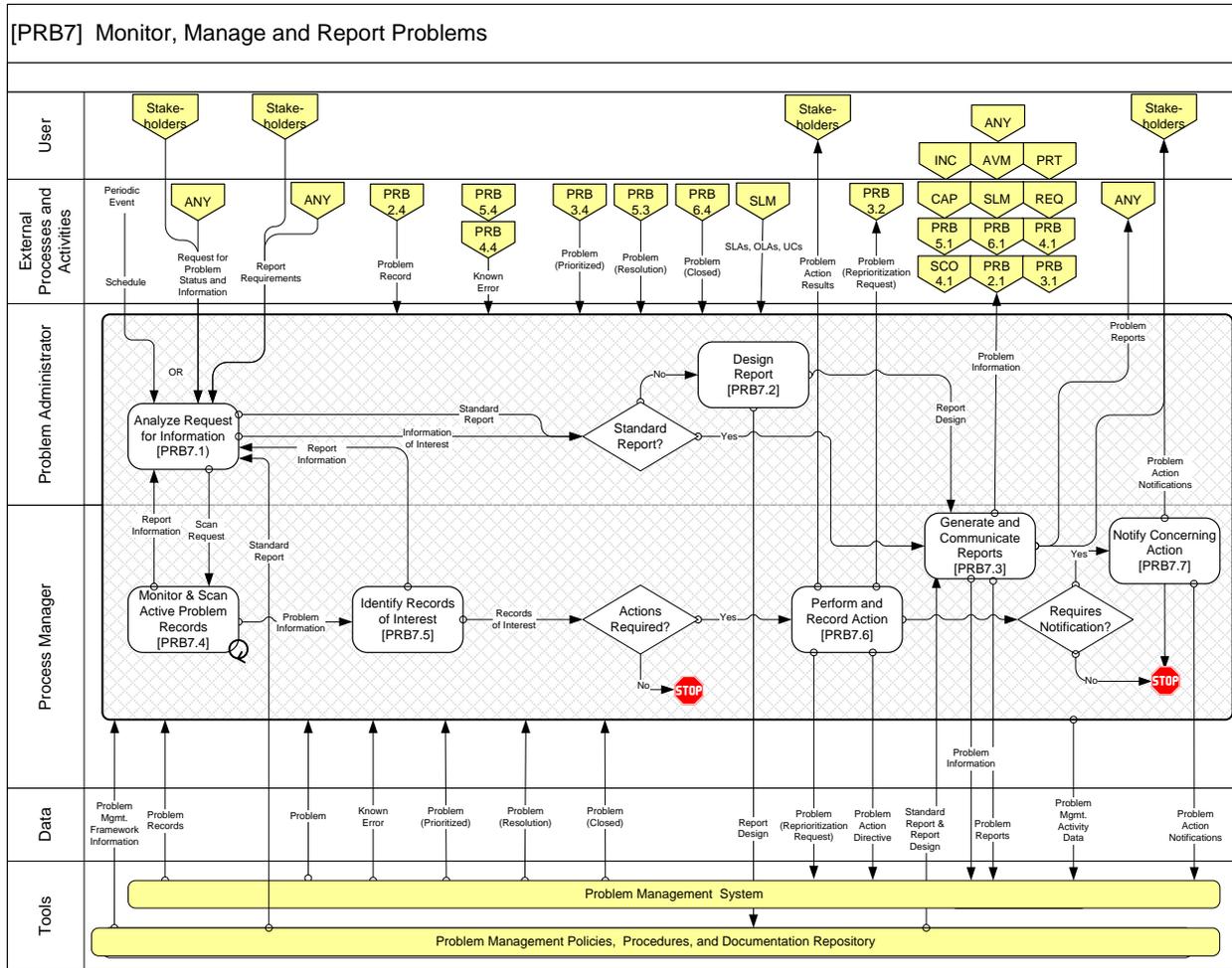


Figure 40 - PRB7 Workflow

8.7.7.1 TASKS

- Analyze Request for Information
- Design Report
- Generate and Communicate Reports
- Monitor and Scan Active Problem Records
- Identify Records of Interest
- Perform and Record Action
- Notify Concerning Action

8.7.8 [PRB8] Evaluate Problem Management Performance

This activity describes the tasks involved in providing ongoing evaluation assessments of the Problem Management process. Performance evaluation of the Problem Management process assists in identification of improvement areas for the overall process (e.g., the foundation and interfaces of the process, activities, and accomplishments, degree of automation, and roles and

responsibilities). Additionally, this activity also implements lessons learned from analysis and input to feed into service improvement.

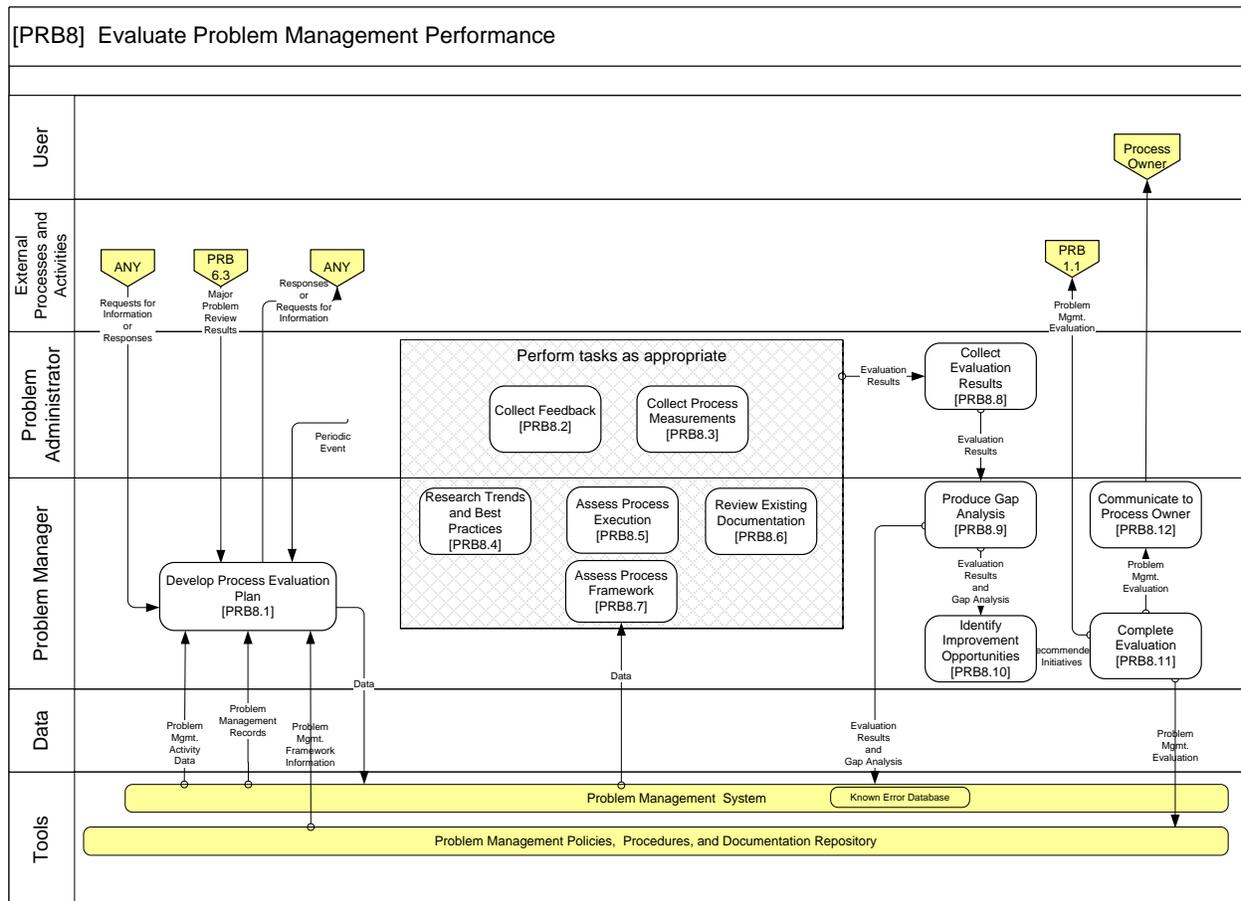


Figure 41 - PRB8 Workflow

8.7.8.1 TASKS

- Develop Process Evaluation Plan
- Collect Feedback
- Collect Process Measurements
- Research Trends and Best Practices
- Review Existing Documentation
- Assess Process Execution
- Collect Evaluation Results
- Produce Gap Analysis
- Identify Improvement Opportunities
- Complete Evaluation
- Communicate to Process Owner

8.8 Roles

Role Name	Brief Role Description and Responsibilities
Problem Management Process Owner	<p>The Problem Management Process Owner is the sponsor of the process and holds the responsibility and executive authority for the overall process results across the enterprise. This authority spans across all internal and external organizations who participate in the process.</p> <p>The Problem Management Process Owner is responsible for ensuring that the process is fit-for-purpose and that all activities defined within the process are undertaken. This responsibility includes oversight of process quality, continual improvement, and compliance with organizational mandates and performance targets.</p> <p>The Problem Management Process Owner is vested with responsibility for all aspects of process design, Change Management, performance metrics, policies, and process automation technologies within Problem Management to ensure compliance with organizational objectives.</p>
Problem Manager	<p>The Problem Manager is responsible for the quality and integrity of the Problem Management process. He/she is the interface to the Service Owners and other process managers. The Problem Manager is the focal point for escalation from other processes. The Problem Manager's responsibilities include:</p> <ul style="list-style-type: none"> Ensuring post-review of Major Problems Ensuring reactive and proactive management of IT Problems and Known Errors Coordinating efforts of all Problem Analysts, including suppliers and external teams, to ensure timely resolution of Problems Owning the Known Error Database and ensuring its maintenance Facilitating Problem quality/audit reviews
Problem Administrator	<p>The Problem Administrator supports the Problem Management Process Manager by managing records, tracking action items and providing process-related reports.</p>
Problem Analyst	<p>The Problem Analyst uses technical knowledge and subject matter expertise to identify Incident trends, identify Problems, determine the root cause of Problems, and initiate appropriate actions. These actions include:</p> <ul style="list-style-type: none"> Identifying the need for a Change Request to resolve the Problem Creating a workaround Performing Problem determination Performing root cause analysis Executing a workaround, if applicable Executing a resolution, if applicable Updating the Problem ticketing system with the root cause and permanent resolution information Updating the closure portion of the ticket, ensuring the cause code reflects the actual cause of the Problem, and all documentation is complete Providing effective resolution to the Problem in accordance with the priority service level and DoD/DoN governance Initiating a permanent fix for the Problem Identifying resolved Problems as candidates for inclusion in the KEDB

Table 9 - Problem Management Roles

Activity	Problem Management Process Owner	Problem Manager	Problem Admin	Problem Analyst
[PRB1] Establish Problem Management Framework	A/C	R/C	I	C
[PRB2] Identify and Log Problem	A	R	I	R/C
[PRB3] Categorize and Prioritize Problem	A	C	I	R
[PRB4] Investigate and Diagnose Problem	A	I	I	R
[PRB5] Resolve Problem	A	C	I	R
[PRB6] Close and Review Problem	A	R	I	C/I
[PRB7] Monitor, Manage and Report Problems	A	R	R	C/I
[PRB8] Evaluate Problem Management Performance	A	R	I	I

Table 10 - Problem Management RACI

Role	Government	Vendor
Problem Management Process Owner	X	
Problem Manager	X	X
Problem Administrator		X
Problem Analyst		X

Table 11 - Government/Vendor Role Assignment

8.9 Information Work Products

The work products indicated in the process workflows include:

- Architecture Baselines and Roadmaps
- Candidate Problem or Improvement Data
- Change Implementation Communication and Progress Data
- Change Implemented
- Change Information
- Change Request
- Change Requests
- Change Schedule
- Charter

- Communication
- Configuration Information
- Data
- End RCA Activities
- Evaluation Results
- Evaluation Results and Gap Analysis
- Event Information
- Events
- Incident Information
- Incident Management Model
- Incident Trends
- Information of Interest
- Input
- Inter-Process Relationships
- IT Portfolio
- Knowledge Information
- Known Error
- Known Error Record
- Known Error Records
- Major Problem Review Results
- Notification
- Notification that Workaround or Root Cause Could Not Be Found
- Policies, Standards, and Models
- Problem
- Problem Action Directive
- Problem Action Notifications
- Problem Action Results
- Problem Data
- Problem Information
- Problem Management Activity Data
- Problem Management Evaluation
- Problem Management Framework Information
- Problem Management Records
- Problem Management Technology Plans
- Problem Record
- Problem Record Audit Issues
- Problem Record Audit Results
- Problem Records

- Problem Reports
- Problem (Resolution)
- Problem Resolution Action Plan
- Problem Status
- Project Proposal
- Proposed Solution
- Recommended Initiatives
- Records of Interest
- Report Design
- Report Requirements
- Request for Problem Status and Information
- Requests for Information or Responses
- Responses or Requests for Information
- Scan Request
- Service Improvement Input
- Service Outage Analysis
- SLAs, OLAs, UCs
- Solution Action Plan Review Response
- Standard Report
- Standard Report and Report Design
- Supplier Information
- Supplier Product and Service Information
- Unmatched Incidents
- Workaround Data

8.10 Performance Metrics

- Difference between HP problem detection and Government problem detection
- Problem ticket creation time
- Number of times priorities have changed, and reasons why
- First pass approval percentage
- Length of time at each step from problem resolution recommendation to problem closure
- Quantity and qualifications of Major Problems being tracked

8.11 Organizational RACI

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
PRB	Problem Management		NCF			A					
PRB1	Establish Problem Management Framework		NCF			R	R	I	I		
PRB2	Identify and Log Problem	Licenses for Tool Access, SM7 HP Conduct Licensing Gap Analysis and Inform Gov Problem Ticket generation Directive and Artifact Portal for Policy Publication Metrics: Difference between HP and Government Problem detection tickets, Monthly Problem Ticket creation time	NCF			R	C	R	R		

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
PRB3	Categorize and Prioritize Problem	Prioritization Schema & methodology, Government led Meetings: Drumbeat, 2 weeks Policies published on Portal Problem records in SM7 Metrics: # of times priorities have changed and reasons why, SM7 Problem records	NCF			R	R	R	C		

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
PRB4	Investigate and Diagnose Problem	Sharing of Non NMCI Known Errors with NMCI, SM7, KM Team Meetings: Drumbeat Problem records in Remedy and SM7 Metrics: # times priorities have changed and reasons why	NCF			R	R	R	R	R	

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
PRB5	Resolve Problem	Define Interfaces (MOU, MOA) to external service providers: DISA, WNY ITA... Recommended Solution to Government RFC Drumbeat Meetings Policies on Portal Problem Records in SM7 Metrics: First Pass Approval %, SM7 record, Quarterly	NCF			R	R	R	R	R	

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPA WAR	Tech Authority
PRB6	Close and Review Problem	Definition and extra requirements for Major Problem, PRB SOP, Government Led Meetings: Major Problem review Polices on Portal Problem records in SM7 PRB Module Metrics: Length of Time at each step from problem resolution recommendation to Problem Closure, SM7, Semi Annual Quantity and Qualifications of Major Problems being tracked, SM7, Quarterly	NCF			R	C	R	C		

ID	Activity	C2 Summit Defined Interfaces	Gov Owner	DONCIO: DON IT Policy	SPONSOR	FCC 10th Fleet	PMO	ES Segment	TXS Segment	SPAWAR	Tech Authority
PRB7	Monitor, Manage, and Report Problem Management		NCF			R	I	R	R		
PRB8	Evaluate Problem Management Performance		NCF			R	I	R	R		

Table 12 – Problem Management RACI Chart

9. CONFIGURATION MANAGEMENT [CM]

9.1 Process Purpose

At a high-level, the purpose of Configuration Management is to identify, control, record, report, audit and verify configuration items, including versions, baselines, constituent components, their attributes, and relationships, and to protect their integrity throughout the lifecycle as required to control the services and IT infrastructure. It is important to mention that CoSC/NGEN CM is focused on a subset of the overarching Department of Defense (DoD) program lifecycle CM. CoSC/NGEN CM is *not* the engineering aspects of DoD program lifecycle CM, nor is CM encompassing Change Management or Release & Deployment Management (both processes are separate and distinct ITSM processes). CoSC/NGEN CM includes the ITSM CM process elements only.

The purpose of this document is to describe the current state of the Navy Marine Corps Intranet (NMCI) CM process Government capabilities as of May 2010, with specifics related to the government C2 touch points in the process. A target state will be prepared as the second Decision Based Workflow (DBW) deliverable in order to perform a gap analysis between where NMCI is now and where NGEN is headed.

The NMCI contract with Hewlett-Packard (HP) is a service contract. This means that the NMCI Program Office (PMW 205) purchases IT services only from the service provider, HP. PMW 205 does not direct, control, or execute any activities of the NMCI CM process. Once again, PMW 205 has identified government process touchpoints where the government participates for the purpose of C2/SA in the current environment.

The process and tools used by HP as the service provider to perform CM are wholly owned by HP and are not visible to NGEN or NMCI Government stakeholders. PMW 205 does not have knowledge of, or insight into, HP's CM processes, practices, data, tools, or procedures for NMCI. Our efforts are geared around trying to understand the current state process, tools, data, and the necessary government touch points for that, as best as possible.

The next step in the DBW is to determine the level of detail required for design and development of the target state CM process activities for the NGEN Program Office (PMW 205) to direct, control, or execute in alignment with the NGEN Acquisition Strategy.

9.2 Process Policies

9.2.1 DoD and DON Policies

This section defines the key DoD and DON Policies that govern the process:

Policy #	Policy Name	Requirement
----------	-------------	-------------

MIL-HDBK-61A(SE)	Configuration Management Guidance	<ul style="list-style-type: none"> Serves as reference for DoD CM managers on how to ensure the application of product and data CM in each life cycle phase Calls out the use of data models, data dictionaries, and CM data object templates as a framework for translating and communicating configuration information in an integrated data environment Defines the CM Plan (CMP) as the document that captures how CM will be implemented
NAVSO P-3692	Independent Logistics Assessment (ILA) Handbook	<ul style="list-style-type: none"> Calls out CM Assessment Criteria as part of Milestone Reviews Key areas: requirements, processes, contractual language, establishment of a Configuration Control Board (CCB), audits, interface controls, and Configuration Status Accounting
DoD Regulation 5000.02	Operation of the Defense Acquisition System	Key areas: requirements, processes, contractual language, establishment of a Configuration Control Board (CCB), audits, interface controls, and Configuration Status

This section defines the specific policies developed to govern the process for NGEN:

Policy #	Policy Name	Requirement
NMCI Contract N00024-00-D-6000	Attachment 9 Configuration Management	<ul style="list-style-type: none"> Identify Configuration

9.3 Process Outcomes

The key qualitative and quantitative outcomes (objectives) of the Process are:

The objectives of the Configuration Management process are:

- Configuration Identification – Create and maintain requirements and classification of configuration item (CI) types, attributes, relationships and data integrity rules.

- Configuration Control – establish criteria and process for managing operational baselines which will include defined criteria for reviewing change information for CI accuracy, risk and impact.
- Configuration Status Accounting – establish reporting criteria and capabilities that enable effective configuration status accounting and reporting.
- Configuration Verification and Audit – establish processes and procedures for verification and audits that ensure CI information matches the physical reconciliation data, that naming conventions are followed, that Definitive Media Library (DML) and secure repositories agree with the CI information and that Requests for Change (RFCs) match the composition of the CI.

9.4 Process Scope

The scope of the Configuration Management (CM) process is for operational support of IT services. Configuration Management (CM) ensures that selected components of a complete service, system or product (the configuration) are identified, baselined and maintained and that changes to them are controlled. It also ensures that releases into controlled environments and operational use are done on the basis of formal approvals. It provides a configuration model of the services, assets and infrastructure by recording the relationships between service assets and configuration items.

9.4.1 Includes

- Planning
- Identification
- Control over the change of CI data
- Status accounting
- Verification and auditing
- Identify and account for all infrastructure category items
- Provide accurate information and support Service Management process areas
- Ensure authorized CIs are accepted and recorded from installation to end of life
- Validate existence of CIs and that they are recorded correctly
- Provide a single source of accurate CI information to facilitate metrics reporting
- Identify the logical/functional relationships between components

9.4.2 Excludes

- Maintaining Asset Details
- Asset Management, although the interface to this process must be managed

- Change Management, although the interface to this process must be managed
- Release and Deployment, although the interface to this process must be managed
- Approving changes to CIs
- Tracking solution development efforts to be deployed
- Approval of changes within the Enterprise
- Scheduling and deployment approval

9.5 Process Interfaces

This section summarizes the interfaces between the process and other ITSM processes. A direct interface occurs when a process provides a work product (input or output) to another process.

Primary interfaces with other processes include the following:

- Asset Management
 - Configuration information
 - Reconciliation information
 - Asset Management Plan
- Release and Deployment
 - Request for Change (RFC)
- Change Management
 - Configuration Item (CI) package information

The following diagram graphically depicts process interface relationships and work products:

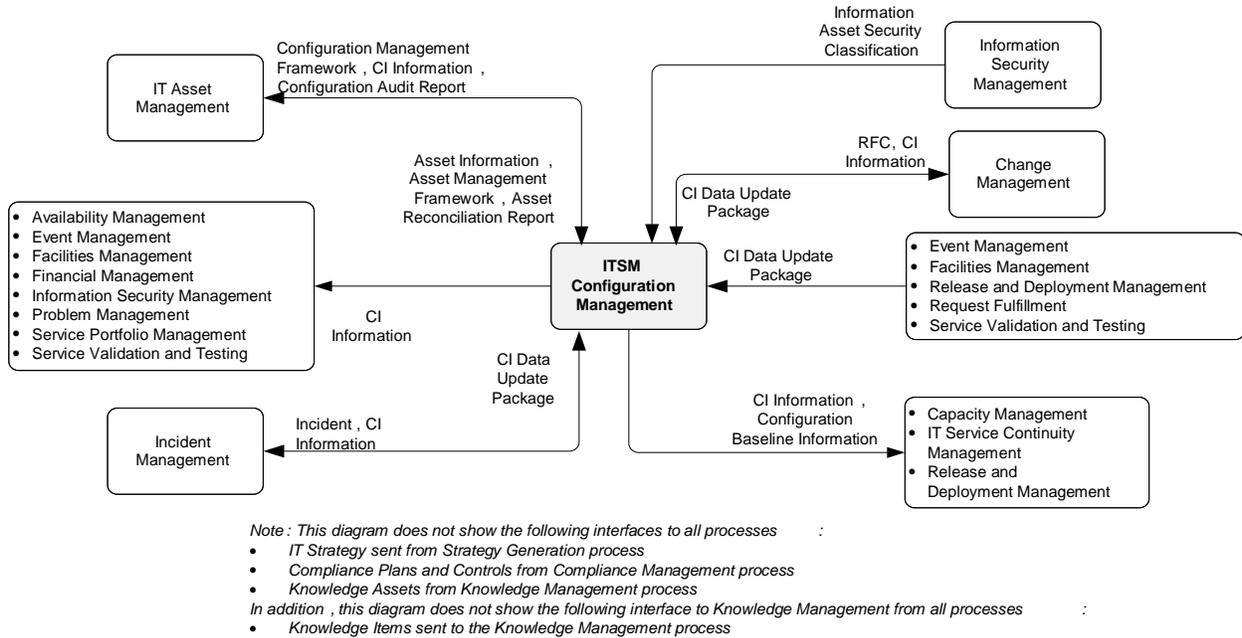


Figure 42 Configuration Management Process Interface Diagram

Process Functional Requirements

This section defines all of the NGEN Functional Area Requirements applicable to the process in a requirements traceability matrix (RTM).

ID	Date Recorded	Functional Area	Requirement
1	2/15/2012	CoSC Contractor CM	Identify and account for all infrastructure category items.
2	2/15/2012	CoSC Contractor CM	Provide accurate information and support to the Service Management process areas.
3	2/15/2012	CoSC Contractor CM	Ensure that only authorized and identifiable CIs are accepted and recorded from installation to end of life (EOL).
4	2/15/2012	CoSC Contractor CM	Facilitate adherence to legal and contractual obligations for software licensing.
5	2/15/2012	CoSC Contractor CM	Validate existence of CIs and make sure that they are correctly recorded.

6	2/15/2012	CoSC Contractor CM	Provide CM-related education programs to support and control processes.
7	2/15/2012	CoSC Contractor CM	Provide a single source of accurate CI information to facilitate metrics reporting.
8	2/15/2012	CoSC Contractor CM	Identify the logical/functional relationships between components that define the IT services.
9	2/15/2012	CoSC Contractor CM	Maintain not only relevant usage information about the assets themselves, but also information about relationships between assets.
10	2/15/2012	CoSC Contractor CM	Maintain the Definitive Solution Library (DSL) to hold and protect the authorized bundles of all software CIs, engineering documents, licensing, and circulating draft documents.
11	2/15/2012	CoSC Contractor CM	Provide and maintain repositories to be controlled by CM including: uCMDB, CMDB and SFCMDB.
12	2/15/2012	CoSC Contractor CM	The NMCI contract requires the implementation of a CM system, including an asset inventory of all hardware and software. It also requires that the items in the asset inventory are maintained by CMDB and its federated link to Asset Manager (AM).

1.12 Process Activities

1.12.1 Process Diagram

This section defines the high level process activities in a standardized swim lane format:

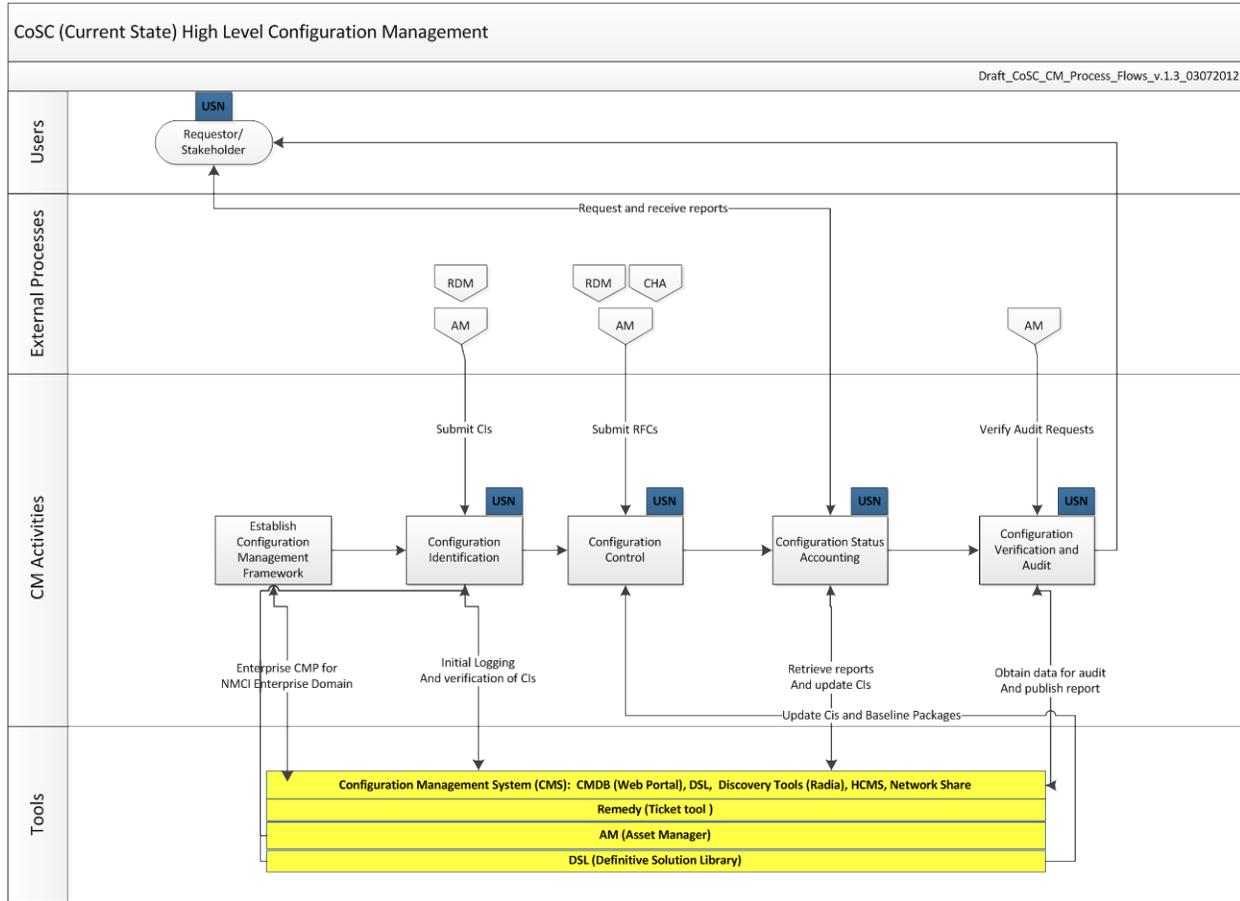


Figure 2: Configuration Management Process Model

*Note: Additional guidance on creating the Process Diagram is provided in Appendix C.

1.12.2 Process Activity Descriptions

This section defines the details of each activity in the process model:

CM-1	Establish Configuration Management Framework	
Description:	<ul style="list-style-type: none"> Create and maintain the Configuration Management Framework. 	
Supplier:	<ul style="list-style-type: none"> Configuration Management 	
Inputs:	<ul style="list-style-type: none"> Enterprise Configuration Management Plan for NMCI Enterprise Domain 	
Standard Operating Procedures	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> CM_Establish_Process Framework_SOP_v1.0 	

(SOPs):	
Outputs:	<ul style="list-style-type: none"> • Updates to Contractor CMP • Scope, Objectives, Goals, Purpose, Capabilities • Roles and Responsibilities • Processes and Procedures • Measurements and Controls • Tool Requirements • Training and Communications
Customer:	<ul style="list-style-type: none"> • CoSC Contractor • PM NEN
Assumptions:	<ul style="list-style-type: none"> • That current contractor is maintaining and updating the CMP to reflect changes to the current CM schema.

CM-2	Configuration Identification	
Description:	Identify and define CI types.	
Supplier:	<ul style="list-style-type: none"> • Contractor Release and Deployment • Contractor Asset Management 	
Inputs:	<ul style="list-style-type: none"> • Request for Change (RFC) post ECCB • Asset CIs 	
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • CM_Configuration_ Identification_SOP_v1.0 	
Outputs:	<ul style="list-style-type: none"> • Logging of CI into CMDB • Register CI after verification 	
Customer:	<ul style="list-style-type: none"> • Asset Management • Requestor/HP Engineering 	
Assumptions:	<ul style="list-style-type: none"> • That all relevant asset CIs are being entered into the CMDB 	

CM-3 Configuration Control	
Description:	Update and maintain CIs.
Supplier:	<ul style="list-style-type: none"> • HP Release and Deployment • HP Asset Management • HP Change Management
Inputs:	<ul style="list-style-type: none"> • DSL entry of approved RFC by notification from RDM entry into Remedy • If there is a BOM approval and hardware order placed • ECCB approval and documents entered into DSL
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • Hewlett Packard Enterprise Services Configuration Management Plan (HPES CMP) • CM_Configuration_Control_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • Service continuity and spares check for AM
Customer:	<ul style="list-style-type: none"> • Contractor Asset Management • Contractor Engineering • Government Touch Point-PM NMCI/CoSC Engineers are involved with CSR and collaboration on solution reviews
Assumptions:	Contractor and their engineering are accountable for the Configuration Control Process. NMCI/CoSC government personnel hold voting roles on the ECCB.

CM-4 Configuration Status Accounting	
Description:	Makes CI and CMS information available to authorized requestors.
Supplier:	<ul style="list-style-type: none"> • Configuration Management
Inputs:	<ul style="list-style-type: none"> • Stakeholder requests report
Standard Operating Procedures	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • CM_Configuration_Status_Accounting_SOP_v1.0

(SOPs):	
Outputs:	<ul style="list-style-type: none"> • Report • Lifecycle Status Check report to Asset Management if there is a BOM entry
Customer:	<ul style="list-style-type: none"> • Government Touch Point- Government is the consumer of this report • Asset Management • Requestor
Assumptions:	Government is requestor of the report that is done through CDRL. The contractor controls the information and tools for the report.

CM-5 Configuration Verification and Audit	
Description:	Verifies how well the contents of the CMS match the IT infrastructure by performing audits.
Supplier:	<ul style="list-style-type: none"> • HP Configuration Management • HP Asset Management
Inputs:	<ul style="list-style-type: none"> • HP Asset Management disposition information • Report Request
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • HPES CMP • CM_Verification and Audit_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • Requested report
Customer:	<ul style="list-style-type: none"> • Requestor/Stakeholder
Assumptions:	Contractor determines the parameters of audits (spot check, ad hoc, canned).

ORGANIZATION AND ROLES

Roles and Organizations

This section defines the CM roles (e.g. Process Owner, Process Manager, Analyst, etc.) and functional organizations (e.g. DA/TA, Logistics, NetOps, etc.) involved in executing the process. This can be in the form of a narrative, table(s), and/or organization chart(s).

1.14 R/A/C/I

This section contains a process-level RACI chart that shows the relationship between the activities and roles within the organization.

Processes may span departmental boundaries; therefore, procedures and work instructions within the process need to be mapped to roles within the process. These roles are then mapped to job functions, IT staff and departments. The Process Owner is accountable for ensuring process interaction by implementing systems that allow smooth process flow.

The Responsible, Accountable, Consulted, Informed (RACI) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks. Listed below are the roles that have been identified in the process.

R (Responsible) – A Responsible organization is involved in the daily execution of process activities. There may be more than one organization responsible for a given activity. Designating an organization as “Responsible” implies that they fall under the guidance and review of the “Accountable” party. Responsible organizations may or may not be organizationally aligned under the Accountable organization.

A (Accountable) – An Accountable organization serves as the overall owner of process quality and end results. There should only be one Accountable organization per process activity.

C (Consulted) – A Consulted organization provides knowledge and/or information to an activity. These organizations function as “part-time” actors in the process by contributing to specific situations, providing insight to others, performing very clear tasks, etc.

I (Informed) – An Informed organization receives specific information about process execution, status, etc.

Process Activities	Current Contractor	Government Process Owner	Government Process Manager
Establish Configuration Management Framework	RACI	I	I
Configuration Identification	RACI	I	I
Configuration Control	RACI	I	I
Configuration Status Accounting	RACI	I	I
Configuration Verification & Audit	RACI	I	I

1.15 Resource Requirements

1.15.1 Resources Required to Execute the Process

Resource Type	Skill	Grade/Skill Level	No. FTEs
Government	Configuration Management Process Owner	Sr.	1
Government	Configuratin Management Process Manager	Sr.	1

Stakeholder Resources

Resource Type	Skill	Grade/Skill Level	No. FTEs
CM Analyst	Competency SME	Government	1
CM Database Administrator	Database Administration	Contractor	1
ITSM-Process Support	Process development	Contractor	1
CM Analyst	Support design of interim CMDB implementation. Support FCA and PCA activities.	Contractor	4

1.15.2 Knowledge, Skills and Abilities (KSAs)

Each role associated with the Configuration Management process has specific knowledge, experience and training requirements, some of the general KSA considerations are as follows:

- Familiarity with PM NEN Documentation to include: NGEN Configuration Management Plan (CMP) and the Systems Engineering Plan (SEP).
- Familiarity with Government Policies: MIL-HDBK-61A and DoD Regulation 5000.02.
- Experience in the following Configuration Management areas (not limited to): requirements management, system development, overall software/system engineering processes, Information Assurance, system installs, software release management, and IT infrastructure management.
- Experience with the Configuration Management process including: CM in Acquisition, Life Cycle CM Sustainment, Operational CM (including System and CIs), Establishment of Baselines, Status Accounting, and Data Delivery.
- Strong written and verbal communication skills.

1.15.3 Identification and Training of Government Personnel

Training and Development requirements for Configuration Management have yet to be determined. This information will become clear after the SOPs are created to articulate the government's C2/SA touch points, the pilot has been performed, and the SOPs have been updated. Training is performed similarly to other processes, such as Change Management, by

having the stakeholders involved in the working sessions, the creation of the materials, and by providing the materials in a final Communications Package.

DATA AND INFORMATION

Data and Information Requirements

This section summarizes the data and information management requirements of the process, and identifies the key consumers (e.g. roles, organizations) of process information work products.

1.17 Information Work Products (IWPs)

This section details the process IWPs including their usage and target audience. IWPs will be used either internally within the process which generated them, or by another process which receives the work product. IWPs will contribute to the Command and Control (C2) analysis and decisions used in managing the process:

IWP	Target Audience	Description/Usage
CDRL3.03-1	Engineering	Provide an accurate network configuration baseline report within 30 calendar days of contract start and updates within 10 calendar days of all system changes or upgrades.
Contractor Configuration Management Plan	Contractor and Government Stakeholders	Contractor owned document that defines the scope, objectives and direction of the current Configuration Management effort.

1.18 Reporting Requirements

This section defines process reports:

Report Elements	Amplifying Information
Report Name	CDRL 3.03-1
Report Description	Provides updates to network configuration baseline.
Report Audience	Government/Engineering
Report Owner	Requestor/Stakeholder
CSFs In Report	Control of the baselines and IT architecture

Report Elements	Amplifying Information
KPIs/Metrics Used In Report	No KPIs or metrics determined.
Report Frequency	As requested, however, CDRL 3.03-10 calendar days after a system change.

PERFORMANCE MANAGEMENT

Current Process Metrics

This section lists the Critical Success Factors (CSFs) and Key Performance Indicators (KPIs) used to baseline and measure process transition success.

Effective day-to-day operation and long-term management of the process requires measuring the process. Reports must be defined, produced and distributed to enable the management of process-related issues and initiatives. Daily performance management occurs with the process manager. Long-term trending analysis and management of significant process activities occurs at the process owner.

A powerful vision and well-defined mission statement are critical to defining enterprise goals and objectives. Process governance starts with establishing objectives for the enterprise, and continuous performance management aids direction of activities aligned with those set objectives. The Process Owner is responsible for measuring and providing value-based reporting. Critical Success Factors (CSFs) identify the most important actions for achieving control over the process and Key Performance Indicators (KPIs) measure whether or not a control is meeting its objective.

Continual service improvement depends on accurate and timely process measurements and relies on obtaining, analyzing, and using information that is practical and meaningful to the process. Measurements of process efficiency and effectiveness enable NGEN management to track process performance and improve overall end-user satisfaction.

The following table summarizes the relationships between process CSFs and KPIs. See Appendix D for a complete list of CSFs and KPIs.

Metrics for the current state of the Configuration Management process have not been defined.

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	TBD	1	TBD
		2	TBD
		3	TBD
		4	TBD
		5	TBD
		6	TBD
		7	TBD
2	TBD		TBD
			TBD
			TBD
			TBD

*Note: Additional metric details incl. threshold and objective values are defined in the SOPs.

1.20 Desired Metrics and Compliance Controls

Metrics have not been determined for the current state of the Configuration Management process, however, the CSFs and KPIs listed below represent what controls may be in place with the current contractor.

Critical Success Factors (CSFs)

- CSF-1 Maintain a complete and comprehensive Configuration Management Plan
- CSF-2 Maintain a standard model to name, categorize and establish relationships between Service Assets and CIs
- CSF-3 Control the relevance of information in the Configuration Management System (CMS)
- CSF-4 Provide Service and Asset visibility and situational awareness through reporting on asset and configuration status and relationships
- CSF-5 Maintain the accuracy of information in the CMS by performing regular verification and audits
- CSF-6 Resolve data integrity exceptions found in the CMS

Key Performance Indicator (KPIs)

- KPI-1 Proportion of Services managed in the CMS to known unmanaged services
- KPI-2 Proportion of managed CIs to known unmanaged CIs
- KPI-3 Proportion of correctly names CIs to incorrectly named CIs
- KPI-4 Proportion of owned CIs to un-owned CIs
- KPI-5 Proportion of CMS data sources to known non-CMS data sources
- KPI-6 Proportion of Controlled to Uncontrolled CIs
- KPI-7 Proportion of CIs with financial information to CIs without financial information
- KPI-8 Proportion of authorized CIs to unauthorized CIs
- KPI-9 Proportion of Software in use to Software licensed KPI-10 Proportion of verified CIs in the CMS to unverified CIs
- KPI-11 Proportion of drift from last approved baseline
- KPI-12 Average time to resolve CMS data integrity exceptions
- KPI-13 Proportion of CIs with data integrity exceptions to CIs without

Operational Metrics

- Total Number of CIs in CMDB
- Number of CIs audited
- Number of CI Errors Discovered
- Configuration Management Tooling Support Level
- Configuration Management Process Maturity
- Number of CI changes
- Number of CI changes without corresponding RFC
- Number of Incidents related to inaccurate CI information
- Number of Change failures related to inaccurate CI information
- Number of Services operating with incomplete CI information
- Number of Services in service catalog
- Number of CIs without assigned ownership

Tolerance Levels

CMDB Accuracy Ratio

TOOLS AND TECHNOLOGY

Tool Requirements

This section defines key tool automation capability, interface, and interoperability requirements:

Requirement	Process Activity
Repository to store CIs to include: baseline information, documents, asset information, and solution packages.	<p>1.0 – Configuration Identification 1.1 Identify new CIs by assigning ID, update current status of already identified CIs.</p> <p>2.0-Configuration Control 2.1 Maintain control over CIs by updating status to include locking baselines, documentation and solution package updates.</p> <p>3.0-Configuration Status Accounting 3.1 Provide reports for specified data with reporting information being taken from associated database.</p> <p>4.0-Configuration Verification & Audit 4.1 Conduct audits against CIs and changes.</p>

1.23 Tools Used to Support the Process

This section defines the requirements met by COSC tools today and documents key gaps:

Requirement	COSC Tool Used Today	Measure -ment	Gap	Recommendation
Configuration Management Database-database for storage of Configuration Items	uCMDB, DSL CMDB, SFCMDB, NetART, HCMS	Partially Meets	Multiple CMDBs not federated. Harris IT's CMDB (HCMS) is standalone but covers all network devices in the environment (25,000+) DSL CMDB is standalone. Government does not have access to uCMDB or HCMS.	Migrate to SM7, Program Level CMDB (CMPRO) Obtain continuous data extractions from each CMDB within then environment.

INTEGRATION AND VALIDATION

Interface Requirements

This section defines the key interfaces with other processes, tools, governance bodies, and resources (service owners, vendors).

Most, if not all ITSM processes rely upon configuration management to perform activities to manage documents, software, hardware and baselines and their respective changes. The Configuration Management lifecycle tasks, standards, and activities must be adopted and integrated in all ITSM process activities related to the identification, control, accounting, validation and auditing of all configuration items.

Interface ID	Interface Description
1	TBD

1.24 Integration Approach

1.24.1 Use Case Selection

This information will be gathered during the Process Pilot.

1.24.2 Workshops and Simulations

This information is to be determined.

1.25 Validation Results and Remediation

This information is to be determined.

Error ID	Validation Scenario	Step Description	Type of Error Found	Error Description
		TBD	TBD	TBD

10. RELEASE AND DEPLOYMENT MANAGEMENT [RDM]

10.1 Process Purpose

The purpose of the Release and Deployment Management is to process and prepare authorized release packages for deployment, to place releases and other desired changes into their target environments, and to activate them in order that the functionality and operational improvements they contain create their intended value.

A release is defined as any collection of hardware, software, documentation, processes, or other components that are required to implement one or more approved changes to IT services.

Definition of Deployment: “movement of new or changed hardware, software, documentation, or process, etc to the live environment.”

10.2 Process Policies

10.2.1 DoD and DON Policies

This section defines the key DoD and DON Policies that govern the process.

The policies governing the Release and Deployment Management process are listed in the main body of the PWS.

10.2.2 Process-Specific Policies

This section defines the specific policies developed to govern the process for NGEN.

Policy Ref.	Policy Name	Requirement
TBD	TBD	TBD

10.3 Process Outcomes

The key qualitative and quantitative outcomes (objectives) of the Process are:

- Risk is minimized for deployment to current services
- Customer and user satisfaction is increased once a deployment takes place
- Planning for deployments is improved, including resources and scheduling
- Only authorized releases are deployed to the live environment
- A new capability is introduced to support business and warfighting goals such as new functionality, minimized risk to existing functionality and service, or audit capability

- The production environment and IT services are protected through the use of formal procedures and checks that include risk assessment and mitigation of risks
- The impact of scheduled outages to the live environment is reduced by bundling multiple changes when possible
- A holistic view of multi-faceted changes that involve activities of multiple organizations is created.
- Releases provide service offering that delivers the expected outcomes and value.
- The customer and stakeholder service requirements are well defined at the outset.
- Released services are fit for purpose and fit for use
- Requirements for releases are established and agreed with affected parties
- Releases of new or changed services and service components are planned
- Releases are designed
- Releases are tested prior to deployment
- Release information is communicated to affected parties
- New capability is introduced on a timely basis, and with minimized risk, disruption, and cost
- Transfers of service responsibility are affected on a timely basis, and with minimized risk, disruption and cost
- All parties involved in a deployment (for example, users of the capabilities being deployed, service providers performing the deployment) are appropriately prepared, trained and skilled to ensure successful deployment
- In the event of failures during deployment, contingency plans ensure the expected level of service quality is delivered
- Approved releases are deployed
- Integrity of hardware, software, and other service components is assured during deployment of the release.
- Unsuccessfully deployed releases are reversed.
- Deployment information is communicated to affected parties.

10.4 Process Scope

Release and Deployment Management covers the planning and direction of the deployment of all software, hardware, and operational processes, including related documentation and operating procedures into the live environment.

The changes that comprise the release are managed by Change Management, and their inclusion in the release can be determined by time, technology interdependencies, target, risk mitigation, organization, scale (multiple copies) or service dependencies. The design of the release will need to consider how rollout is achieved.

NGEN will provide a Systems Integration Environment (SIE) that will provide the ability to engineer, certify, and accredit complete network solutions prior to implementation. The SIE will be an end-to-end systems integration, modeling, and test environment for hardware, software, applications, etc.

To ensure that only tested, verified and authorized releases are introduced into the live environment, NGEN shall ensure that release management processes and tools facilitate the planning and direction of the rollout of software, related hardware, documentation, and operating procedures.

Deployment is primarily triggered by an instruction to roll out any approved combination of software, related hardware, documentation, and operating procedures to one or more defined targets (for example: systems, user groups) within constraints such as cost and time. An alternative trigger for the initiation of deployment relates to the transfer of the responsibility for one or more services between providers or across business or organizational boundaries. At the other end of the scale, the implementation work related to a change which impacts a single CI is also performed by this process.

The completion of each deployment is indicated when the stakeholders affirm that the expected outcomes of a deployment are achieved and a business-as-usual operational service state has been attained.

10.4.1 Includes

- Release design, creation, and testing
- Specifying the deployment model for a release. The deployment model provides a template of the activities and plans from which specific deployment instances can be customized for geography, scale, local conditions, and other factors
- Checking and testing training materials and incorporating them into the deployment model
- Verification of successful release package installation, including ensuring that the integrity of function has been maintained
- Roll back (also known as back-out) mechanisms and procedures
- Release installation and activation using the change management process
- Large hardware/software rollouts
- Bundling or batching of related changes using the change management process
- Protecting the live environment
- Deployment planning and co-ordination with affected parties
- Identification of resources (hardware, software, processes and procedures, and staff) to be deployed, or to be transferred between service providers
- Creating capabilities and procedures to support deployment activities, and to verify the readiness of and account for resources impacted

- Creating a plan for continuity of service in the event of service failure
- Execution of the deployment plan, including:
- Electronic distribution of software and other soft-copy items
- Invoking logistical movements for physical items
- Installing technical resources
- Activating the desired configuration
- Testing the installation against defined criteria (as provided in the Release Package and Change)
- Back out of installed items, when needed
- Delivering training
- Providing initial user assistance

10.4.2 Excludes

- Application Management (creation of functionality, usage procedures, training materials, and any other release deliverable)
- Management of change requests (Change Management)
- Logistics and movement of physical asset (Asset Management)
- Preparation and commissioning of the supporting environment (Facilities Management)
- Accounting for capital transfers and deployment expenditures (Financial Management)
- Program and project management techniques
- Updates to the CMS (Configuration Management)

10.5 Process Interfaces

This section summarizes the interfaces between the process and other ITSM processes. A direct interface occurs when a process provides a work product (input or output) to another process.

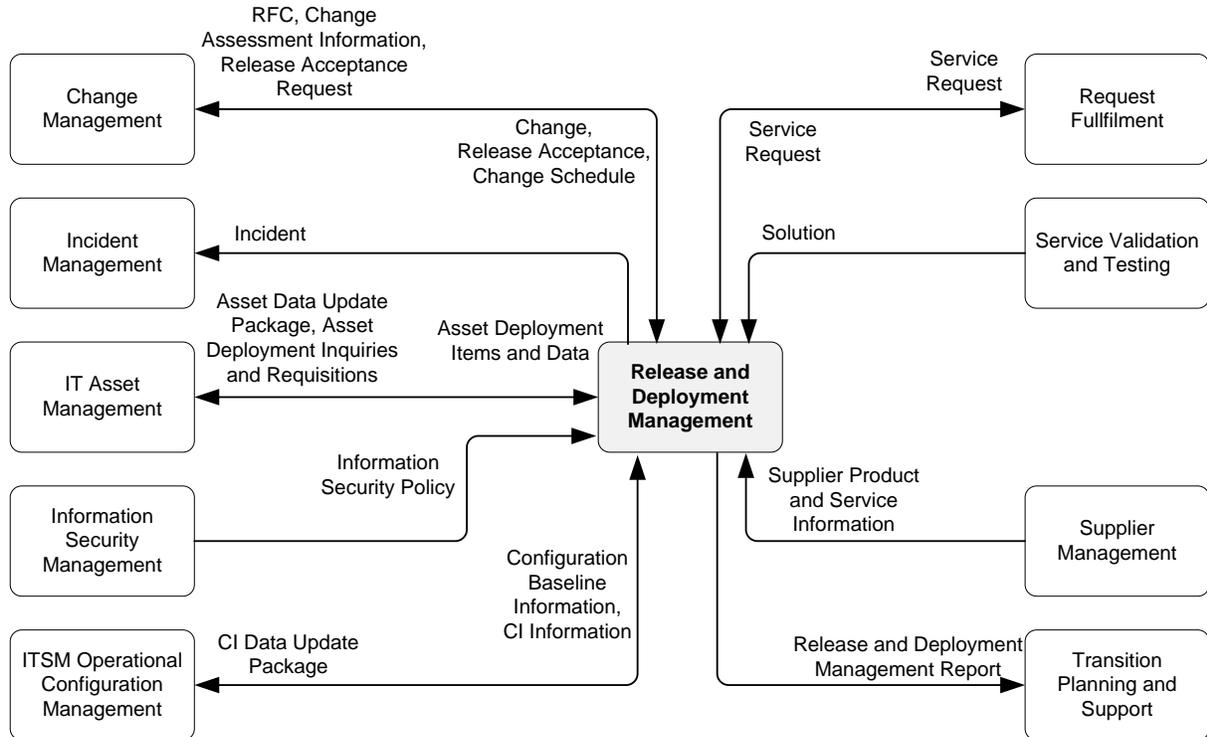
Primary interfaces to other processes include the following:

- Access Management / Information Security Management - Some deployments may include requests for access (Access Management) or information security modifications (Information Security Management).
- Asset Management – Release and Deployment Management provides release packages and other necessary data on controlled assets that are released to the NGEN enterprise. Asset Management provides information about assets being deployed and prepares assets before they are deployed.
- Change Management – Provides changes to be packaged into the release, as well as initial scheduling for the change(s) and deployment. If a failed deployment cannot be

successfully backed-out, a change request may need to go to Change Management to deal with the issue

- Compliance Management – Ensures adherence to Federal laws and regulations, DOD/DON policies, procedures, and NGEN stakeholder commitments.
- Configuration Management – Provides Release and Deployment Management with CI records and information for items being changed, modified, or removed. Release and Deployment Management provides CI update packages back to Configuration Management.
- Incident Management - If service is inadvertently interrupted during deployment, an incident is sent to Incident Management.
- Operations - Solutions deployed using Release and Deployment Management are handed over to be operated by Operations.
- Request Fulfillment - Service requests involving simple deployments are typically sent directly from Request Fulfillment to Request and Deployment Management.
- Application Management - After a solution has been accepted, it must be packaged for deployment by Release and Deployment Management. Alpha and beta versions may also be packaged in the same way. Solutions that do not require packaging may be provided directly to Deployment Management.

The following diagram graphically depicts process interface relationships and work products:



Note: This diagram does not show the following interfaces to all processes:

- IT Strategy sent from Strategy Generation process
- Compliance Plans and Controls from Compliance Management process
- Knowledge Assets from Knowledge Management process

In addition, this diagram does not show the following interface to Knowledge Management from all processes:

- Knowledge Items sent to the Knowledge Management process

Figure 1: Release and Deployment Management Process Interface Diagram

10.6 Process Functional Requirements

This section defines all of the NGEN Functional Area Requirements applicable to the process in a requirements traceability matrix (RTM).

ID	Date Recorded	Functional Area	Requirement
			TBD

10.7 Process Activities

10.7.1 Process Diagram

This section defines the high level process activities in a standardized swim lane format (the process model should always be aligned to the current version of the NNPDMD document):

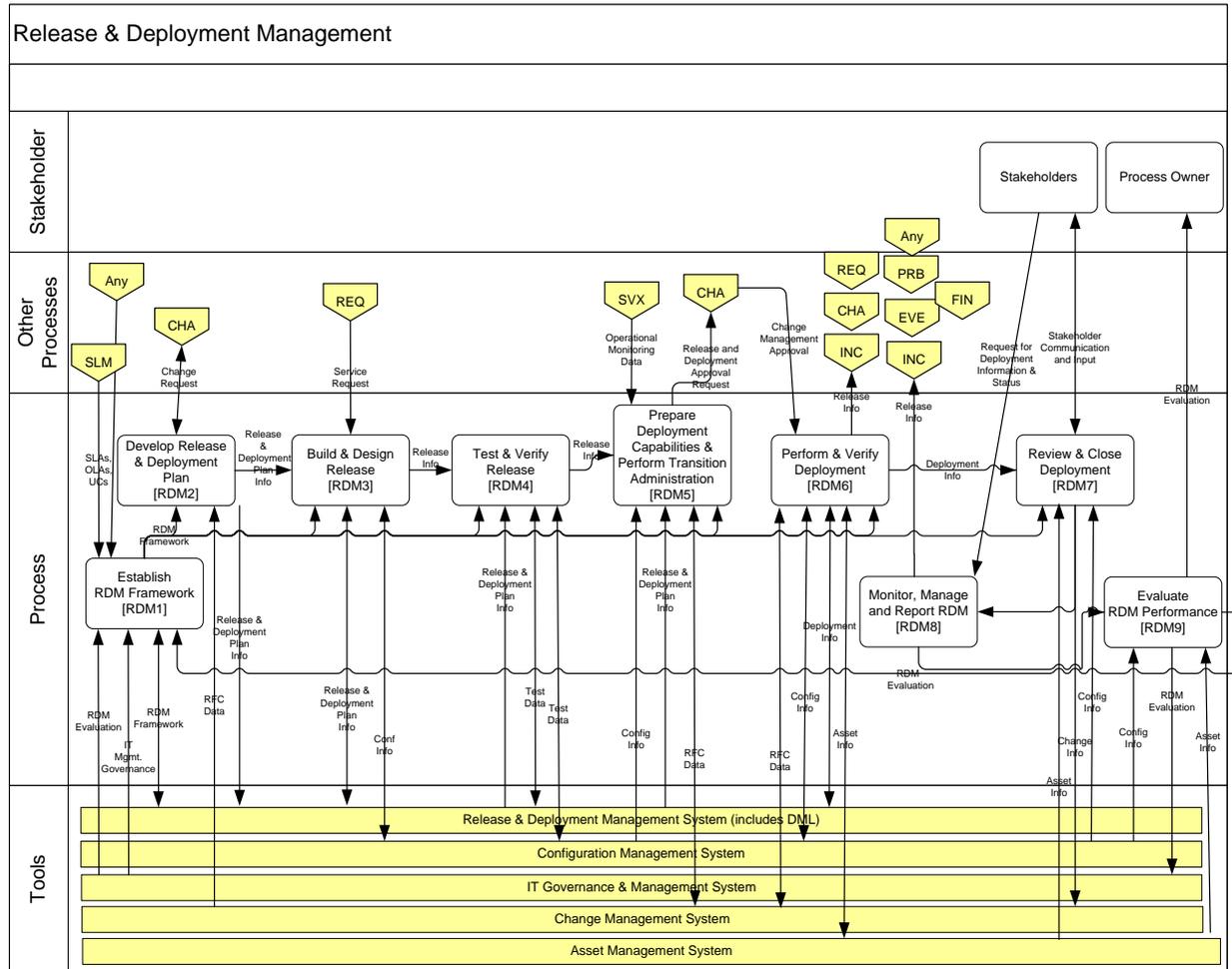


Figure 2: Release and Deployment Management Process Model

*Note: Additional guidance on creating the Process Diagram is provided in Appendix C.

10.7.2 Process Activity Descriptions

This section defines the details of each activity in the process model:

RDM 1	Establish RDM Framework	
Description:	This activity defines all direction, guidance, policies, and procedures for how the RDM process will be performed taking direction from DON policies, Mission objectives and IT strategy.	
Supplier:	<ul style="list-style-type: none"> • PM NEN RDM Manager • PM NEN RDM Owner • PM NEN Contractors and • PM NEN Stakeholders 	
Inputs:	<ul style="list-style-type: none"> • CoSC • CDRLs • Configuration Management Plan • DoDI 5000.2 • DoDI 8320.02 	
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • RDM_Establish_Process_Framework_SOP_v1.0 	
Outputs:	<ul style="list-style-type: none"> • Scope, Objectives, Goals, Purpose, Capabilities • Roles and Responsibilities • Processes and Procedures • Measurements and Controls • Tool Requirements / Gap Analysis • Training and Communications 	
Customer:	All NEN users	
Assumptions:	<ul style="list-style-type: none"> • Establishing the framework is a collaborative effort between the Government and Contractor • The Government will approve the final framework prior to 	

		implementation <ul style="list-style-type: none"> • The Framework will adopted by all Government and Contractor personnel to achieve standardization and quality objectives
--	--	--

RDM 2		Title Develop Release and Development Plan
Description:	This activity determines the approach for how each release is prepared and the type of deployment. The release planning covers the approach for building, testing and verifying the release, including the possible need for pilot deployments, as well as establishing a model for how the finalized release should be deployed.	
Supplier:	<ul style="list-style-type: none"> • Change Management 	
Inputs:	<ul style="list-style-type: none"> • Changes • Validation and test plans • Calendars and schedules • Risk Management • Release owner assigned • Configuration management 	
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • RDM_Develop_Release and Deployment_Plan_SOP_v1.0 	
Outputs:	<ul style="list-style-type: none"> • Deployment Plan • Pending and Scheduled changes • Updated Master Release Schedule • Risk Management Plans • Defined Deployment Model • Remediation and Back-Plans • Stakeholder Communication Plans • Identified CIs of assets affected by deployment 	
Customer:	Transition Engineering Team	

	Assumptions:	<ul style="list-style-type: none"> •
--	--------------	---

RDM 3	Build and Design Release	
	Description:	This activity determines what needs to be built for the release and how it will be assembled and deployed. Release build, installation, and rollback scripts are designed at a high level. Software and hardware components are obtained for the build activity and the test environment is created.
	Supplier:	<ul style="list-style-type: none"> • RDM Planning
	Inputs:	<ul style="list-style-type: none"> • Service Resilience Plans • Solution Design • Solution Assembly • Operational Documentation • Configuration Information • Asset Availability Information • Change Implementation Communication • Release and Deployment Management Report • Release Revision Request
	Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • RDM_Design and Build_Release_SOP_v1.0
	Outputs:	<ul style="list-style-type: none"> • Asset Deployment Inquiries and Requisitions • Implementation Progress Data • CI Data Update Package • Release • Release and Deployment Management Activity Data
	Customer:	Validation and Test
	Assumptions:	<ul style="list-style-type: none"> •

RDM 4	Test and Verify Release	
	Description:	Tests the built Release Package to determine if installation,

		configuration, and rollback work properly.
	Supplier:	<ul style="list-style-type: none"> • RDM Engineering
	Inputs:	<ul style="list-style-type: none"> • Release • Configuration Information • Asset Availability Information • Change Implementation Communication • Release Acceptance
	Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • RDM_Test and Verify_Release_SOP_v1.0
	Outputs:	<ul style="list-style-type: none"> • Asset Deployment Inquiries and Requisitions • Implementation Progress Data • Release Acceptance Request • Release • Release Revision Request • Release and Deployment Management Activity Data
	Customer:	Deployment Team
	Assumptions:	<ul style="list-style-type: none"> •

RDM 5 Prepare Deployment capabilities and Perform Transition Administration		
	Description:	In this activity, the deployment capabilities for each deployment are prepared.
	Supplier:	Validation and Test
	Inputs:	<ul style="list-style-type: none"> • Accepted Solution • Asset Availability Information • Configuration Information • Deployment Rework Directive • Release • Stakeholder Notification
	Standard Operating	SOPs Exist for This Activity? Yes

Procedures (SOPs):	<ul style="list-style-type: none"> RDM_Prepair_Deployment Capabilities and Perform Transition Administration_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> Asset Data Update Package Asset Deployment Inquiries and Requisitions Release and Deployment Information Deployment Items Manifest Release and Deployment Management Activity Data Training Master Software library
Customer:	Deployment
Assumptions:	<ul style="list-style-type: none">

RDM 6 Perform and Verify Deployment	
Description:	This activity executes all tasks necessary to complete the actual deployment. In this activity, the capability status would move from “Not Deployed” to “Deployed.”
Supplier:	<ul style="list-style-type: none"> Transition Administrator
Inputs:	<ul style="list-style-type: none"> Change Implementation Communication Configuration Information Deployment Items Manifest Deployment Rework Directive Release Service Request Service Request Response Solution Installed Stakeholder Notification
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> RDM_Perform and Verify_Deployment_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> Access Work Request Asset Asset Data Update Package

		<ul style="list-style-type: none"> • CI Data Update Package • Release and Deployment Information • Release and Deployment Management Activity Data • Deployment Rework Directive • Implementation Progress Data • Incident • Information Security Work Request • Solution Installed
	Customer:	End user
	Assumptions:	<ul style="list-style-type: none"> •

RDM 7 Review and Close Deployment		
	Description:	This activity reviews the tasks completed during deployments and determines that all objectives of the deployment plan were met. A management plan is established for outstanding risks, issues, incidents and known errors before the deployment is closed. Deployment is completed with a handover of the support to Service Operations.
	Supplier:	<ul style="list-style-type: none"> • Deployment Team
	Inputs:	<ul style="list-style-type: none"> • Implementation Progress Data • Incidents • Deployed changes
	Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • RDM_Review and Close_Deployment_SOP_v1.0
	Outputs:	<ul style="list-style-type: none"> • Customer Satisfaction Issue • Release and Deployment Information • Post-Deployment Analysis • Release and Deployment Management Activity Data
	Customer:	End user

	Assumptions:	<ul style="list-style-type: none"> •
--	--------------	---

RDM 8 Monitor, Manage and Report RDM	
Description:	This activity involves the overall monitoring of work within the process and reporting on specific items or general status to stakeholders.
Supplier:	<ul style="list-style-type: none"> • Stakeholders • End users
Inputs:	<ul style="list-style-type: none"> • Release Acceptance Request • Release Acceptance • Release and Deployment Management Report • Customer Satisfaction Results and Trends • Release and Deployment Management Activity Data • Report Request
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> • RDM_Monitor_Manage_Report_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> • Release and Deployment Management Activity Data • Release and Deployment Management Report • Stakeholder Notification
Customer:	RDM Process Owner RDM Process Manager Stakeholders
Assumptions:	<ul style="list-style-type: none"> •

RDM 9 Evaluate RDM Performance	
Description:	Identifies what improvements can be made to the Release and Deployment Management process using information from Post

Implementation Review (PIR).	
Supplier:	<ul style="list-style-type: none"> RDM Monitoring Stakeholders
Inputs:	<ul style="list-style-type: none"> Release and Deployment Management Operational, Service and Technical metrics
Standard Operating Procedures (SOPs):	SOPs Exist for This Activity? Yes <ul style="list-style-type: none"> RDM_Monitor_Evaluate_SOP_v1.0
Outputs:	<ul style="list-style-type: none"> Release and Deployment Management Evaluation
Customer:	RDM Process Owner, Manager, and Stakeholders
Assumptions:	<ul style="list-style-type: none">

ORGANIZATION AND ROLES

10.8 Roles and Organizations

This section defines the roles (e.g. Process Owner, Process Manager, Analyst, etc.) and functional organizations (e.g. DA/TA, Logistics, NetOps, etc.) involved in executing the process.

Role Name	Brief Role Description
Release and Deployment Management Process Owner	The Release and Deployment Process Owner is accountable to senior management for the proper design, execution, and improvement of the process. This role: <ul style="list-style-type: none"> Ensures that the process is being carried out, but does not run the day-to-day operation of the process Receives regular updates concerning the performance of the process and represents this process concerning all decisions being made by senior management

Release and Deployment Manager	The Release and Deployment Management Manager over see’s the day-to-day operations of Deployment Management. This role: Assign Process Responsibilities to Organizations Communicate and Deploy Framework Create Project Proposals Define Measurements and Controls Define Process Policies, Standards, and Conceptual Models Determine Process Data Requirements Determine Process Procedures Determine Process Relationships to Other Processes Identify Process Roles and Responsibilities
Release and Deployment Administrator	The Release and Deployment Administrator supports the Release Manager. This role: Manages records, tracking action items, and providing process-related reports

Table 1 - Release and Deployment Management Roles

10.9 R/A/C/I

This section contains a process-level RACI chart that shows the relationship between the activities and roles within the organization.

Processes may span departmental boundaries; therefore, procedures and work instructions within the process need to be mapped to roles within the process. These roles are then mapped to job functions, IT staff and departments. The Process Owner is accountable for ensuring process interaction by implementing systems that allow smooth process flow.

The Responsible, Accountable, Consulted, Informed (RACI) model is a method for assigning the type or degree of responsibility that roles (or individuals) have for specific tasks. Listed below are the roles that have been identified in the process.

R (Responsible) – A Responsible organization is involved in the daily execution of process activities. There may be more than one organization responsible for a given activity. Designating an organization as “Responsible” implies that they fall under the guidance and review of the “Accountable” party. Responsible organizations may or may not be organizationally aligned under the Accountable organization.

A (Accountable) – An Accountable organization serves as the overall owner of process quality and end results. There should only be one Accountable organization per process activity.

C (Consulted) – A Consulted organization provides knowledge and/or information to an activity. These organizations function as “part-time” actors in the process by contributing to specific situations, providing insight to others, performing very clear tasks, etc.

I (Informed) – An Informed organization receives specific information about process execution, status, etc.

Process Activities	Release & Deployment Management Process Owner	Release & Deployment Management Manager	Release Owner	Release Specialist	Deployment Specialist	Release and Deployment Administrator	Stakeholder
RDM1 Establish Release and Deployment Management Framework	R	A,C		I	I		
RDM2 Plan Release and Deployment Program		R,A	R,C,I	C,I	C,I		I
RDM3 Design and Build Release		I	R	A,C	C,I	C,I	
RDM4 Test and Verify Release	I	I	R,C,I	A,C,I	C,I		
RDM5 Prepare Deployment Capabilities and Transition Administration		R,C,I		C,A	A,C,I	A,C,I	
RDM6 Perform Deployment and Activate Service		C,I		C,I	R,A	A,C,I	
RDM7 Review and Close Deployment		R,A		C,I	C,I	C,I	
RDM8 Monitor, Manage, and Report Release and Deployment Management	I	R,A		C	C		
RDM9 Evaluate Release and Deployment Management Performance	C	R,A		I	I	I	

This Role based RACI is supplemented with an Organizational RACI which can be found in APPENDIX E.

10.10 Resource Requirements

10.10.1 Resources Required to Execute the Process

TBD

10.10.2 Knowledge, Skills and Abilities (KSAs)

TBD

10.10.3 Identification and Training of Government Personnel

TBD

DATA AND INFORMATION

10.11 Data and Information Requirements

This section summarizes the data and information management requirements of the process, and identifies the key consumers (e.g. roles, organizations) of process information work products.

10.12 Information Work Products (IWPs)

This section details the process IWPs including their usage and target audience. IWPs will be used either internally within the process which generated them, or by another process which receives the work product. IWPs will contribute to the Command and Control (C2) analysis and decisions used in managing the process:

IWP	Target Audience	Description/Usage
TBD	TBD	TBD

10.13 Reporting Requirements

This section defines process reports:

Report Elements	Amplifying Information
Report Name	Post Implementation Review (PIR)
Report Description	A review of changes selected by government stakeholders in CAB and ECCB
Report Audience	CAB and ECCB
Report Owner	Supplier
CSFs In Report	Overall RDM success rate
KPIs/Metrics Used In Report	Successful scheduled and unscheduled changes. Changes with problems and unsuccessful changes.
Report Frequency	Monthly

PERFORMANCE MANAGEMENT

10.14 Current Process Metrics

This section lists the Critical Success Factors (CSFs) and Key Performance Indicators (KPIs) used to baseline and measure process transition success.

Effective day-to-day operation and long-term management of the process requires measuring the process. Reports must be defined, produced and distributed to enable the management of process-related issues and initiatives. Daily performance management occurs with the process manager. Long-term trending analysis and management of significant process activities occurs at the process owner.

A powerful vision and well-defined mission statement are critical to defining enterprise goals and objectives. Process governance starts with establishing objectives for the enterprise, and continuous performance management aids direction of activities aligned with those set objectives. The Process Owner is responsible for measuring and providing value-based reporting. Critical Success Factors (CSFs) identify the most important actions for achieving control over the process and Key Performance Indicators (KPIs) measure whether or not a control is meeting its objective.

Continual service improvement depends on accurate and timely process measurements and relies on obtaining, analyzing, and using information that is practical and meaningful to the process. Measurements of process efficiency and effectiveness enable NGEN management to track process performance and improve overall end-user satisfaction.

The following table summarizes the relationships between process CSFs and KPIs. See Appendix D for a complete list of CSFs and KPIs.

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	TBD	1	TBD
		2	TBD

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
		3	TBD
		4	TBD
2	TBD	1	TBD
		2	TBD
		3	TBD
		4	TBD

*Note: Additional metric details incl. threshold and objective values are defined in the SOPs.

10.15 Desired Metrics and Compliance Controls

This section provides a narrative description of additional metrics and compliance controls applicable to the process, but not currently in place to support Transition.

TBD

TOOLS AND TECHNOLOGY

10.16 Tool Requirements

This section defines key tool automation capability, interface, and interoperability requirements:

Requirement	Process Activity
Change Ticketing Management System	Creating, tracking, closing and management of changes
Configuration Management System	Allow for the tracking and management of new and changed CIs

10.17 Tools Used to Support the Process

This section defines the requirements met by COSC tools today and documents key gaps:

Requirement	COSC Tool Used Today	Measure -ment	Gap	Recommendation
Change Tracking	BMC Remedy	Partially Meets		TBD

INTEGRATION AND VALIDATION

10.18 Interface Requirements

This section defines the key interfaces with other processes, tools, governance bodies, and resources (service owners, vendors):

Interface ID	Interface Description
TBD	TBD

10.19 Integration Approach

10.19.1 Use Case Selection

TBD

10.19.2 Workshops and Simulations

TBD

10.20 Validation Results and Remediation

TBD

Error ID	Validation Scenario	Step Description	Type of Error Found	Error Description
TBD	TBD	TBD	TBD	TBD

APPENDIX A – CHANGE MANAGEMENT STANDARD OPERATING PROCEDURE



Change Management
Standard Operating Procedures
Version: 1.0

DATE: 08 March 2012
Program Executive Office Enterprise Information Systems
Program Manager, Next Generation Enterprise Network
1325 10th Street, SE, Suite 301
Washington, DC 20374

PREPARED

Rajan Sharma
Change Management Process Owner
Naval Enterprise Networks

Date

CONCURRENCE

Basam Hasan
ITSM Lead
Naval Enterprise Networks
,

Date

Dan Hickey
Deputy Program Manager
Naval Enterprise Networks

Date

APPROVED

Shawn P. Hendricks
Captain, USN
Program Manager
Naval Enterprise Networks

Date

**Note: The signatures above certify this template has been approved for PMW 205 NGEN Program use. Once completed, this document and its contents are under the authority of the NGEN Process Owner, who is solely accountable for its stewardship, use, and maintenance.*

Table of Contents

1.	Purpose.....	1
2.	Scope.....	1
3.	PROCESS ACTIVITIES Overview	1
3.1	Procedures.....	1
3.1.1	[CHA1] Establish Change Management Process Framework	1
3.1.2	[CHA2] Create Request for Change (RFC).....	7
3.1.3	[CHA3] Assess and Prioritize RFC.....	10
3.1.4	[CHA4] Authorize ROM Development.....	13
3.1.5	[CHA5] Conduct Systems Engineering.....	16
3.1.6	[CHA6] Change Package Approval	21
3.1.7	[CHA8] Review and Close Change.....	25
	APPENDIX A: Acronyms.....	28
	APPENDIX B: Process Diagram Legend	31

11. PURPOSE

This Standard Operating Procedure (SOP) is designed to provide for standard, repeatable, and measurable process for Change Management (CHA) for government retained roles within the United States Navy (USN) Continuity of Services Contract (CoSC) environment in preparation for transitioning to the Next Generation Enterprise Network (NGEN).

Table 1-1 Authoritative Documents, References, Policies and Standards

Domain	Document ID	Title
TBD	TBD	TBD

12. SCOPE

This document describes the procedures implemented to support the government's role in achieving command and control of the current CoSC Service Delivery contract. These procedures will define the roles and responsibilities of the Process Owner, Process Manager, and Change Management personnel. This document will be an appendix to the HP-ES' Enterprise Configuration Management Plan for NMCI Enterprise Domain.

This document provides process steps and tools used in supporting the CoSC Change Management interface (touch) points between the Government and the CoSC Service Provider (HP-ES). It documents the data exchanges between parties during the CHA and other Information Technology Service Management (ITSM) processes. Further, it explains the use of the related Change Management toolset used in this processing.

13. PROCESS ACTIVITIES OVERVIEW

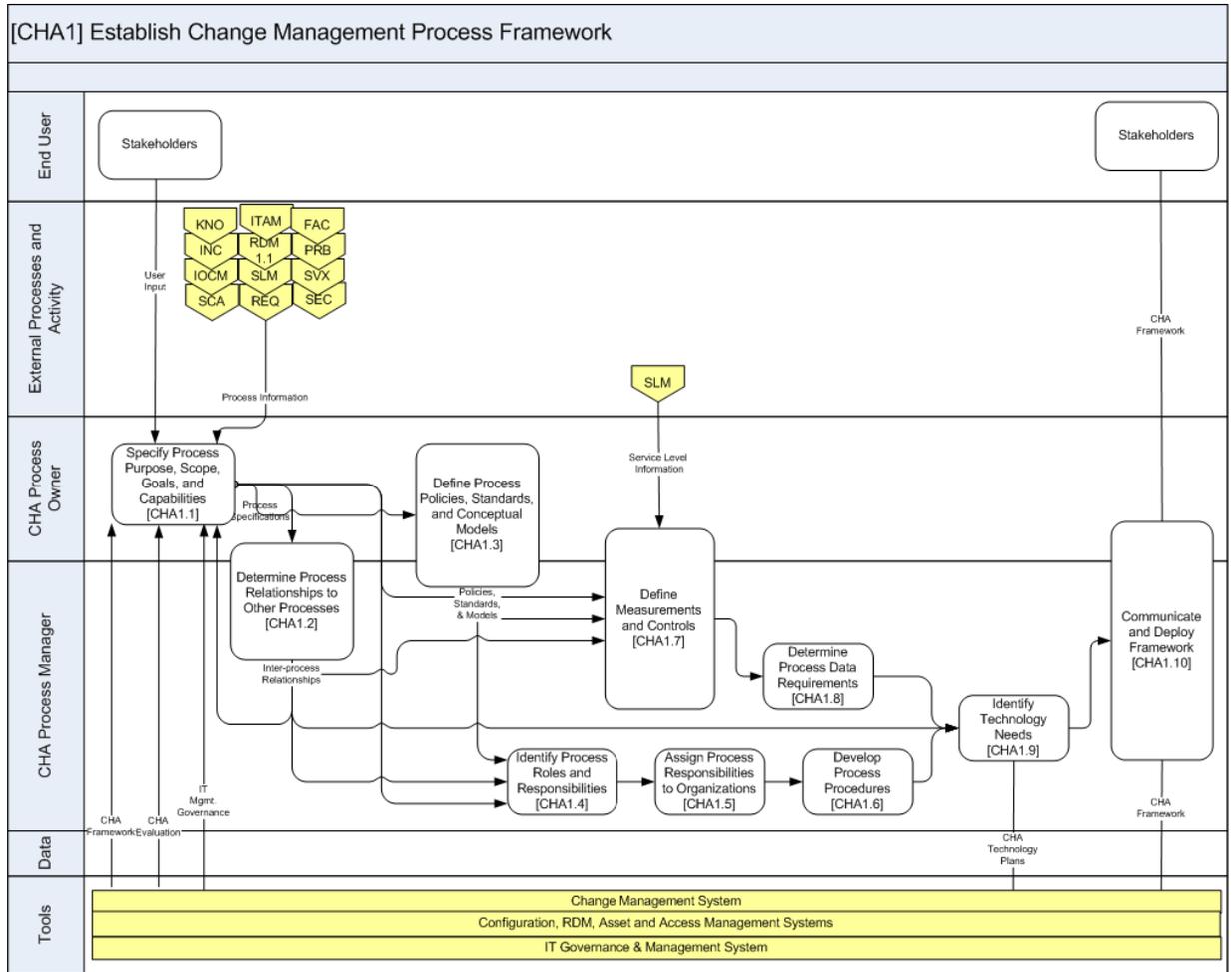
This section provides an overview of CHA activities.

13.1 Procedures

The following procedures provide a description of the tasks necessary to complete each CHA activity. A graphical representation of the tasks is provided followed by a table containing additional details supporting the tasks.

13.1.1 [CHA1] Establish Change Management Process Framework

The Change Management Process Framework defines the end-to-end approach of establishing the processes, procedures, roles, performance management capabilities and supporting tools needed to execute Change Management.



1.0 CHA_Establish_Process_Framework_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Define Process Purpose, Scope, Goals and Capabilities	Define the scope, goals and capabilities of the process, ensuring they meet the program's overall strategic vision	Process Owner	Define the following: <ul style="list-style-type: none"> • Purpose • Scope • Goals • Capabilities

2	Determine process relationship to other processes	Define and validate the integration with other IT Service Management (ITSM) and business processes	<ul style="list-style-type: none"> • CHA Process Owner • CHA Process Manager • Other Process Owners and Process Managers • External contractors 	<ul style="list-style-type: none"> • Identify and document dependencies on inputs, outputs, and data requirements • Define tool touch points
3	Define Process policies, standards, and conceptual models	Define the set of procedures that will be used to ensure consistent, repeatable practices across the enterprise	<ul style="list-style-type: none"> • CHA Process Owner • CHA Process Manager 	<ul style="list-style-type: none"> • Define standards to ensure standardized, cross-enterprise operations • Establish a conceptual model to test and validate proposed standards, policies and practices
4	Identify process roles and responsibilities	Define the various roles necessary to fully execute the process. For each role, define the scope, boundary and responsibilities for which the role will be responsible	<ul style="list-style-type: none"> • CHA Process Manager • External Contractor 	<ul style="list-style-type: none"> • Define the set of roles necessary to fully execute the process, ensuring that there is sufficient segregation of duties and responsibilities.
5	Assign process responsibilities to the organization	Map the responsibilities to the various departments / commands that will execute the process	<ul style="list-style-type: none"> • CHA Process Manager • External Contractor 	<ul style="list-style-type: none"> • Align role with process activities and stakeholder responsibilities • Determine where the roles must reside in the organizational structure • Align roles with stakeholders' responsibilities

				<ul style="list-style-type: none"> • Suggest modifications / adjustments when gaps are identified
6	Develop process procedures	Document the detailed procedures necessary to ensure the flawless execution of the process	<ul style="list-style-type: none"> • CHA Process Manager • External Contractor 	<ul style="list-style-type: none"> • For each process activity, identify the tasks comprising that activity • Document the detailed procedures necessary to ensure the flawless execution of the activity
7	Define measurements and control	Document the measurements that will be captured to ensure effective management oversight. Put controls in place to validate that policies and procedures are being followed	<ul style="list-style-type: none"> • CHA Process Owner • External Contractor 	<ul style="list-style-type: none"> • Define the set of measurements that allow management to evaluate the performance of the process • Define the set of controls that allow management to determine whether established policies and procedures are effective, and are being followed.
8	Determine process data requirements	Define the data set necessary for the effective execution of the process	<ul style="list-style-type: none"> • CHA Process Owner • CHA Process Manager 	<ul style="list-style-type: none"> • Identify and document the data set that must be received, ensuring that its format, frequency, timing, and dependencies are known and understood by the originator and recipient.
9	Identify technology needs	Define the automated tools and/or procedures necessary for the effective execution of the process	<ul style="list-style-type: none"> • CHA Process Owner • CHA Process Manager 	<ul style="list-style-type: none"> • Identify the suite of automated tools and/or monitoring devices necessary to minimize the amount of human intervention.

10	Communicate and deploy framework	Notify all relevant stakeholders of the frameworks' purpose and intent	<ul style="list-style-type: none"> CHA Process Owner 	<ul style="list-style-type: none"> Via established communication means, notify all relevant stakeholder of the process's scope, capabilities, expectations, and limitations.
-----------	----------------------------------	--	---	---

13.1.1.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym CHA						
Assumptions: The Government Process Owner will define the scope, goals, objectives, and measures that will be followed by external contractors executing the system.						
Government-to-Government Memoranda of Agreement (MOA) and/or Memoranda of Understanding (MOU) will be executed as necessary to ensure seamless interaction between Government entities						
Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
All steps in establishing the CHA framework	Process Owner	SE&I				
All steps in establishing the CHA framework	Process Manager	SE&I				
All steps in establishing the CHA framework	Contractor	HP-ES				

13.1.1.2 DECISION TIMELINES

TBD

13.1.1.3 TOOLS

TBD

13.1.1.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
------	----------------

Change Management Process Owner	Accountable for the end-to-end operation of the CHA process and for ensuring it achieves its purpose and objectives, and sustains consistent operation across all stakeholders.
Change Management Process Manager	Responsible for daily operation of the process in accordance with established policies, procedures, and standards. Provides input to Process Owner on potential process improvements.
Contractor	HP-ES currently operates and manages the CHA activities on a daily basis. Proposed changes are submitted to the Government for review and approval prior to scheduling and implementation.
Other Process Owners	Owners of other ITSM or business processes that have a dependency upon, or may be impacted by, the CHA process.

13.1.1.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

CHA 1	Process Owner	Process Manager	Other Process Owners	External Contractor
Specify purpose, goals, scope, and objectives	A	C	I	I
Determine relationship to other process	A	R	C	C/I
Define policies, standards and conceptual models	A	R		C/I
Identify roles and responsibilities	A	R	C/I	C/I
Assign responsibilities to organization	A	R	I	I
Develop process procedures	A	R	C/I	C/I
Define measures and controls	I	A/R	I	C/I

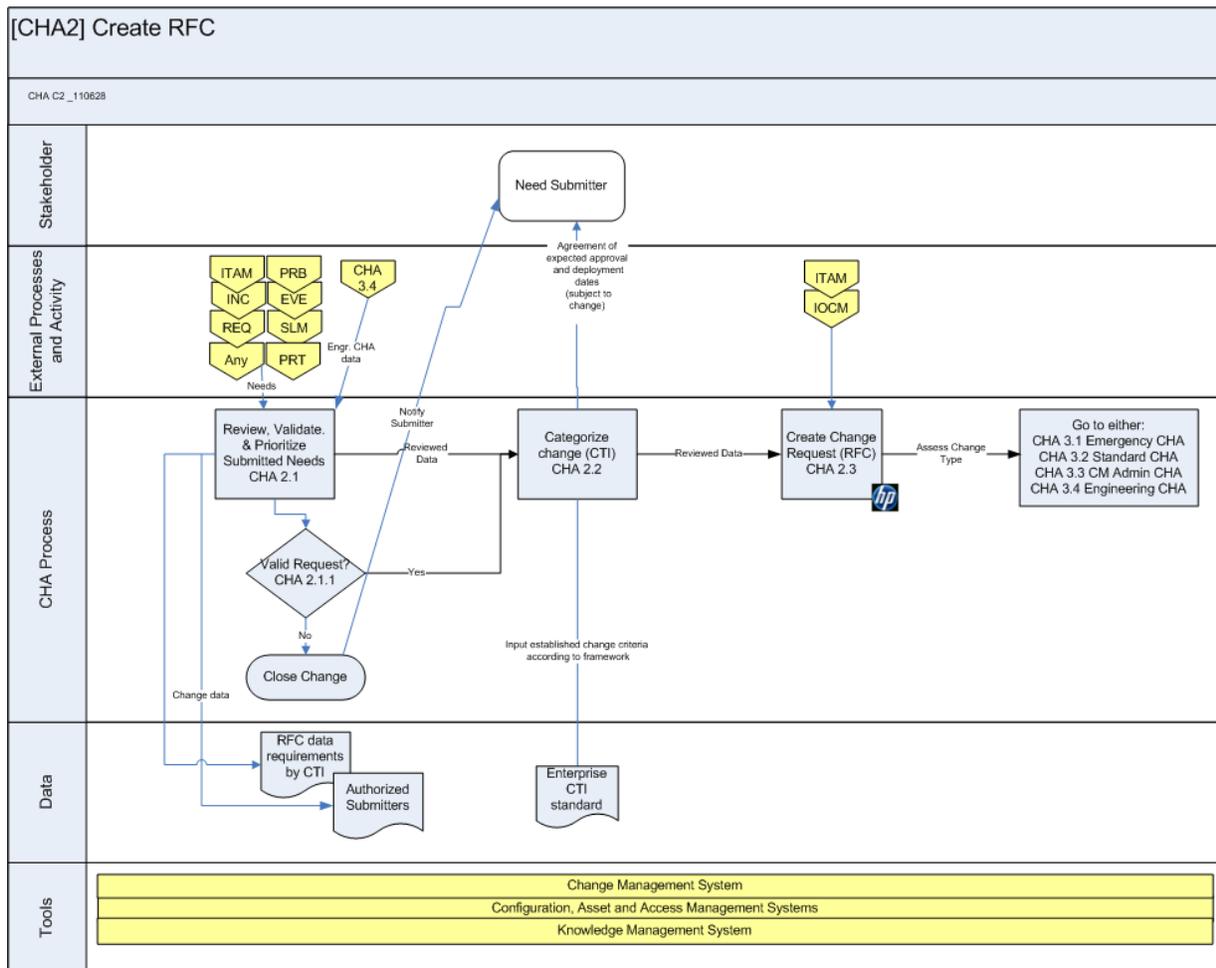
Determine Data Requirements	C	A/R	C/I	C/I
Identify Technology Needs	A	R	C	C
Communicate and Deploy Framework	A/R	C/I	C/I	C/I

13.1.1.6 METRICS

TBD

13.1.2 [CHA2] Create Request for Change (RFC)

This activity defines the steps necessary to create a RFC for review and approval prior to scheduling and implementation.



CHA_Create RFC SOP_v1.0				
2.0				
Step	Process Model Task	Action	Role	Details
1	Review, validate and prioritize submitted need	Assess the proposed change to determine urgency, impact and criticality	Change Sponsor	Define the following: <ul style="list-style-type: none"> • Reason for RFC • Urgency • Criticality • Impact to other CIs
2	Categorize RFC	Assign the RFC to one of the previously established categories	• External Contractor	• Categorize RFC according to previously established criteria (scope, level of effort, criticality, urgency, etc.)
3	Create Change Request	Create the RFC according to established procedure	• External Contractor	• Enter required RFC information into automated tracking tool (Remedy)

13.1.2.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym CHA						
Assumptions: Request for Changes will adhere to previously established criteria.						
Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Requirements
Review, validate and prioritize submitted RFC	CHA Process Manager	External Contractor				
Categorize RFC	CHA Process Manager	External Contractor				
Create Change Request (RFC)	CHA Process Manager	External Contractor				

13.1.2.2 DECISION TIMELINES

TBD

13.1.2.3 TOOLS

The current tool used in this activity is Remedy.

13.1.2.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
Change Management Process Manager	Responsible for the receipt, review, prioritization, and categorization of all submitted requests for change
Change Sponsor	Individual or group responsible for assessing the need for change and creating initial request
Other Process Owners	Receive notification of proposed request and assess potential impact to inter-dependent processes

13.1.2.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

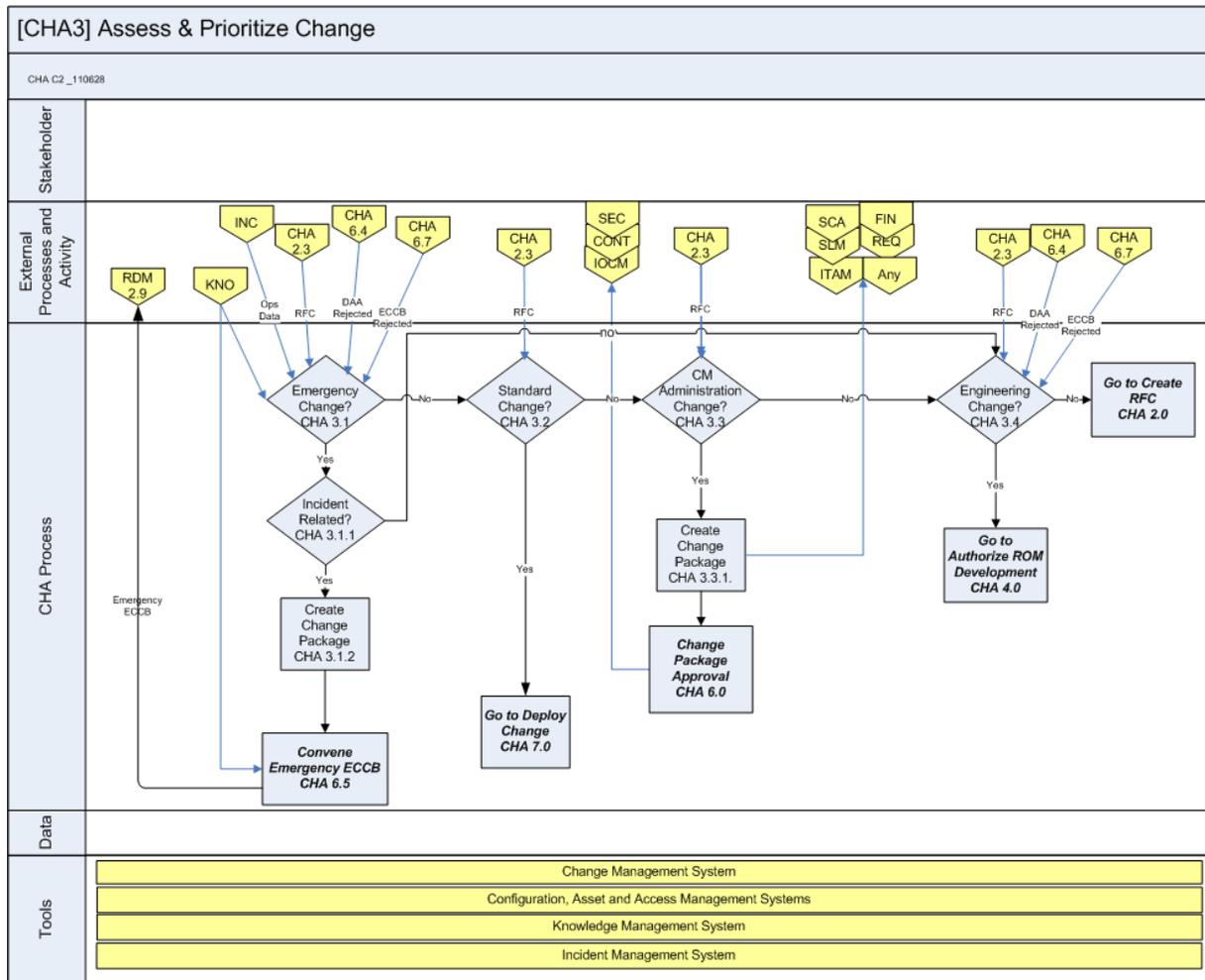
CHA 2	Process Manager	Change Sponsor	Other Process Owners	External Contractor
Assess need for proposed change	I	A/R	I	I
Receive, review, validate, prioritize, and categorize submitted RFC	A	C	I	C/I
Create automated Change Request	A	I	I	C/I

13.1.2.6 METRICS

TBD

13.1.3 [CHA3] Assess and Prioritize RFC

This activity defines the steps necessary to assess and prioritize the submitted request for change.



3

3.0 CHA_Assess and Prioritize_Change_SOP_v1.0				
Step	Process Model Task	Action	Role	Details

1	Determine if RFC is an emergency change	Assess the submitted request to determine whether the change must be immediately implemented	Change Manager	Determine the following: <ul style="list-style-type: none"> • Is this change urgently required? • Is it incident-related? • Will implementation delay impact service availability?
2	Determine if RFC is a standard change	Assess submitted change to determine if it is a standard (pre-approved) change	• External Contractor	• Assess submitted change to determine whether change can be implemented using previously established protocols
3	Determine if RFC is an administrative change	Assess submitted change to determine if it is an administrative change	• External Contractor	• Assess submitted change to determine whether change can be categorized as an administrative change
4	Determine if RFC is an engineering change	Assess submitted change to determine if it requires engineering input and support	• External Contractor	• Assess submitted change to determine if the request will require the assessment and involvement of network engineers.

13.1.3.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym CHA						
Assumptions: Submitted requests for change are assessed according to previously established and agree-upon parameters. Changes to criteria will be negotiated between the Government and the executing Contractor.						
Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Requirements
Determine whether RFC	CHA Process	External Contractor				

is an emergency	Manager					
Determine whether RFC is a standard change	CHA Process Manager	External Contractor				
Determine whether RFC is an administrative change	CHA Process Manager	External Contractor				
Determine whether change is an Engineering Change	CHA Process Manager	External Contractor				

13.1.3.2 DECISION TIMELINES

TBD

13.1.3.3 TOOLS

The current tool used in this activity is Remedy.

13.1.3.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
Change Management Process Manager	Responsible for receiving RFCs from the Change Sponsor and determining whether it should be classified as an Emergency, Standard, Administrative, or Engineering change.
Change Sponsor	Individual or group responsible for assessing the need for change and creating initial request
Other Process Owners	Receive notification of proposed request and assess potential impact to inter-dependent processes

13.1.3.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

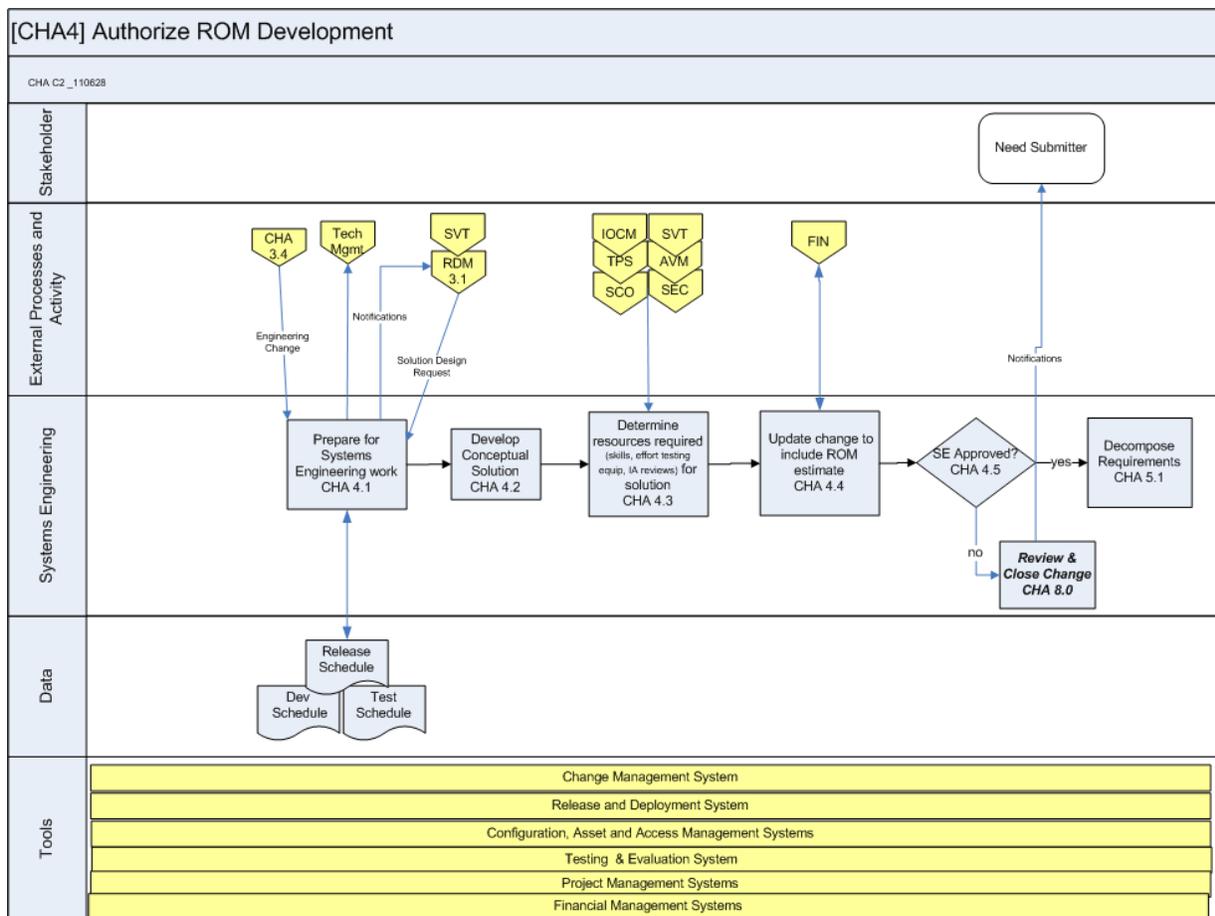
CHA 3	Process Manager	Change Sponsor	Other Process Owners	External Contractor
Determine RFC classification	A	C/I	I	R

13.1.3.6 METRICS

TBD

13.1.4 [CHA4] Authorize ROM Development

This activity defines the steps necessary to authorize ROM development.



4.0 CHA_Authorize_ROM_Development_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Prepare for Systems Engineering Work	Gather all necessary input from stakeholders	Systems Engineer	Determine the following: <ul style="list-style-type: none"> • Critical requirements • Optional requirements • Assumptions • Constraints
2	Develop conceptual model	Using received input, design conceptual model for stakeholder review	<ul style="list-style-type: none"> • Systems Engineer • Change Sponsor • Relevant Stakeholders 	<ul style="list-style-type: none"> • Utilizing appropriate tools, schematics, and other material, prepare a conceptual model, ensuring all required elements are included
3	Determine resource requirements	Determine the level of effort required to complete the assignment	<ul style="list-style-type: none"> • Systems Engineer 	<ul style="list-style-type: none"> • Determine whether assignment can be completed in the specified timeframe using existing resources, while considering competing priorities / projects
4	Update RFC to include ROM estimate	Update RFC with ROM estimate	<ul style="list-style-type: none"> • Systems Engineer 	<ul style="list-style-type: none"> • Access the RFC and include the ROM estimate, including any back up material that may be required.
5	Systems Engineering approved?	Decision point	<ul style="list-style-type: none"> • ECCB 	<ul style="list-style-type: none"> • After reviewing the RFC and the ROM estimate, the ECCB will approve or deny the RFC. If denied, the process ends. If approved, the process proceeds with Activity 5.

13.1.4.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym CHA
Assumptions: The ECCB will be comprised of representatives from both the Navy and the Service Provider. The ECCB will have approval/veto authority over all submitted changes.

Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Requirements
Prepare for Systems Engineering work	Systems Engineer	SE&I				
Develop conceptual solution	Systems Engineer	SE&I				
Determine resources required	Systems Engineer	SE&I				
Update RFC to include ROM estimate	Systems Engineer	SE&I				
System Engineering approved	ECCB	SE&I				

13.1.4.2 DECISION TIMELINES

TBD

13.1.4.3 TOOLS

The current tool used in this activity is Remedy.

13.1.4.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
Systems Engineer	Responsible for receiving the RFC, assessing the proposed change and then developing a conceptual model based upon its requirements. The SE is responsible for providing a level of effort estimate to the Change Sponsor and the ECCB.
Change Sponsor	Receive and assess ROM estimate received from SE

ECCB	Board responsible for assessing required inputs, ROM estimates, urgency and criticality of proposed changes, and deciding whether to approve or deny the RFC.
------	---

13.1.4.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

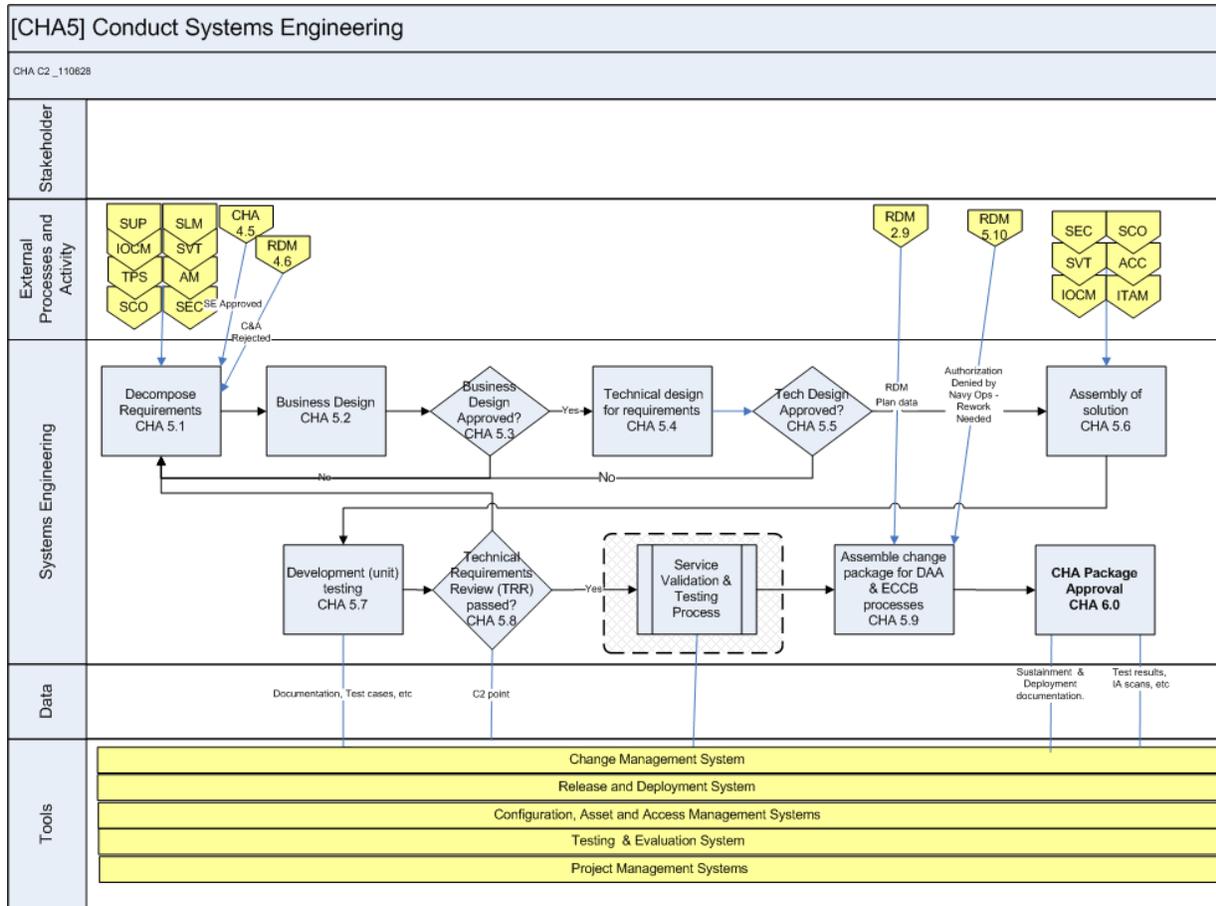
CHA 4	Systems Engineer	Change Sponsor	Other Process Owners	ECCB
Prepare for Systems Engineering work	A/R	I		
Develop conceptual model	A/R	I		
Determine resource requirements	A/R	I		I
Update RFC with ROM estimates	A/R	I		I
SE Approval / Rejection	C/I	I		A/R

13.1.4.6 METRICS

TBD

13.1.5 [CHA5] Conduct Systems Engineering

This activity defines the steps necessary to conduct Systems Engineering.



5

5.0 CHA_Conduct_Systems_Engineering_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Decompose requirements	Break requirements down into their smallest useable sub-components	Systems Engineer	Determine the following: <ul style="list-style-type: none"> • Critical requirements • Optional requirements • Business requirements • Technical requirements • Assumptions • Constraints

2	Prepare Business Design	Prepare Business Design documentation	<ul style="list-style-type: none"> • Systems Engineer 	<ul style="list-style-type: none"> • Utilizing appropriate tools, schematics, and other material, prepare business design documentation, ensuring all required elements are included
3	Business Design Approval	Decision Point	<ul style="list-style-type: none"> • Change Sponsor 	<ul style="list-style-type: none"> • The Change Sponsor reviews the submitted Business Design documentation and either approves or rejects it. If rejected, return to step 5.1
4	Prepare Technical Design	Prepare Technical Design documentation	<ul style="list-style-type: none"> • Systems Engineer 	<ul style="list-style-type: none"> • Utilizing appropriate tools, schematics, and other material, prepare technical design documentation, ensuring all required elements are included
5	Technical Design Approval	Decision point	<ul style="list-style-type: none"> • Chief Engineer (CHENG) 	<ul style="list-style-type: none"> • The CHENG reviews the submitted Technical Design documentation and either approves or rejects it. If rejected, return to step 5.1
6	Assemble solution	The approval solution is assembled	<ul style="list-style-type: none"> • Systems Engineer 	<ul style="list-style-type: none"> • The SE assembles the approved solution utilizing all required business and technical components
7	Development (unit) testing	The assembled solution is unit tested	<ul style="list-style-type: none"> • Systems Engineer 	<ul style="list-style-type: none"> • The assembled solution is unit tested according to previously established unit testing procedures and protocols
8	Technical Requirements Review (TRR)	Decision Point	<ul style="list-style-type: none"> • TRR Board 	<ul style="list-style-type: none"> • Using previously established testing and an evaluation criterion, the TRR Board approves or rejects the results of the Development Testing. If rejected, return to step 5.1
9	Assemble Change Package	All components necessary for the Change Package are assembled	<ul style="list-style-type: none"> • Systems Engineer 	<ul style="list-style-type: none"> • Approved solution is assembled according to previously established procedures and protocols

13.1.5.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym CHA						
Assumptions: Development (unit) testing procedures are established and administered by the CHENG and are not subject to external review or modification.						
Constraints:						
Process Point	Responsible Parties					
	Position	Org	Name	Contact Info	Tools	Tool Requirements
Decompose requirements	Systems Engineer	SE&I				
Prepare Business Design	Systems Engineer	SE&I				
Business Design Approval / Rejection	Change Sponsor	TBD				
Prepare Technical Design	Systems Engineer	SE&I				
Technical Design Approval / Rejection	CHENG	SE&I				
Assemble solution	Systems Engineer	SE&I				
Development (unit) testing	Systems Engineer	SE&I				
TRR Review Approval / Rejection	CHENG	SE&I				
Assemble Change Package	Systems Engineer	SE&I				

13.1.5.2 DECISION TIMELINES

TBD

13.1.5.3 TOOLS

TBD

13.1.5.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
Systems Engineer	Responsible for: <ul style="list-style-type: none"> decomposing received requirements into smallest useable sub-components. preparing Business Design documentation Technical Design documentation assembling solution development (unit) testing assembling Change Package
Change Sponsor	Approving / rejecting Business Design documentation
Chief Engineer (CHENG)	Approving / rejecting Technical Design documentation
Technical Requirements Review Board	Approving / rejecting development (unit) testing results

13.1.5.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

CHA 5	Systems Engineer	Change Sponsor	CHENG	TRRB
Decompose requirements	A/R			
Prepare Business Design	A/R	C	C	
Business Design Approval / Rejection	I	A/R		
Prepare Technical Design	A/R		C	
Technical Design Approval / Rejection	I		A/R	
Assemble solution	A/R	I		
Development (unit) testing	A/R	I		

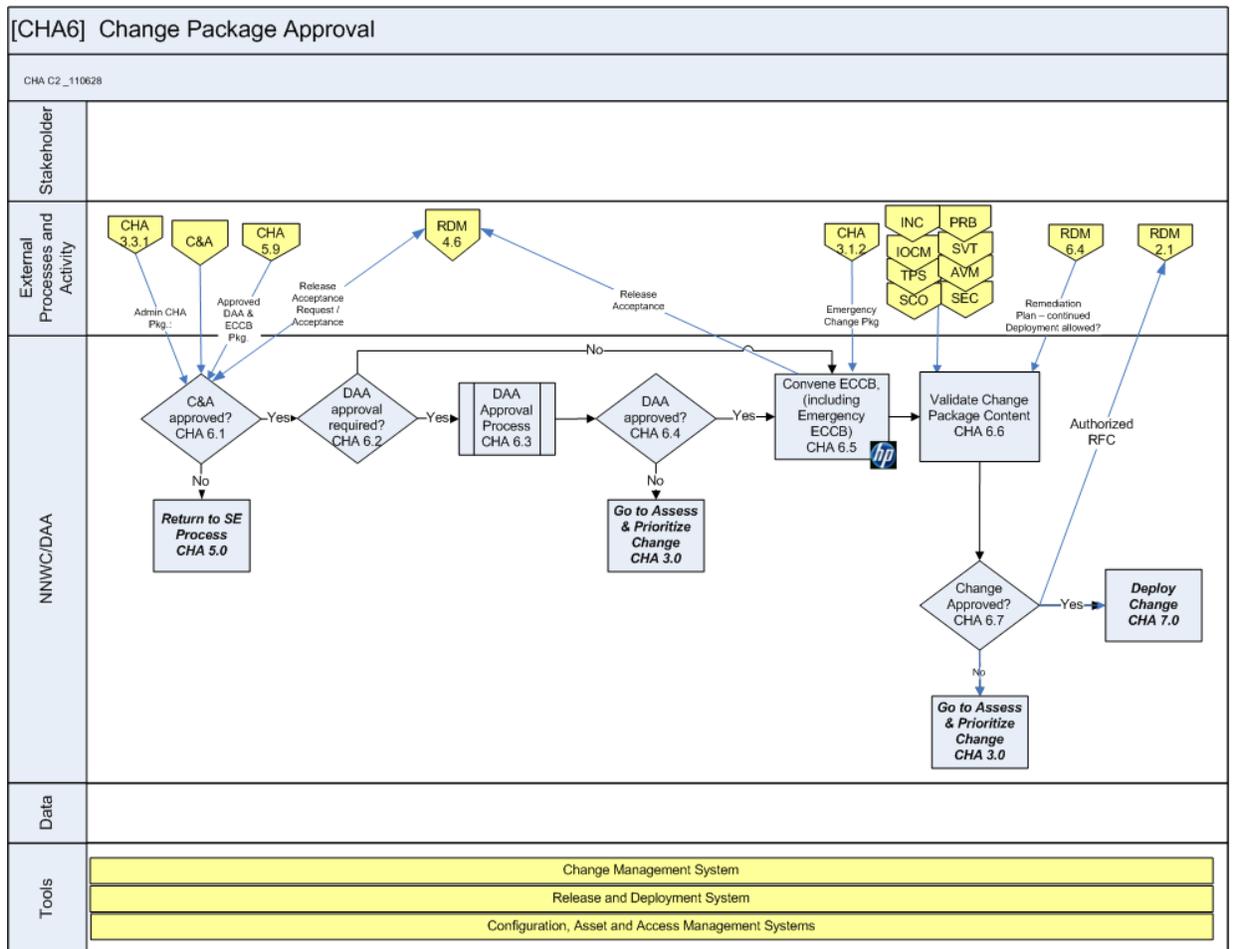
TRRB Approval / Rejection	C/I	I	I	A/R
Assemble Change Package	A/R	I		

13.1.5.6 METRICS

TBD

13.1.6 [CHA6] Change Package Approval

This activity defines the steps necessary to approve the submitted Change Package.



6.0 CHA_Change_Package_Approval_SOP_v1.0

Step	Process Model Task	Action	Role	Details
------	--------------------	--------	------	---------

1	Decompose requirements	Break requirements down into their smallest useable sub-components	Systems Engineer	Determine the following: <ul style="list-style-type: none"> • Critical requirements • Optional requirements • Business requirements • Technical requirements • Assumptions • Constraints
2	Prepare Business Design	Prepare Business Design documentation	• Systems Engineer	• Utilizing appropriate tools, schematics, and other material, prepare business design documentation, ensuring all required elements are included
3	Business Design Approval	Decision Point	• Change Sponsor	• The Change Sponsor reviews the submitted Business Design documentation and either approves or rejects it. If rejected, return to step 5.1
4	Prepare Technical Design	Prepare Technical Design documentation	• Systems Engineer	• Utilizing appropriate tools, schematics, and other material, prepare technical design documentation, ensuring all required elements are included
5	Technical Design Approval	Decision point	• Chief Engineer (CHENG)	• The CHENG reviews the submitted Technical Design documentation and either approves or rejects it. If rejected, return to step 5.1
6	Assemble solution	The approval solution is assembled	• Systems Engineer	• The SE assembles the approved solution utilizing all required business and technical components
7	Development (unit) testing	The assembled solution is unit tested	• Systems Engineer	• The assembled solution is unit tested according to previously established unit testing procedures and protocols

8	Technical Requirements Review (TRR)	Decision Point	<ul style="list-style-type: none"> • TRR Board 	<ul style="list-style-type: none"> • Using previously established testing and an evaluation criterion, the TRR Board approves or rejects the results of the Development Testing. If rejected, return to step 5.1
9	Assemble Change Package	All components necessary for the Change Package are assembled	<ul style="list-style-type: none"> • Systems Engineer 	<ul style="list-style-type: none"> • Approved solution is assembled according to previously established procedures and protocols

13.1.6.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym CHA						
Assumptions: Development (unit) testing procedures are established and administered by the CHENG and are not subject to external review or modification.						
Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Requirements
Decompose requirements	Systems Engineer	SE&I				
Prepare Business Design	Systems Engineer	SE&I				
Business Design Approval / Rejection	Change Sponsor	TBD				
Prepare Technical Design	Systems Engineer	SE&I				
Technical Design Approval / Rejection	CHENG	SE&I				
Assemble solution	Systems Engineer	SE&I				
Development (unit) testing	Systems Engineer	SE&I				
TRR Review Approval / Rejection	CHENG	SE&I				

Assemble Change Package	Systems Engineer	SE&I				
--	-----------------------------	-----------------	--	--	--	--

13.1.6.2 DECISION TIMELINES

TBD

13.1.6.3 TOOLS

TBD

13.1.6.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
Systems Engineer	Responsible for: <ul style="list-style-type: none"> decomposing received requirements into smallest useable sub-components. preparing Business Design documentation Technical Design documentation assembling solution development (unit) testing assembling Change Package
Change Sponsor	Approving / rejecting Business Design documentation
Chief Engineer (CHENG)	Approving / rejecting Technical Design documentation
Technical Requirements Review Board	Approving / rejecting development (unit) testing results

13.1.6.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

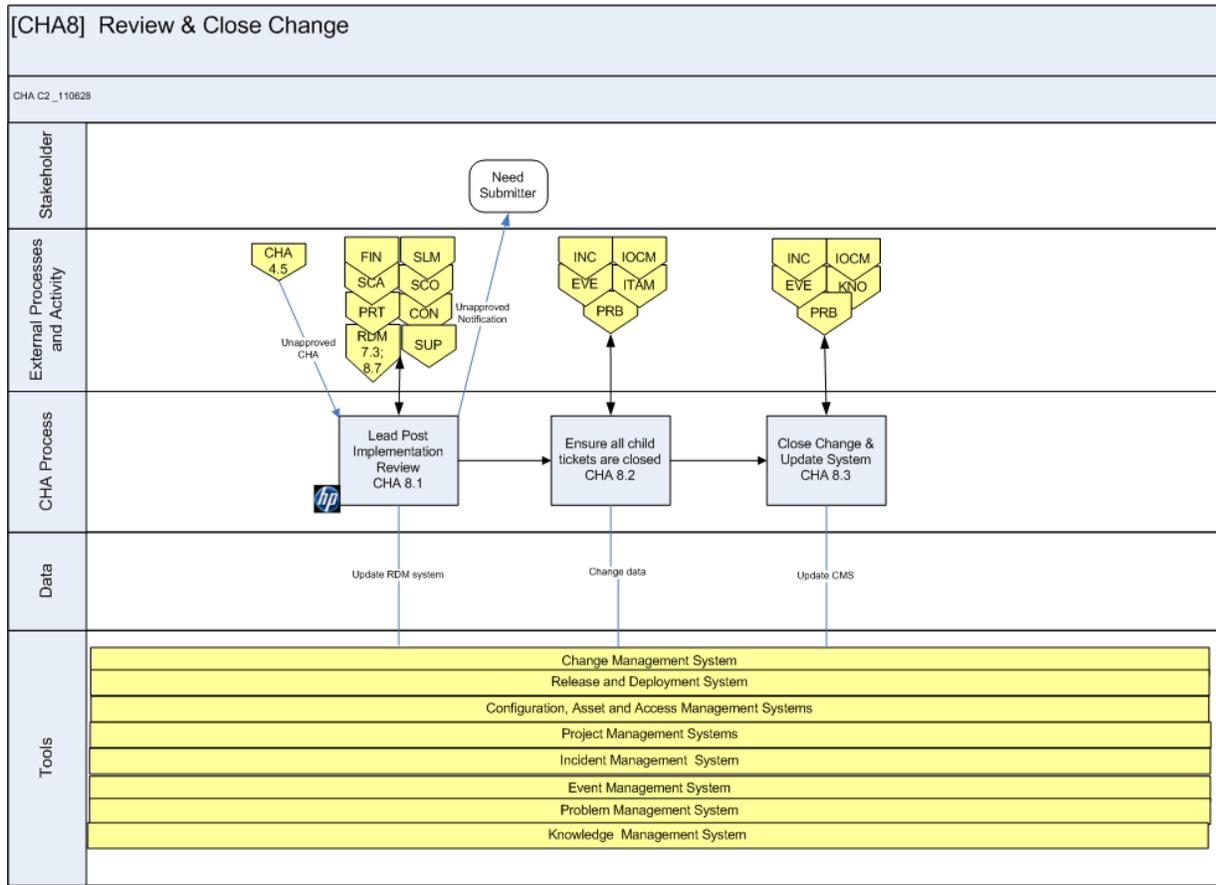
CHA 6	Systems Engineer	Change Sponsor	CHENG	TRRB
Decompose requirements	A/R			
Prepare Business Design	A/R	C	C	
Business Design Approval / Rejection	I	A/R		
Prepare Technical Design	A/R		C	
Technical Design Approval / Rejection	I		A/R	
Assemble solution	A/R	I		
Development (unit) testing	A/R	I		
TRRB Approval / Rejection	C/I	I	I	A/R
Assemble Change Package	A/R	I		

13.1.6.6 METRICS

TBD

13.1.7 [CHA8] Review and Close Change

This activity defines the steps necessary to review and close the approved and implemented change.



8

8.0 CHA_Review and Close_Change_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Lead Post-Implementation Review	Gather information from implemented change (metrics, statistics, issues, etc.)	External Contractor	Determine the following: <ul style="list-style-type: none"> • Successful vs. unsuccessful change • Estimated vs. actual time to implement • Issues encountered • Lessons learned

2	Close all child tickets	Ensure that related tickets are closed	<ul style="list-style-type: none"> External Contractor 	<ul style="list-style-type: none"> If there is more than one ticket associated with the change, ensure that all children tickets are properly closed
3	Close Change and Update System	Formally close RFC and update ancillary records as necessary	<ul style="list-style-type: none"> External Contractor 	<ul style="list-style-type: none"> After formal review, the parent, and all associated child tickets, are closed, and associated records (e.g. CMDB) are updated

13.1.7.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym CHA						
Assumptions: The Government will actively participate in the post-implementation review.						
Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Requirements
Lead post-implementation review	CHA Process Manager	TBD				
Close all associated child tickets	CHA Process Manager	TBD				
Close RFC and Update System	CHA Process Manager	TBD				

13.1.7.2 DECISION TIMELINES

TBD

13.1.7.3 TOOLS

TBD

13.1.7.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
------	----------------

CHA Process Manager	Responsible for: <ul style="list-style-type: none"> • Leading post-implementation review • Distributing metrics associated with RFC • Capturing lessons learned • Capturing issues encountered • Closing all associated children tickets • Formally closing parent RFC • Ensuring CMDB and associated records are updated
---------------------	--

13.1.7.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

CHA 8	CHA Process Manager	Change Sponsor	ECCB
Lead post-implementation review	A/R	C/I	I
Close all associated child ticket	A/R	I	I
Close parent RFC and update system	A/R	I	I

13.1.7.6 METRICS

TBD

Acronyms

ACRONYM	DEFINITION
AMDB	Asset Management Database
AMIP	Asset Management Implementation Plan
AMP	Asset Management Plan
AMP	Availability Management Plan
AS	Acquisition Strategy
ASN-RDA	Office of the Assistant Secretary of the Navy (Research, Development and Acquisition)
ATO	Authority to Operate
BCP	Business Continuity Plan
C&A	Certification and Accreditation

C2	Command and Control
CAB	Change Advisory Board
CANES	Consolidated Afloat Networks and Enterprise Services
CBT	Computer-Based Training
CDRL	Contract Data Requirements List
CDS	Cross Domain Security
CI	Configuration Item
CLIN	Catalog Line Item Number
CMDB	Configuration Management Database
CMIS	Capacity Management Information System
CMP	Configuration Management Plan
CMS	Change Management System
CND	Computer Network Defense
CO/CO	Contractor Owned / Contractor Operated
COI	Communities of Interest
CONOPS	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial Off the Shelf
CYBERCOM	Fleet Cyber Command
DAA	Designated Accrediting Authority
DFS	Distributed File System
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DM	Decision Meeting
DMZ	Demilitarized Zone
DoD	Department of Defense
DON	Department of the Navy
DON CIO	Department of Navy Chief Information Officer
DR	Disaster Recovery
DV	Desktop Virtualization
ECCB	Engineering Change Control Board
ECP	Engineering Change Proposal
EDSS	Engineering Design and Support Services
EILT	Executive Integration Leadership Team
ES	Enterprise Services
ESDS	Electronic Software Delivery Services
ESL	Enterprise Software Licensing
EUHW	End-User Hardware
GFY	Government Fiscal Year
GIG	Global Information Grid
GNO	Global Network Operations
GO/CO	Government Owned / Contractor Operated
HDD	Hard Disk Drive
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alerts
IDE	Integrated Data Environment
IM/IT	Information Management / Information Technology
IPR	In Progress Review

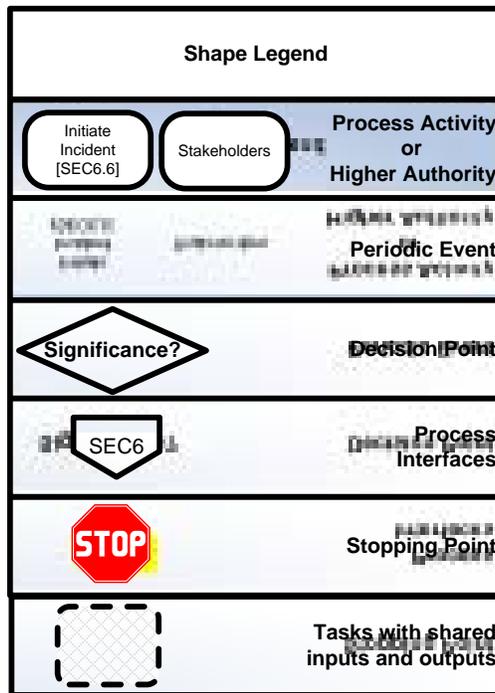
ISOOA	Independent Security Operations Oversight and Assessment
IT-21	Information Technology for the 21st Century
LCAB	Local Change Advisory Board
MCEN	Marine Corps Enterprise Network
MD	Management Domain
NCMO	Navy Circuit Management Office
NCPDM	Navy CoSC Process Definition Model
NEN	Naval Enterprise Networks
NET	NMCI Enterprise Tool
NetOps	Network Operations
NNE	Naval Networking Enterprise
NNPDM	Navy NGEN Process Definition Model
NNWC	Naval Network Warfare Command
NSA	National Security Agency
NSA	National Security Agency
NSIB	NGEN Senior Integration Board
OCONUS	Outside the United States
OEM	Original Equipment Manufacturer
ONE-NET	OCONUS Navy Enterprise Network
QA	Quality Assurance
RAS	Remote Access Service
RFC	Requests for Change
RFP	Request for Proposal
RFQ	Request for Quote
ROM	Rough Order of Magnitude
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SECCONOPs	Security Concept of Operations
SEM	Security Event Management
SITREP	Situation Report
SLA	Service Level Agreement
SME PED	Secure Mobile Environment Portable Electronic Device
SRM	Supplier Relationship Management
SW	Software
TCB	Transition Control Board
TMP	Transition Management Plan
TRRB	Training Readiness Review Board
TXS	Transport Services
USMC	United States Marine Corps
USN	United States Navy
VTC	Video Conferencing
VV&R	Verification, Validation, and Reporting
WAN	Wide Area Network

Process Diagram Legend

The Process Activity diagrams in this document are created using a standardized Microsoft Visio template. The Process Activity Diagrams are developed in the form of a ‘swim lane’, which depicts sequential process tasks horizontally, with all of roles, functions, interfaces, data, and tools that interact with process activities listed vertically.

The Process Activity Diagram template is owned and maintained by the ITSM Architect and may be obtained with permission from the ITSM workspace on the PEO EIS portal.

The shape legend used to create the Process Activity Diagram is given below:



APPENDIX B – DATA MANAGEMENT STANDARD OPERATING PROCEDURE

Not to be disclosed outside the Government except IAW the referenced non-disclosure agreement



Data Management
Standard Operating Procedures
Version: 1.00

DATE: 8 March 2012
Program Executive Office Enterprise Information Systems
Program Manager, Next Generation Enterprise Network
1325 10th Street, SE, Suite 301
Washington, DC 20374

PREPARED

John Stefaney
Data Management Process Owner
Naval Enterprise Networks

Date

CONCURRENCE

Basam Hasan
ITSM Lead
Naval Enterprise Networks
,

Date

Dan Hickey
Deputy Program Manager
Naval Enterprise Networks

Date

APPROVED

Shawn P. Hendricks
Captain, USN
Program Manager
Naval Enterprise Networks

Date

**Note: The signatures above certify this template has been approved for PMW 205 NGEN Program use. Once completed, this document and its contents are under the authority of the NGEN Process Owner, who is solely accountable for its stewardship, use, and maintenance.*

Table of Contents

1.	Purpose.....	1
2.	Scope.....	1
3.	PROCESS ACTIVITIES Overview	1
3.1	Procedures.....	1
3.1.1	[DAT 1] Establish a Data Management Process Framework	1
3.1.2	[DAT 2] Plan Data Portfolio Architecture.....	7
3.1.3	[DAT 3] Acquire and Prepare Data.....	12
3.1.4	[DAT 4] Control, QA, Deploy and Maintain Data	16
3.1.5	[DAT 5] Back-up and Restore	27
3.1.6	[DAT 6] Archive and Dispose	32
3.1.7	[DAT 7] Monitor, Report and Manage Data Management	36
3.1.8	[DAT 8] Evaluate Data Management.....	38
	APPENDIX A: Acronyms.....	1
	APPENDIX B: Process Diagram Legend	2

1 **14. PURPOSE**

2 This Standard Operating Procedure (SOP) is designed to provide for standard, repeatable, and
3 measurable process for Data Management government retained roles within the United States
4 Navy (USN) Continuity of Services Contract (CoSC) environment in preparation for
5 transitioning to the Next Generation Enterprise Network (NGEN).
6

7 **Table 1-1 Authoritative Documents, References, Policies and Standards**

Domain	Document ID	Title
DON	CoSC Contract Attachment 4, Delivery / Transition of NMCI IP Section 1.8.4	Delivery of Intellectual Property

8
9

10 **15. SCOPE**

11 This document describes the procedures implemented to support the government's role in
12 achieving command and control of the current CoSC Service Delivery contract. These
13 procedures will define the roles and responsibilities of the Process Owner, Process Manager, and
14 other key process personnel.
15

16 This document provides identifies the tasks and tools used in supporting the CoSC Data
17 Management interface (touch) points between the Government and the CoSC Service Provider
18 (HP-ES). It documents the data exchanges between parties during used by Data Management and
19 other Information Technology Service Management (ITSM) processes.
20

21 **16. PROCESS ACTIVITIES OVERVIEW**

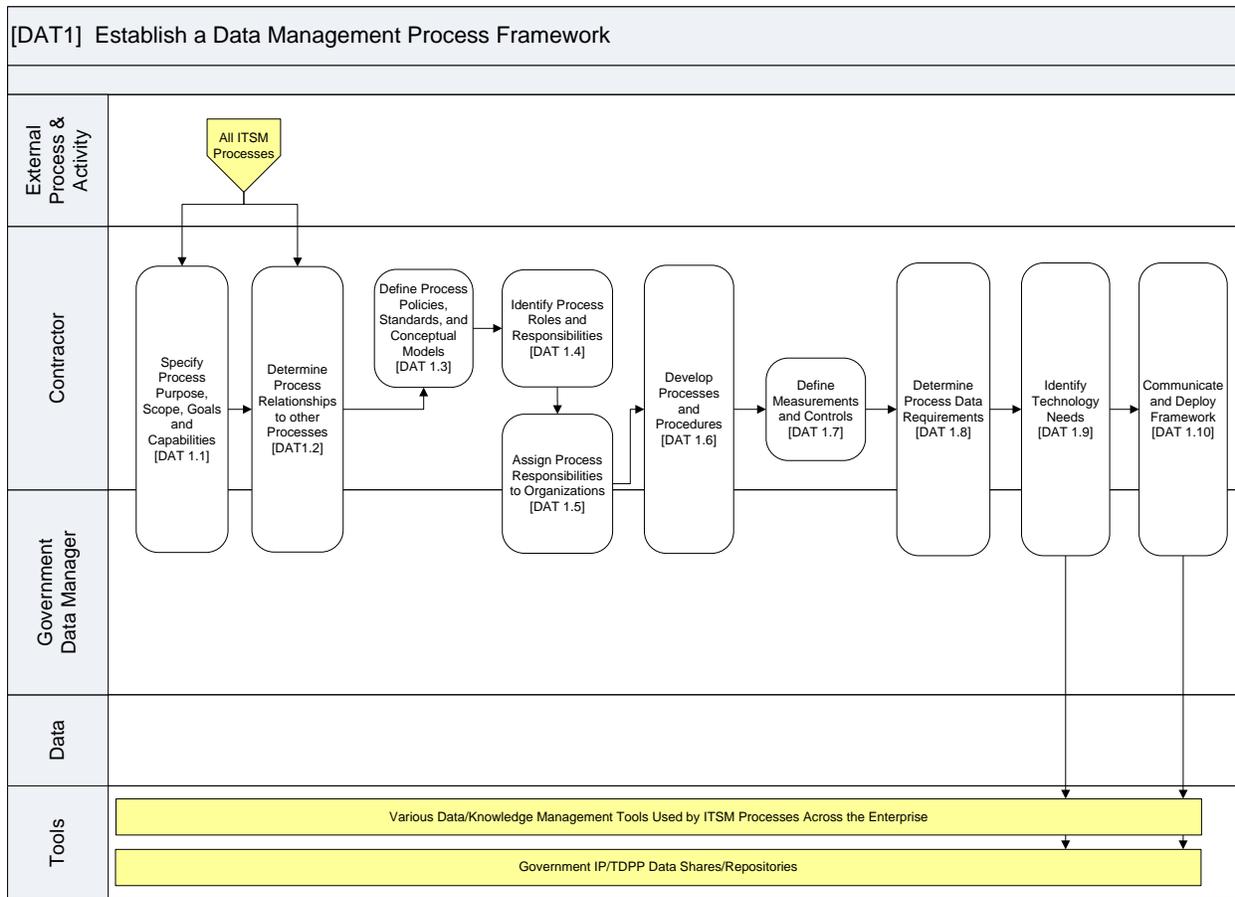
22 This section provides an overview of Data Management activities.

23 **16.1 Procedures**

24 The following procedures provide a description of the tasks necessary to complete each Data
25 Management activity. A graphical representation of the tasks is provided followed by a table
26 containing additional details supporting the tasks.
27

28 **16.1.1 [DAT 1] Establish a Data Management Process Framework**

29 The Data Management Process Framework defines the end-to-end approach of establishing the
30 processes, procedures, roles, performance management capabilities and supporting tools needed
31 to execute Data Management.
32



33
34

1.0 DAT_Establishing_Process_Framework_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
11	Specify Processes, Purpose, Scope, Goals and Capabilities	Gather input from stakeholders and document the process scope, objectives and boundaries	<ul style="list-style-type: none"> Contractor DAT Process Owner DAT Process Manager 	Define the following: <ul style="list-style-type: none"> Purpose Objectives Scope Goals Capabilities
12	Determine relationships to other processes	Define the integrations and dependencies with other IT Service Management (ITSM) and	<ul style="list-style-type: none"> Contractor DAT Process Owner DAT Process Manager Other Process 	<ul style="list-style-type: none"> Identify and document dependencies on inputs, outputs or activities Define tool touch or integration points

		business processes	Owners and Managers	
13	Define process policies, standards, and conceptual models	Establish the standards required to achieve consistent, repeatable practices across the enterprise	<ul style="list-style-type: none"> • Contractor • DAT Process Owner • DAT Process Manager 	<ul style="list-style-type: none"> • Define standards that must exist to achieve standardized, cross-enterprise operations • Establish a concept model to validate and test standards, policies and practices
14	Identify processes roles and responsibilities	Define the roles required to achieve process objectives	<ul style="list-style-type: none"> • Contractor • DAT Process Owner • DAT Process Manager 	<ul style="list-style-type: none"> • Considering the scope and objectives of the process, define the required roles needed to achieve operational success. • Define and document roles
15	Assign process responsibilities to organizations	Outline the organization construct identifying the location of defined roles	<ul style="list-style-type: none"> • Contractor • DAT Process Owner • DAT Process Manager 	<ul style="list-style-type: none"> • Align roles with process activities and stakeholder responsibilities • Determine where roles must reside within the enterprise / organization • Align roles with stakeholders' responsibilities
16	Develop processes and procedures	Engage the appropriate stakeholders to define the process procedures required to achieve objectives	<ul style="list-style-type: none"> • Contractor • DAT Process Owner • DAT Process Manager 	<ul style="list-style-type: none"> • Establish collaboration sessions with impacted stakeholders to develop process activities • Document processes and procedures sufficient to achieve consistency in operations across the organization/enterprise
17	Define measurements and controls	Establish the controls, measurements and reports necessary to	<ul style="list-style-type: none"> • Contractor • DAT Process Owner DAT Process 	<ul style="list-style-type: none"> • Define Critical Success Factors for the process • Identify Key Performance Indicators that can be

		monitor process success	Manager	measured <ul style="list-style-type: none"> Define reports and dashboards needed to monitor process performance
18	Determine process data requirements	Define the data inputs and outputs related to the process and ensure they are properly addressed in the process	<ul style="list-style-type: none"> Contractor DAT Process Owner DAT Process Manager 	<ul style="list-style-type: none"> Identify inputs for each process activity Identify outputs from process actions Align inputs and outputs with processes and tools to ensure they are sufficiently addressed, owned and managed
19	Identify technology needs	Identify and document the process activities that benefit from tool automation	<ul style="list-style-type: none"> Contractor DAT Process Owner DAT Process Manager 	<ul style="list-style-type: none"> Identify opportunities where automation and tool capabilities deliver efficiencies or are required by the process Document functional tool requirements describing the required functionality
20	Communicate and deploy the process framework	Prepare communications, training and other engagement to support widespread adoption of the process	<ul style="list-style-type: none"> Contractor DAT Process Owner DAT Process Manager 	<ul style="list-style-type: none"> Identify organizational impacts of the process Identify training requirements Define communication plan Identify role touch points and need for support Implement communications and deployment strategy

35

36 **16.1.1.1 CURRENT OPERATIONS POINTS OF CONTACT**

37

Process Acronym [DAT1.0] Establish Data Management Framework
Assumptions: Process Owner is accountable for the Data Management process but the process details will be developed primarily by the contractor and approved by the Government. The Government gathers its requirements and injects them into the process through collaboration with the contractor
Constraints:

	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
All steps in establishing the DAT framework	Process Owner	Logistics				
All steps in establishing the DAT framework	Data Manager	Logistics				
All steps in establishing the DAT framework	Contractor	HP-ES				

38

39 **16.1.1.2 DECISION TIMELINES**

40 Discussed in weekly meetings between HP-ES and the Government Data Management Process
 41 Manager

42

43 **16.1.1.3 TOOLS**

44 No specific tools are identified for developing the outcomes of [DAT 1.0]. All associated
 45 authoritative data outputs will be stored and maintained in the NGEN authoritative data source
 46 library.

47

48 **16.1.1.4 ROLES AND RESPONSIBILITIES**

49 The following table lists the roles and responsibilities for execution of this SOP.

50

Role	Responsibility
Data Management Process Owner	Accountable to ensure that the DAT process achieves its purpose and objectives and that it can support and sustain consistent operations across all stakeholders.
Data Management Process Manager	Responsible for managing seam issues, directing Government activities and supporting Contractor actions. Provides input and supports establishment of process activities that can be consistently deployed and enforced in daily operations.
Contractor	HP-ES operates and manages the Data

	Management activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations
Other Process Owners	Process owners of other ITSM or business processes that have a dependency or integration point with the DAT process

51
 52
 53
 54
 55
 56

16.1.1.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

DAT 1	Contractor	Process Owner	Process Manager	Other Process Owners
Specify process purpose, scope, goals and capabilities	R	A/R	R	C/I
Determine process relationships to other processes	R	A/R	R	C/I
Define process policies, standards and concept models	R	A/C	C	C/I
Identify process roles and responsibilities	R	A/C	C	C/I
Assign process responsibilities to organizations	R	A/R	R	C/I
Develop process and procedures	R	A/R	R	C/I
Define measurements and controls	R	A/C	C	C/I
Determine process data requirements	R	A/R	R	C/I
Identify technology needs	R	A/R	R	C/I
Communicate and deploy framework	R	A/R	R	C/I

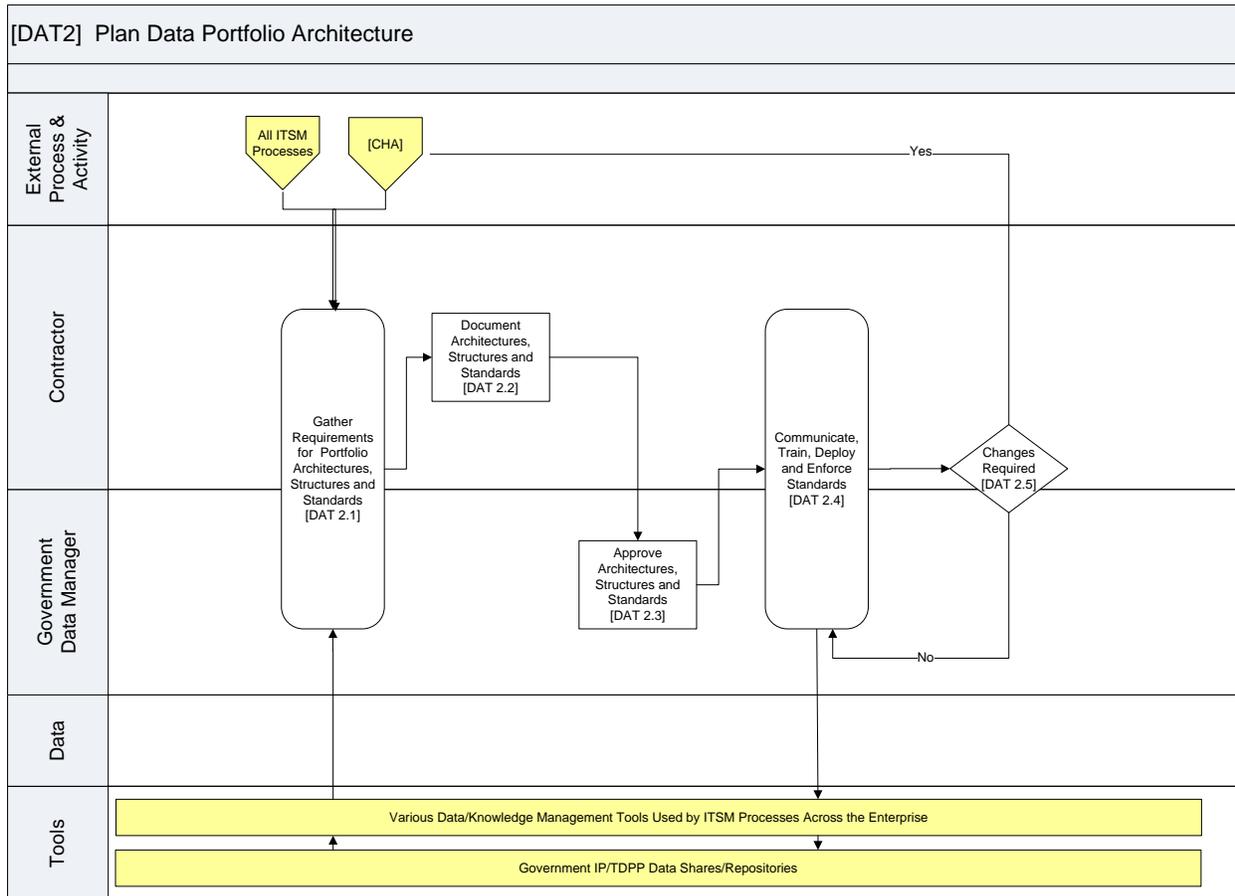
57
 58
 59
 60

16.1.1.6 METRICS

No metrics are identified to measure performance of the DAT Framework

61 **16.1.2 [DAT 2] Plan Data Portfolio Architecture**

62 Establishment of the Data Portfolio Architecture is achieved through Contractor and Government
 63 collaboration to define requirements, repositories, technology, guidance and standards for
 64 program data. This includes taxonomy, metadata and quality standards that are applied as
 65 appropriate to NGEN data.



66
 67
 68

2.0 DAT_Plan_Portfolio_Architecture_SOP_v1.0				
Step	Process Model Task	Action	Role(s)	Details
1	Gather requirements for portfolio architectures, structures and standards	Engage appropriate stakeholders to identify requirements for architecture and standards	<ul style="list-style-type: none"> Contractor Data Manager 	<ul style="list-style-type: none"> Meet with stakeholders to gather all data architecture requirements Based on DoD guidance , identify standards for data normalization and to facilitate data access (i.e.

				Metadata standards) <ul style="list-style-type: none"> Identify acceptable data formats and technology that support open yet controlled sharing of information
2	Document architecture and standards	The Contractor documents standards to the degree necessary to achieve consistent, enforceable standards	<ul style="list-style-type: none"> Contractor 	<ul style="list-style-type: none"> Using approved templates or formats, document the establish architecture and document content and formatting standards
3	Approve architecture and standards	Approve contractor developed architectures and standards to be deployed across the enterprise	<ul style="list-style-type: none"> DAT Process Owner 	<ul style="list-style-type: none"> Gather appropriate stakeholders Review standards against requirements Approve or remediate standards
4	Communicate, train, deploy and enforce standards	Implement the standards approved by the Government.	<ul style="list-style-type: none"> Contractor Data Manager 	<ul style="list-style-type: none"> Assess organizational change and organizational impacts of the standards Develop training Develop communication strategy Deploy training and support adoption Monitor process and enforce standards
5	Architecture or Standards change required	Decision point, are changes to the data portfolio or its associated architecture needed?	<ul style="list-style-type: none"> Contractor Data Manager 	<ul style="list-style-type: none"> Monitor process architecture and standards to determine if a change is required Engage the change management process as appropriate to facilitate changes to portfolio, standards and architecture

70 **16.1.2.1 CURRENT OPERATIONS POINTS OF CONTACT**

71

Process Acronym [DAT2] Plan Portfolio Architecture						
Assumptions: Process Owner is accountable for the Data Management process but the architecture and standard details will be developed by the contractor and approved by the Government						
Constraints: DM processes are primarily developed and executed by the contractor. Government involvement in the development of standards has been limited to GPR IP/TDPP.						
Responsible Parties						
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
DAT 1,4,5	Process Manager	Logistics			Homeport, IP Inventory	
DAT 3	Process Owner	Logistics APLM				

72

73 **16.1.2.2 DECISION TIMELINES**

74 Updates to standards can be implemented only in monthly CDRL reports.

75

76 **16.1.2.3 TOOLS**

77 No specific tool use in the activities of this process

78

79 **16.1.2.4 ROLES AND RESPONSIBILITIES**

80 The following table lists the roles and responsibilities for execution of this SOP.

81

82

Role	Responsibility
Contractor	The contractor retains responsibility for developing, implementing architecture and standards and for enforcing standards within their own organization.
Data Management Process Owner	Accountable to ensure that the DAT architecture and standards meet requirements and are approved by the Government stakeholders.
Data Management Process Manager	Responsible for managing seam issues, directing Government activities and supporting Contractor actions. Provides input and supports establishment of architectures and standards that can be consistently deployed and enforced in daily operations.

83

84 **16.1.2.5 R/A/C/I**

85 This following table contains a task-level RACI chart designating which of the above roles are
 86 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process
 87 Activity task:
 88

DAT 2	Contractor	Process Owner	Process Manager
Gather requirements for portfolio architectures, structures, and standards	A/R	C/I	R
Document architectures, structures and standards	A/R	C/I	C/I
Approve architectures, structures and standards	C/I	A/R	C/I
Communicate, train, deploy and enforce standards	A/R	C/I	R
Changes required	A/R	C/I	C/I

89

90

91 **16.1.2.6 METRICS**

92 No specific metrics are captured for establishing DAT Architecture and Standards

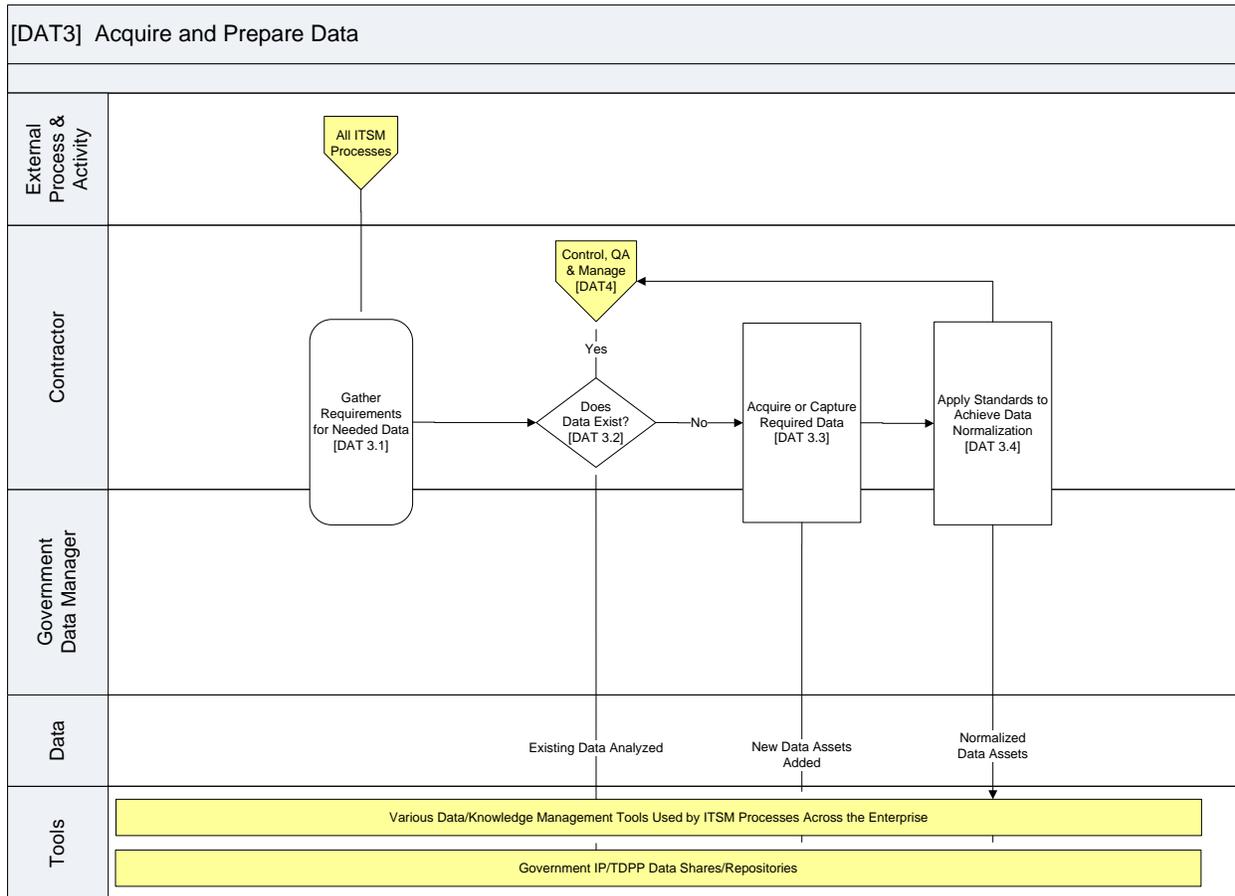
93

94

95

96 **16.1.3 [DAT 3] Acquire and Prepare Data**

97 Data is acquired from many sources, including data operational process data capture. This
 98 information then goes through standardization and preparation for publication and access by
 99 appropriate stakeholders. Many tools across the enterprise will be used for data capture and
 100 acquisition.



101
 102
 103

3.0 DAT_Aquire_Prepare_SOP_v1.0				
Step	Process Model Task	Action	Role(s)	Details
1	Gather requirements for needed data	Identify the data requirements to achieve DAT objectives	<ul style="list-style-type: none"> Contractor Data Manager 	<ul style="list-style-type: none"> Identify data requirements that align to NGEN's data management strategy and objectives Consult with government and other supporting contractors to identify data

				required to support the network
2	Does the required data exist?	Identify if the needed data exists or needs to be created	<ul style="list-style-type: none"> • Contractor • Data Manager 	<ul style="list-style-type: none"> • Search through existing data repositories to determine if data exists or if it needs to be developed.
3	Capture required data	Capture the required data using appropriate tools, templates and standards	<ul style="list-style-type: none"> • Contractor • Data Manager 	<ul style="list-style-type: none"> • Capture the required data using the appropriate tools and leveraging designated standards, templates and architectures
4	Apply standards to achieve data normalization	Standardize data through applying defined standards and structures	<ul style="list-style-type: none"> • Contractor • Data Manager 	<ul style="list-style-type: none"> • Verify that the incumbent contractor has effectively applied standards to CDRL reports • Work with all owners of authoritative data sources to verify that standards are being applied to data assets

104

105 **16.1.3.1 CURRENT OPERATIONS POINTS OF CONTACT**

106

Process Acronym [DAT 3.0] Acquire and Prepare Data						
Assumptions: The contractor will have primary responsibility for identifying and capturing the appropriate data however, the Government Data Manager will gather the Government requirements and will assess the contractors scope of data captured to ensure it achieves desired objectives.						
Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
1-4	Process Manager	Logistics			Authoritative Data Sources	

107

108 **16.1.3.2 DECISION TIMELINES**

109 Updates to data repository occur monthly.

110

111 **16.1.3.3 TOOLS**

112 A large variety of tools are used to acquire and prepare data [DAT 3.0]. A list of tools used to
 113 capture and manage data is identified in the NGEN Data Management Plan (DMP).

114

115 **16.1.3.4 ROLES AND RESPONSIBILITIES**

116 The following table lists the roles and responsibilities for execution of this SOP.

117

Role	Responsibility
Contractor	The contractor is a primary provider of data where they capture data in the process of daily operations. As a part of this data capture, the contractor also prepares data to comply with published standards.
Data Manager	Although many of the activities are primarily contractor performed processes, the Data Manager is critical in identification of the requirements and ensuring data is properly prepared.

118

119 **16.1.3.5 R/A/C/I**

120 This following table contains a task-level RACI chart designating which of the above roles are
 121 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process
 122 Activity task:

123

DAT 3	Contractor	Process Owner	Process Manager
Gather requirements for needed data	A/R	C/I	R
Does the data exist?	A/R	C/I	C/I
Acquire or capture required data	A/R	C/I	R
Apply standards to achieve data normalization	A/R	C/I	R

124

125

126 **16.1.3.6 METRICS**

127 The following metrics will be captured for data capture

128

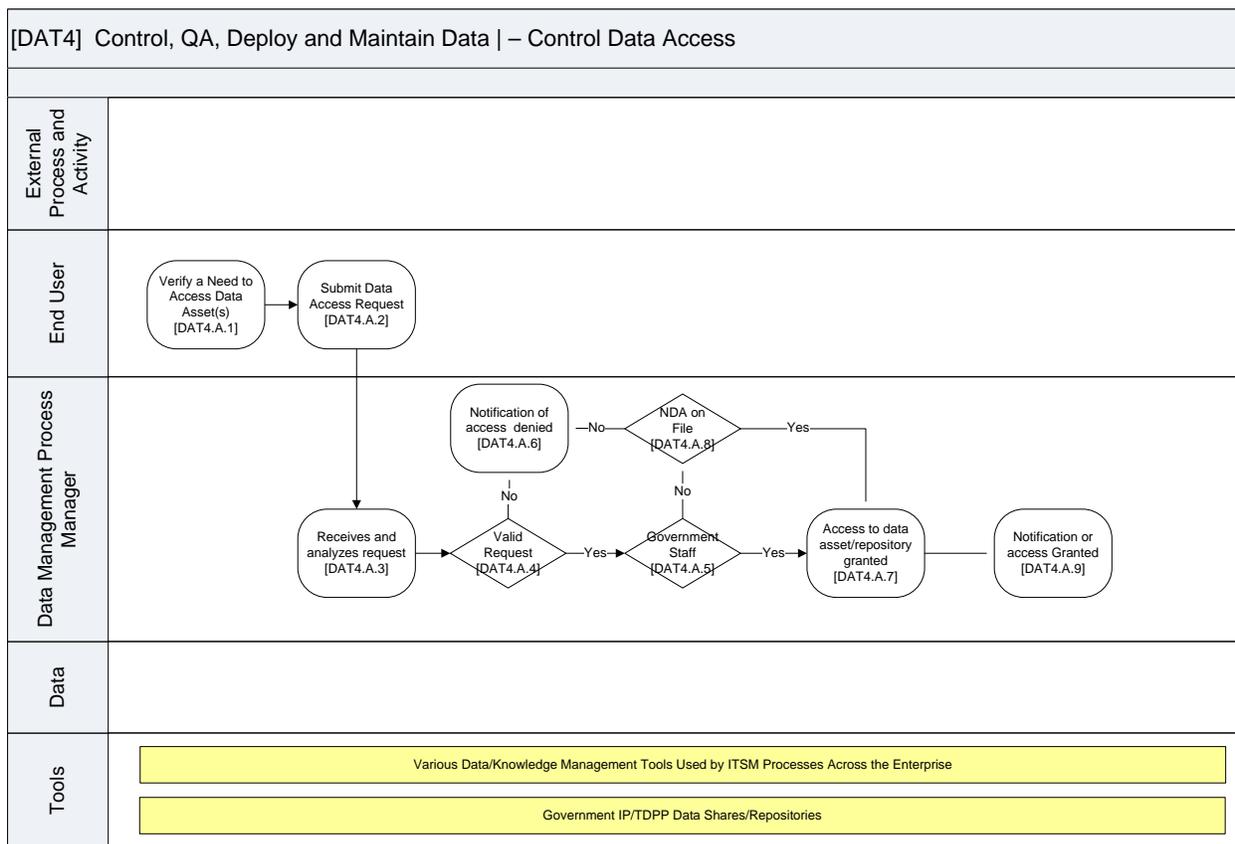
Metric – KPI # 1 Count of Artifacts on the IP Share	
Description	Monthly report of the number of new, modified or archived data assets in the IP/TDPP repository
Relevance	Medium – Facilitates a general inventory of data assets and provides trending that could have a significant impact on the value and quality of the data repository.
Target Values	N/A
Calculation	Monthly total number data assets added, modified or archived
Notes	

129
130

131 **16.1.4 [DAT 4] Control, QA, Deploy and Maintain Data**

132 Two key activities performed by the Government in this area consist of the Government’s
 133 process for controlling access to the data. It also includes inspection, acceptance and
 134 remediation effort focused on audits and analysis of select data assets to determine if the assets
 135 conform to the acceptance criteria defined in CoSC Attachment 4. The Government directs
 136 remediation of assets that do not meet acceptance criteria. The Incumbent Contractor remediates
 137 data assets as directed to achieve Government acceptance. Government requested data (such as
 138 data supporting Incentive Projects) is also reviewed by Government subject matter experts
 139 (SMEs) for acceptance in this step.
 140

141 **DAT 4.A Control Data Access**



142
143

4.A DAT_Control_Access_SOP_v1.0				
Step	Process Model Task	Action	Role(s)	Details
1	Verify a need for data access	Determine that access to the desired data is a	<ul style="list-style-type: none"> Any NGEN program stakeholder 	<ul style="list-style-type: none"> Confirm the authorization request is a valid request for access

		valid request		
2	Submit data access request	Complete and submit a data access request form	<ul style="list-style-type: none"> Any NGEN program stakeholder 	<ul style="list-style-type: none"> Complete the required steps documented in the data access form. If a contractor, obtain appropriate Government sponsor approval
3	Receive and analyze the data access request	Receive and analyze the request	<ul style="list-style-type: none"> Data Manger 	<ul style="list-style-type: none"> Receive the request and confirm that all required steps have been taken for request. Confirm that there is a valid need for the access
4	Request Approved?	Decision point, is the data access request approved or denied?	<ul style="list-style-type: none"> Data Manger 	<ul style="list-style-type: none"> Based on the defined criteria make a determination if the request is approved or denied
5	Government data access request?	Is the request for a Government employee	<ul style="list-style-type: none"> Data Manager 	<ul style="list-style-type: none"> If yes, proceed to granting access
6	Valid NDA on file	Request for contractor access require a signed NDA	<ul style="list-style-type: none"> Data Manager 	<ul style="list-style-type: none"> Does the contractor's employer have a signed NDA on file with the NEN Program? If yes, access can be granted. If no, access denied.
7	Access to data asset/repository granted	Perform the steps needed to grant the access requested	<ul style="list-style-type: none"> Data Manger 	<ul style="list-style-type: none"> Determine if access is to a specific data asset, to a repository or to the full set of data Perform actions required to grant access Send communication to the requestor or the person receiving access notifying

				them that access is has been granted.
8	Notification of access granted	End-user or requestor receives notification of access granted	• Data Manager	• End-use or requestor confirms notification of access received.

144

145 **16.1.4.1 CURRENT OPERATIONS POINTS OF CONTACT**

146

Process Acronym [DAT 4A] Control, QA, Maintain Data Control Access to Data						
Assumptions:						
Constraints:						
		Responsible Parties				
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
1,2,8	End-user or Requestor	Any NGEN affiliated stakeholder			Excel Request Template	
3,4,5,6,7	Data Manager	Logistics			IP Shares SearchNAVY	

147

148 **16.1.4.2 DECISION TIMELINES**

149 Data requests are received and analyzed on a first come, first serve basis.

150

151 **16.1.4.3 TOOLS**

152 The IP Shares are utilized to grant access to users with a vetted need to know, SearchNAVY is
 153 used to facilitate mining of the IP corpus.

154

155 **16.1.4.4 ROLES AND RESPONSIBILITIES**

156

157 The following table lists the roles and responsibilities for execution of this SOP.

158

Role	Responsibility
NGEN Stakeholder	Any person with legitimate reason to request access to NGEN Data.

Data Manager	Controls the practices of requesting access and determines if there is a need to access data and verifies that all required steps have been completed to grant the requested access
---------------------	---

159
 160
 161
 162
 163

16.1.4.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

DAT 4A	Contractor	Process Owner	Process Manager	End-Users
Verify a need to access data assets	C/I	A	R	R
Submit data access request	C/I	A	R	R
Receive and analyze request	C/I	A	R	C/I
Valid access request	C/I	A	R	C/I
Determine if the request is for Government staff	C/I	A	R	C/I
Determine if NDA is on file	C/I	A	R	C/I
Provide access to data repository	R	A	R	C/I
Notification of access request denied	C/I	A	R	C/I
Notification of access request granted	C/I	A	R	C/I

164
 165
 166
 167
 168

16.1.4.6 METRICS

The following metrics will be captured for data capture

Metric – KPI # 5 Mean Time to Publish	
Description	Measurement of average time required to publish data to the data repository once a need has been identified
Relevance	Medium
Target Values	Less than 30 days

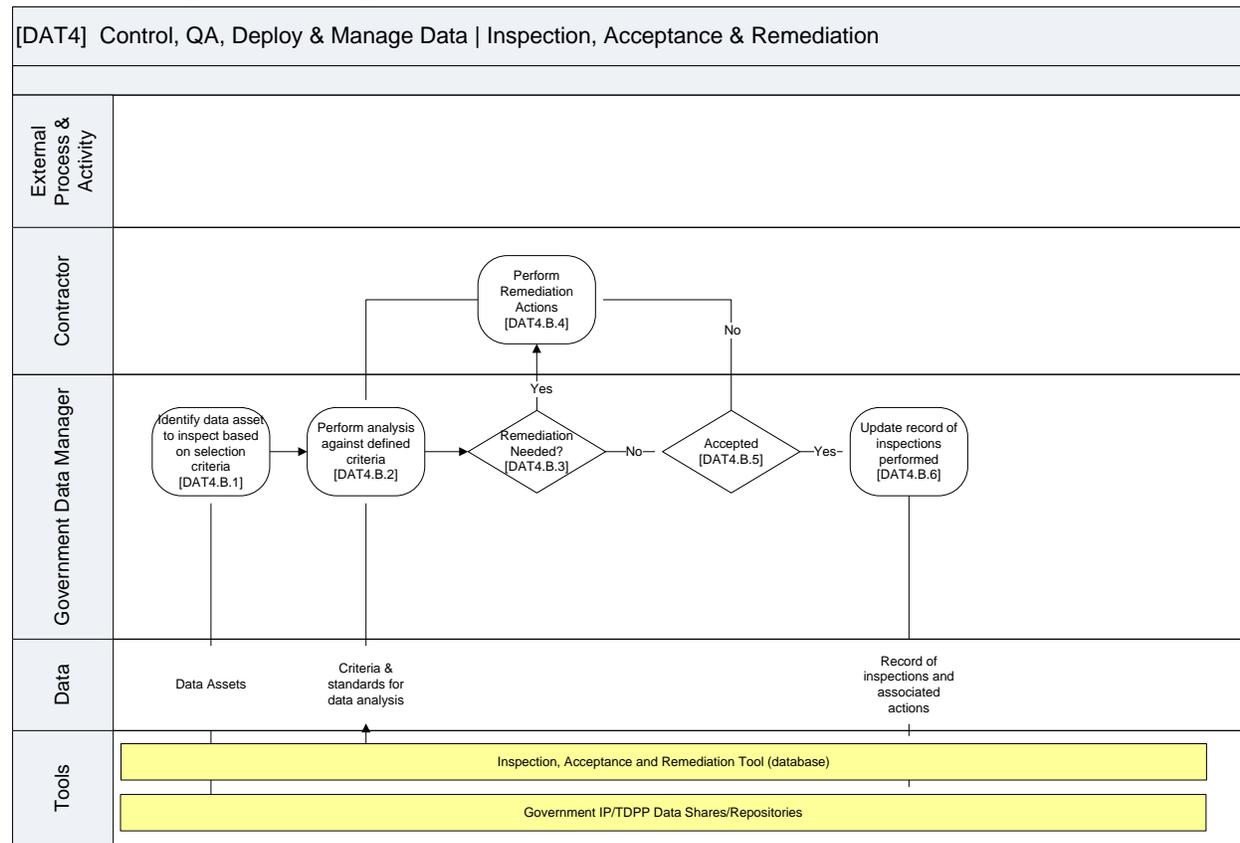
Calculation	Total time elapsed between identification of data gap to the data actually being published to the repository divided by the number of gaps identified multiplied by one hundred.
Notes	

169

170

171
 172

[DAT4.B] Inspection, Acceptance and Remediation Sub-Process



173
 174

4.B DAT_IA&R_SOP_v1.0				
Step	Process Model Task	Action	Role(s)	Details
•	Identify data asset to inspect based on selection criteria [DAT 4.B.1]	From the data repository assets are identified for inspection and remediation prior to acceptance	• Data Manager	• Specific data assets are identified for inspection and remediation based on prioritization and need for the data.
•	Perform analysis against defined criteria [DAT 4.B.2]	Using defined criteria, the asset is evaluated for acceptance	• Data Manager	• Identify the criteria for analysis based on the data type and its purpose • Assess the data asset

•	Determine is remediation is required [DAT 4.B.3]	Decision point, is remediation required to get the asset up to requirements?	• Data Manager	<ul style="list-style-type: none"> Based on analysis, is the data asset acceptable as-is? Is remediation required? Is it accepted with exception for the successor contractor to remediate later?
•	Perform remediation actions [DAT 4.B.4]	Complete actions to complete remediation	• Contractor	<ul style="list-style-type: none"> Review the remediation requirements and associated timelines Assign a resource to perform the remediation Perform actions required to complete remediation Record actions taken Resubmit to Government for review
•	Accepted [DAT 4.B.5]	Decision point to determine if the data is accepted	• Data Manager	<ul style="list-style-type: none"> Based on analysis of the data and its associated requirements, is the data accepted?
•	Update record of inspections performed [DAT 4.B.6]	Update inspection record of assets reviewed	• Data Manager	<ul style="list-style-type: none"> Update the record log of assets reviewed and the outcome of the review

175

176 **16.1.4.7 CURRENT OPERATIONS POINTS OF CONTACT**

177

Process Acronym [DAT 4.0] Control, QA, Deploy and Maintain Data Inspection, Acceptance & Remediation						
Assumptions: FAR 46 requires IA&R activities associated with program data assets						
Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
1, 2, 3, 5, 6,	Process Manager	Logistics			IA&R Database	

178

179 **16.1.4.8 DECISION TIMELINES**

180 Decision timeline for Inspection, Acceptance and Remediation is based on the type of asset
 181 being evaluated and the requirements of the Government customer. Data must be accepted
 182 before it can be delivered, prioritization of datasets for inspection and acceptance must be in
 183 alignment with the transition of services.

184
 185 **16.1.4.9 TOOLS**

186 The IA&R database is used to maintain the inspection criteria and records the assets inspected,
 187 accepted, and remediated. This database will then be used to determine if data sets are ready for
 188 Delivery at that time of transition.

189
 190 **16.1.4.10 ROLES AND RESPONSIBILITIES**

191 The following table lists the roles and responsibilities for execution of this SOP.
 192

Role	Responsibility
Contractor	The contractor retains responsibility performing remediation actions and resubmitting to the Government
Data Manager	Provides the staffing, criteria and approach for the IA&R tasking.

193
 194 **16.1.4.11 R/A/C/I**

195 This following table contains a task-level RACI chart designating which of the above roles are
 196 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process
 197 Activity task:

DAT 4B	Contractor	Process Owner	Process Manager
Identify data asset to inspect based on selection criteria	C/I	A	R
Perform analysis against defined criteria	C/I	A	R
Remediation needed	C/I	A	R
Perform remediation actions	R	A	R
Asset accepted	C/I	A	R
Update record of inspections performed	C/I	A	R

198
 199
 200
 201
 202

16.1.4.12 METRICS

The following metrics will be captured for data capture

Metric -- KPI # 5 Mean Time to Remediate	
Description	Average time required to make modifications once the Government identifies the need for remediation
Relevance	Medium
Target Values	30 days
Calculation	Monthly total number of work days required to complete remediation actions divided by the number of remediation actions complete
Notes	Some data assets require a significant amount of tie to remediate based upon their complexity. The goal of 30 days is a contractual requirement within Attachment 4; however there is no penalty for missing the goal.

203
 204

Metric – KPI # 7 Percentage of Inspections Requiring Remediation	
Description	Of the total inspections complete, what percentage of the data assets required remediation
Relevance	Medium
Target Values	NA
Calculation	Monthly number of data assets requiring remediation divide by the total number of inspections multiplied by one hundred
Notes	

205
 206

Metric – KPI # 8 Number of Artifacts Accepted

Description	Total count of data artifacts accepted after completing inspection.
Relevance	Medium
Target Values	NA
Calculation	Monthly total number of data artifacts accepted after completing the inspection. Total does not include artifacts that went through remediation.
Notes	

207

208

Metric – KPI # 9 Number of Artifacts Accepted with Exception

Description	Total count of data artifacts accepted with remediation actions pending
Relevance	Medium
Target Values	NA
Calculation	Monthly total number of data artifacts accepted with pending remediation actions
Notes	

209

210

Metric – KPI # 10 Number of Artifacts Remediated

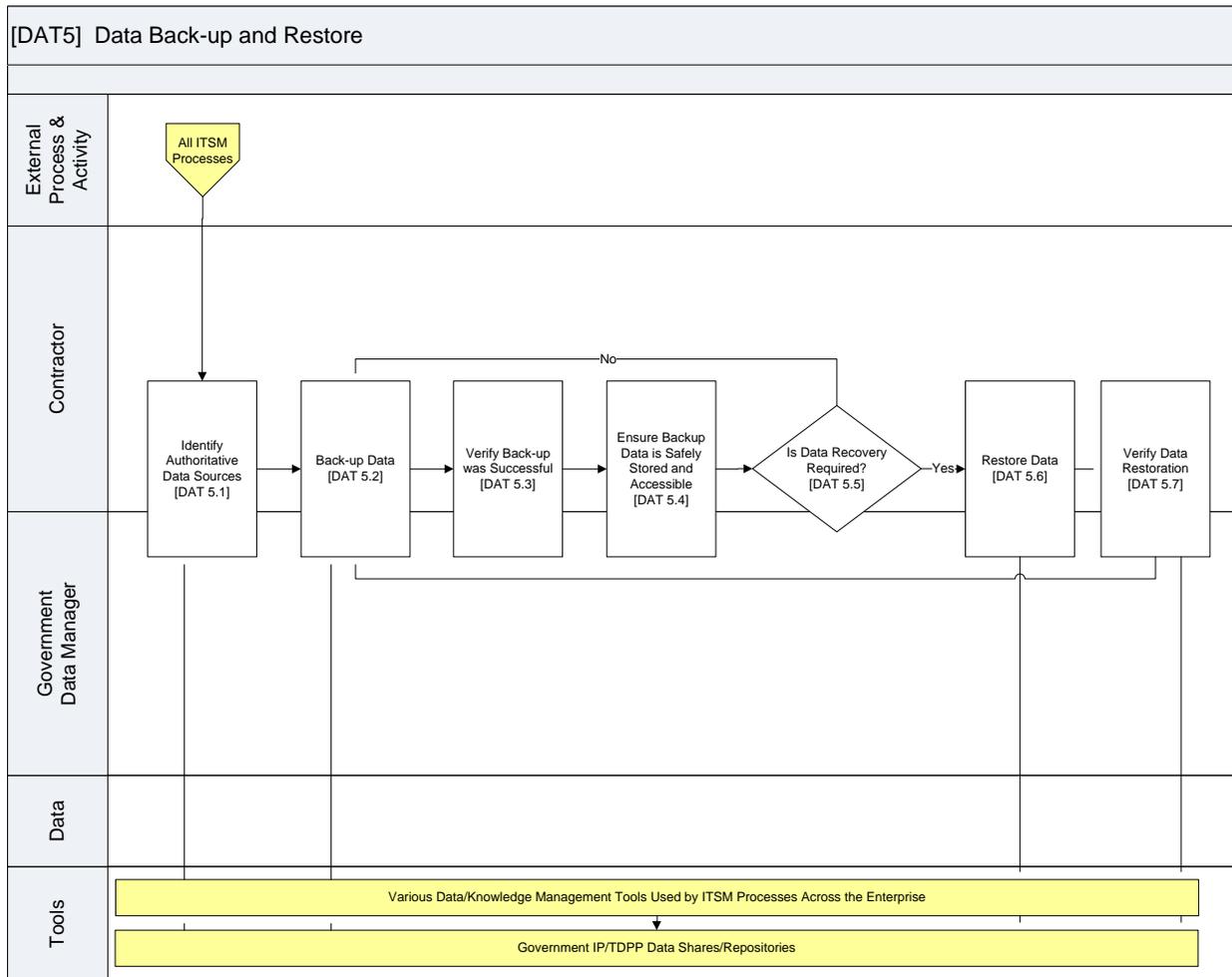
Description	Total count of data artifacts remediated
Relevance	Medium
Target Values	NA
Calculation	Monthly total of data artifacts remediated
Notes	

211

212
213

214
 215 **16.1.5 [DAT 5] Back-up and Restore**

216 Data is a valuable asset that must be protected through adequate back-up procedures for all
 217 authoritative data sources and associated assets. Recovery is a vital aspect of this process.
 218 Recovery processes efficiently and effectively restores data so that it continues to be available
 219 and accessible.



220
 221
 222

5.0 DAT_Back-up_Restore_SOP_v1.0				
Step	Process Model Task	Action	Role(s)	Details
1	Identify authoritative data sources	Identify the authoritative data sources that fall under data back-	<ul style="list-style-type: none"> Contractor DAT Process Owner 	<ul style="list-style-type: none"> Validate a list of authoritative data sources that must be backed up.

		up guidelines	<ul style="list-style-type: none"> • DAT Process Manager 	
2	Back-up data	Perform back-up procedures	<ul style="list-style-type: none"> • Contractor • Data Manager 	<ul style="list-style-type: none"> • Complete the required steps to effectively back up data. • These steps will be specific to the data repository being backed up. See work instructions for each data system/tool
3	Verify back-up was successful	Validate back-up completed successfully	<ul style="list-style-type: none"> • Contractor • Data Manger 	<ul style="list-style-type: none"> • Run appropriate tests to confirm back-up completed successfully covering all data.
4	Ensure backed data is safely stored and accessible	Store data back-ups in a place that is secure and accessible	<ul style="list-style-type: none"> • Contractor • Data Manager 	<ul style="list-style-type: none"> • Establish a safe and secure location for data back-up that is accessible but protected separately from the original data.
5	Is data recovery required?	Decision point: is data recovery required?	<ul style="list-style-type: none"> • Contractor • Data Manager 	<ul style="list-style-type: none"> • Determine if there has been a loss or degradation of data requiring a data restoration or recovery
6	Perform data recovery	Restore required data into its authoritative data source	<ul style="list-style-type: none"> • Contractor • Data Manager 	<ul style="list-style-type: none"> • Perform procedures to restore data from the most recent back-up • Specific procedures will depend on the source and type of data to be restored. See specific work instructions for the designated data source
7	Verify data recovery	Verify that the data was effectively recovered or restored	<ul style="list-style-type: none"> • Contractor • Data Manager 	<ul style="list-style-type: none"> • Perform a validation of the data assets to ensure that appropriate recovery was achieved • Document any known gaps of lost data

				<ul style="list-style-type: none"> • Provide a report of the analysis
--	--	--	--	--

223

224 **16.1.5.1 CURRENT OPERATIONS POINTS OF CONTACT**

225

Process Acronym [DAT 5.0] Data Back-up and Restore						
Assumptions: The Government and Contractors will both have responsibilities for data back-up and recovery based on the data source.						
Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
1	DAT Process Owner	Logistics				
1-7	Data Manager	Logistics			IP Shares SearchNAVY	
1-7	Contractor	HP				

226

227 **16.1.5.2 DECISION TIMELINES**

228 Data back-up and recovery timelines will vary depending on agreements supporting the specific
 229 data repository. Some data is of a critical nature requiring immediate restoration while some
 230 data sources may allow for multiple days for the recovery.

231

232 **16.1.5.3 TOOLS**

- The IP data share repositories
- Various data repositories used by operations and ITSM teams across the enterprise.

235

236 **16.1.5.4 ROLES AND RESPONSIBILITIES**

237

238 The following table lists the roles and responsibilities for execution of this SOP.

239

Role	Responsibility
DAT Process Owner	Has accountability to ensure that the data sources are appropriately identified and

	requirements recorded
Data Manager	Controls the practices of data back-up and recovery of the Government’s IP data shares
Contractor	Has accountability to perform back-up and recovery for all contractor provided data repositories and tools

240

241 **16.1.5.5 R/A/C/I**

242 This following table contains a task-level RACI chart designating which of the above roles are
 243 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process
 244 Activity task:

DAT 5	Contractor	Process Owner	Process Manager
Identify authoritative data sources	R	A	R
Back-up data	A/R	C/I	R
Verify back-up was successful	A/R	C/I	R
Ensure back-up data is safely stored and accessible	A/R	C/I	R
Is data recovery required	A/R	C/I	R
Restore Data	A/R	C/I	R
Verify data restoration	A/R	C/I	R

245

246

247 **16.1.5.6 METRICS**

248

Metric – KPI # 16 Mean Time to Restore	
Description	Average time required to restore data once a need has been identified
Relevance	High
Target Values	NA
Calculation	Total time required to restore data divided by the number of requests multiplied by one-hundred.

Notes	
--------------	--

249

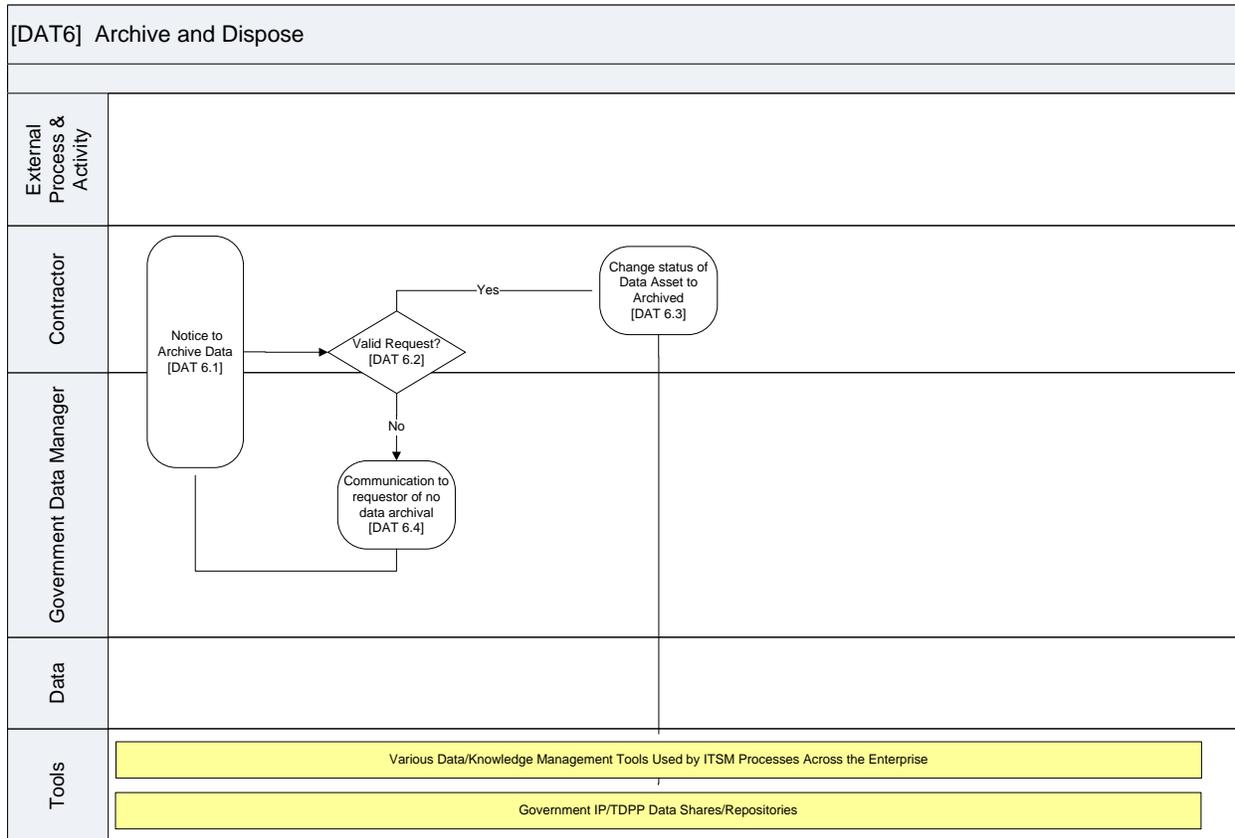
250

251

252

253 **16.1.6 [DAT 6] Archive and Dispose**

254 When a data asset has reached its effective end of life or it is determined to be inaccurate or
 255 inappropriate, the asset is archived. For data assets that are stored in the authoritative data
 256 sources and on the data shares, the Incumbent Contractor performs this function as part of its
 257 Data Management responsibilities. Data assets are not deleted but their status is change to
 258 indicate that the asset is no longer in use. The data assets remain in an archive where they can be
 259 accessed as appropriate for historical and program related needs.



260
 261
 262

6.0 DAT_Archive_Dispose_SOP_v1.0				
Step	Process Model Task	Action	Role(s)	Details
1	Notice to archive data	Request to archive data is received	<ul style="list-style-type: none"> Data Manager 	<ul style="list-style-type: none"> A notice to archive data is received by the data manager. Can come through a variety of channels Contractor can be one of

				the channels of a request to archive data
2	Valid Request?	Decision Point, is the request a valid request for data archival?	<ul style="list-style-type: none"> • Data Manager 	<ul style="list-style-type: none"> • The request is reviewed and assessed to determine if the request is valid. • Contractor and other stakeholders may be consulted related to the request
3	Change status of data asset to archived	The status of the data asset is changed to archived	<ul style="list-style-type: none"> • Data Manager 	The data asset is edited and appropriate changes are made to change the status to an archived status
4	Communication to requestor of no data archival	Communication to the requestor related to the decision not to archive the requested data	<ul style="list-style-type: none"> • Data Manager 	<ul style="list-style-type: none"> • Results of the analysis is documented and communicated back to the requestor • A new request for data archive will need to be submitted to reconsider the issue/request

263

264 **16.1.6.1 CURRENT OPERATIONS POINTS OF CONTACT**

265

Process Acronym [DAT 6.0] Archive and Dispose Data						
Assumptions:						
Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
1-4	Data Manager	Logistics			IP Inventory	

266

267 **16.1.6.2 DECISION TIMELINES**

268 Data is archived as needed when assets are determined to be at their end of life. The IP Inventory
 269 is published monthly; any changes to the status of a data asset must be updated within the IP
 270 Inventory by the end of the month.

271

272 **16.1.6.3 TOOLS**

273 The IP Inventory enables users to view standard metadata about each NMCI data asset. The
 274 Status column denotes if the data asset has been archived.

275

276 **16.1.6.4 ROLES AND RESPONSIBILITIES**

277

278 The following table lists the roles and responsibilities for execution of this SOP.

279

Role	Responsibility
Data Manager	Control and manage the practices of reviewing requests for data archival. Although the Data Manager is listed as the party responsible, He/she will manage a team performing many of the tasks over which he/she is responsible.

280

281 **16.1.6.5 R/A/C/I**

282 This following table contains a task-level RACI chart designating which of the above roles are
 283 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process
 284 Activity task:

DAT 6	Contractor	Process Owner	Process Manager
Notice to archive data	A/R	C/I	R
Valid Request	A/R	C/I	R
Change status of data asset to archived	A/R	C/I	R
Communication to requestor of data archival	A/R	C/I	R

285

286

287 **16.1.6.6 METRICS**

288 The following metrics will be captured for data capture

289

Metric – KPI # 6 Mean Time to Remediate	
Description	Monitoring and reporting on the average time required to analyze a request a remediation request (including data archival).

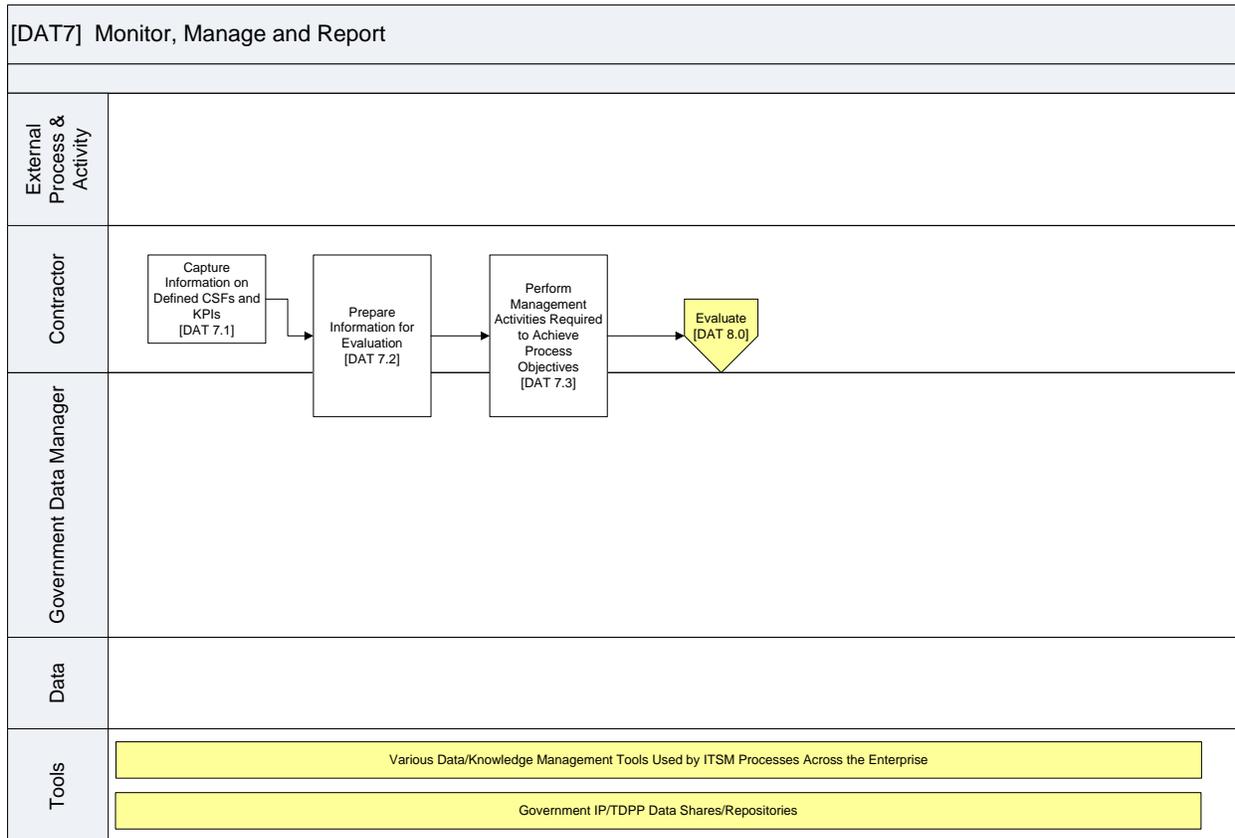
Relevance	High
Target Values	NA
Calculation	Total time required to review and respond to a remediation request divided by the number of requests multiplied by one-hundred.
Notes	Internal report to measure response to data archival requests.

290

291

292 **16.1.7 [DAT 7] Monitor, Report and Manage Data Management**

293 Gathering the data required to assess the effectiveness of the Data Management process provide
 294 the information needed to make operational adjustments in the daily operations of the process.
 295 They also feed the evaluation of the process that identifies opportunities to improve through
 296 Continual Service Improvement.



297
 298
 299

7.0 DAT_Monitor_Repot_Mange_SOP_v1.0				
Step	Process Model Task	Action	Role(s)	Details
1	Capture information on defined CSFs and KPIs	Gather information from reports supporting CSFs and KPIs	<ul style="list-style-type: none"> • Data Manager 	<ul style="list-style-type: none"> • Gather data from process performance reports • Confirm that adequate and quality information is available for analysis

2	Prepare information for evaluation	Prepare gathered data to support effective analysis	<ul style="list-style-type: none"> • Data Manager 	<ul style="list-style-type: none"> • Normalize data for comparison • Format information and prepare for presentation and use in analysis of the process
3	Perform management activities required to achieve process objectives	Use the information gathered to make operational adjustments to process activities	<ul style="list-style-type: none"> • Data Manager 	<ul style="list-style-type: none"> • Assess the data gathered to determine if objectives are being met • Determine if adjustments are needed to daily process activities • Identify actions required to adjust process activities to achieve desired outcomes

300

301 **16.1.7.1 CURRENT OPERATIONS POINTS OF CONTACT**

302

Process Acronym [DAT 7.0] Monitor, Report and Manage						
Assumptions:						
Constraints:						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
1-3	Data Manager	Logistics				

303

304 **16.1.7.2 DECISION TIMELINES**

305 The Data Manager will review reports for process activities as frequently as they deem necessary
 306 to monitor process performance and make required adjustments. Most of the activities will occur
 307 weekly to support DAT working group meetings.

308

309 **16.1.7.3 TOOLS**

310 TBD

311

312 **16.1.7.4 ROLES AND RESPONSIBILITIES**

313

314 The following table lists the roles and responsibilities for execution of this SOP.

315

Role	Responsibility
Data Manager	Oversees the actions and activities focused on gathering data and DAT management operations.

316

317 **16.1.7.5 R/A/C/I**

318 This following table contains a task-level RACI chart designating which of the above roles are
 319 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process
 320 Activity task:

DAT 7	Contractor	Process Owner	Process Manager
Capture information on defined CSFs and KPIs	A/R	C/I	R
Prepare information for evaluation	A/R	C/I	R
Perform management activities required to achieve process objectives	A/R	C/I	R

321

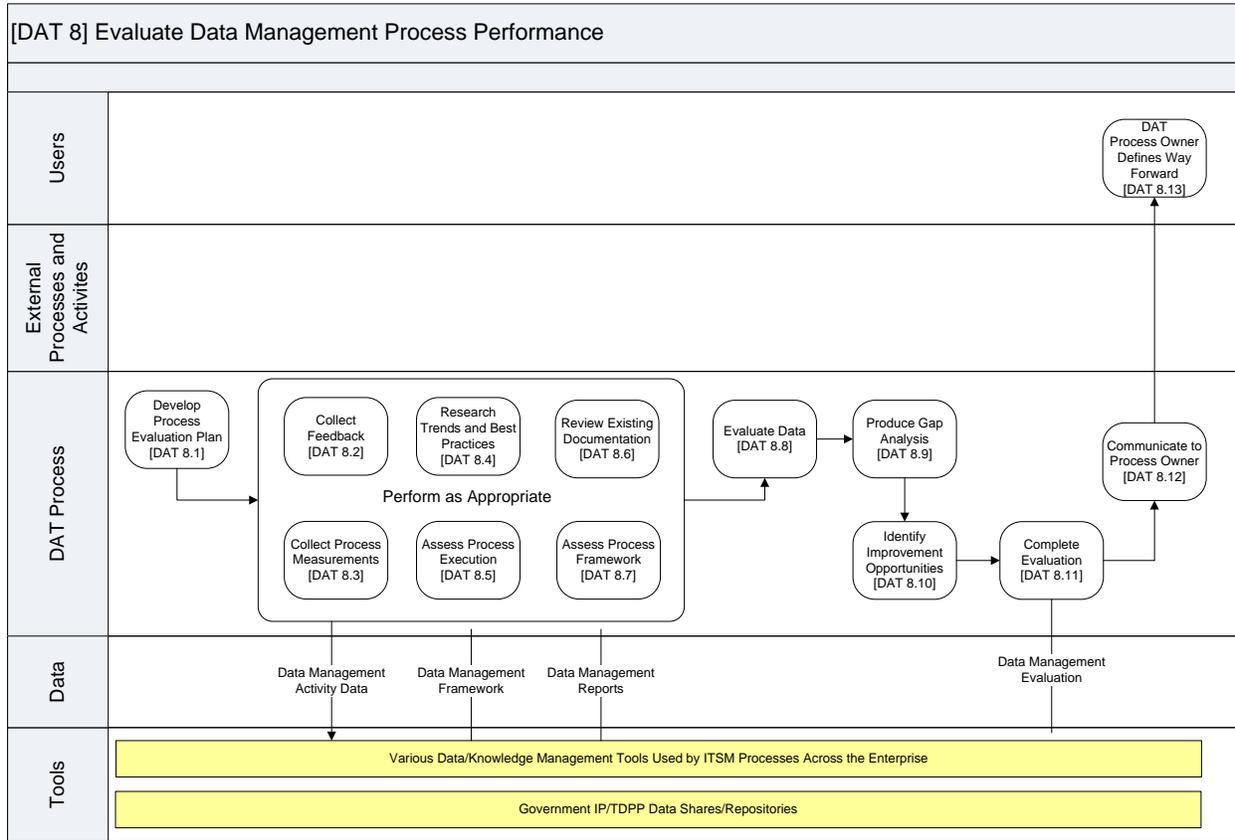
322 **16.1.7.6 METRICS**

323 The following metrics will be captured for data capture
 324 NA

325

326 **16.1.8 [DAT 8] Evaluate Data Management**

327 Monitoring and evaluating process performance along with the activities required to maintain a
 328 standard and consistent process across the enterprise is a vital part of the Data Management
 329 process. The tasks defined below outline the considerations and activities that must be
 330 performed by the Data Manager as a part of evaluating the overall effectiveness of the process.



331
 332
 333

8.0 DAT_Monitor_Evaluate_SOP_v1.0				
Step	Process Model Task	Action	Role(s)	Details
1	Develop process evaluation plan	Establish the processes required to monitor and evaluate DAT process performance	<ul style="list-style-type: none"> Data Manager 	<ul style="list-style-type: none"> Define the Critical Success Factors (CSFs) and Key Performance Indicators (KPIs) used to monitor process performance. Define the periods of evaluation and expectations for process review Define and align roles and responsibilities for performing defined tasks

2	Collect feedback	Gather data related to process performance	• Data Manager	• Define what data can be gathered
3	Collect process measurements	Process gathered data and perform analysis and calculate defined measurements	• Data Manager	• Gather, process data so that it can be analyzed
4	Research trends and best practices	Identify trends and successful practices that are or should be incorporated into the DAT process	• Data Manager	<ul style="list-style-type: none"> • Identify trends associated with the DAT process • Identify benefits and successes of the process • Identify good practices that could help improve DAT process tasks
5	Assess process execution	Analyze data gathered to assess the effectiveness and efficiency of the DAT process	• Data Manager	• Analyze the data gathered to determine required actions to support and improve the DAT process
6	Review existing documentation	Review the defined process to determine if changes are needed or beneficial	• Data Manager	<ul style="list-style-type: none"> • Review the documented process and compare analysis results with established practices • Identify training opportunities to better establish existing processes • Identify opportunities to improve the DAT process or the existing documentation
7	Assess the process framework	Review the process framework for opportunities to improve tasks and activities that address process gaps	• Data Manager	<ul style="list-style-type: none"> • Evaluate the process framework to identify gaps that may be causing process pain points • Identify where failure points have occurred or could occur • Establish a Continual Process Improvement

				practice that includes process stakeholders
8	Evaluate data	Evaluate all the data gathered and potential recommendations for CPI	• Data Manager	<ul style="list-style-type: none"> • Evaluate all data gathered • Review recommendations and suggestions
9	Produce gap analysis	Produce a gap analysis recommendations	• Data Manger	<ul style="list-style-type: none"> • Produce a report of the gap analysis and recommendations • Prepare to present the gathered information to stakeholders and process governance teams
10	Identify improvement opportunities	With the input of stakeholders and process governance teams, identify the actions required to better achieve process objectives	• Data Manager	<ul style="list-style-type: none"> • Meet with stakeholders and process Governance roles to review and assess recommendations • Make decisions on recommendations to address gaps identified
11	Complete evaluation	Document the steps needed to complete the recommendations of the DAT leadership team	• Data Manager	<ul style="list-style-type: none"> • Document and communicate decisions and prepare for actions to support their implementation
12	Communicate to process owner	Provide documented recommendations for process owner review	• Data Manager	<ul style="list-style-type: none"> • Document outcomes, recommendations and decisions related to CPI for the DAT process • Meet with and review the outcomes with the process owner

13	DAT process owner defines way forward	Data Management Process Owner produces recommendations and actions to achieve the intended modifications and improvements for the process	<ul style="list-style-type: none"> • Process Owner 	<ul style="list-style-type: none"> • The process owner reviews all recommendations and provides direction on the course to achieve the intended results • Resources, funding and timelines are established • Process improvement project initiated
----	---------------------------------------	---	---	---

334

335 **16.1.8.1 CURRENT OPERATIONS POINTS OF CONTACT**

336

Process Acronym [DAT 8.0] Evaluate Data Management						
Assumptions:						
Constraints:						
Responsible Parties						
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
1-12	Data Manager	Logistics				
13	Data Process Owner	Logistics				

337

338 **16.1.8.2 DECISION TIMELINES**

339 A formal process reviews will occur at least annually however a review can occur any time the
 340 Data Manager or Process Owner determine there is a need or opportunity for improvement.

341

342 **16.1.8.3 TOOLS**

343 No tools are specifically identified to support the evaluate activities

344

345 **16.1.8.4 ROLES AND RESPONSIBILITIES**

346

347 The following table lists the roles and responsibilities for execution of this SOP.

348

Role	Responsibility
------	----------------

Data Manager	Oversees the actions and activities focused on CPI. The gathering, monitoring and evaluation of the process is a responsibility of the Data Manager.
Data Process Owner	Makes final decisions on the way forward and provided the required support for a successful outcome.

349

350 **16.1.8.5 R/A/C/I**

351 This following table contains a task-level RACI chart designating which of the above roles are
 352 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process

353 Activity task:

DAT 8	Contractor	Process Owner	Process Manager
Develop process evaluation plan	R	A	R
Collect feedback	A/R	C/I	R
Collect process measurements	A/R	C/I	R
Research trends and best practices	A/R	C/I	R
Assess process execution	A/R	C/I	R
Review existing documentation	A/R	C/I	R
Assess process framework	A/R	C/I	R
Evaluate data	A/R	C/I	R
Produce gap analysis	A/R	C/I	R
Identify improvement opportunities	A/R	C/I	R
Complete evaluation	A/R	C/I	R
Communicate to process owner	A/R	C/I	R
Data process owner defines way forward	A/R	C/I	R

354

355

356 **16.1.8.6 METRICS**

357 No metrics are specifically defined to measure the evaluation step in the process cycle.

358

Acronyms

Acronym	Description

Process Diagram Legend

Figure 5 provides the descriptions of the shapes used in the high level and detailed process diagrams.

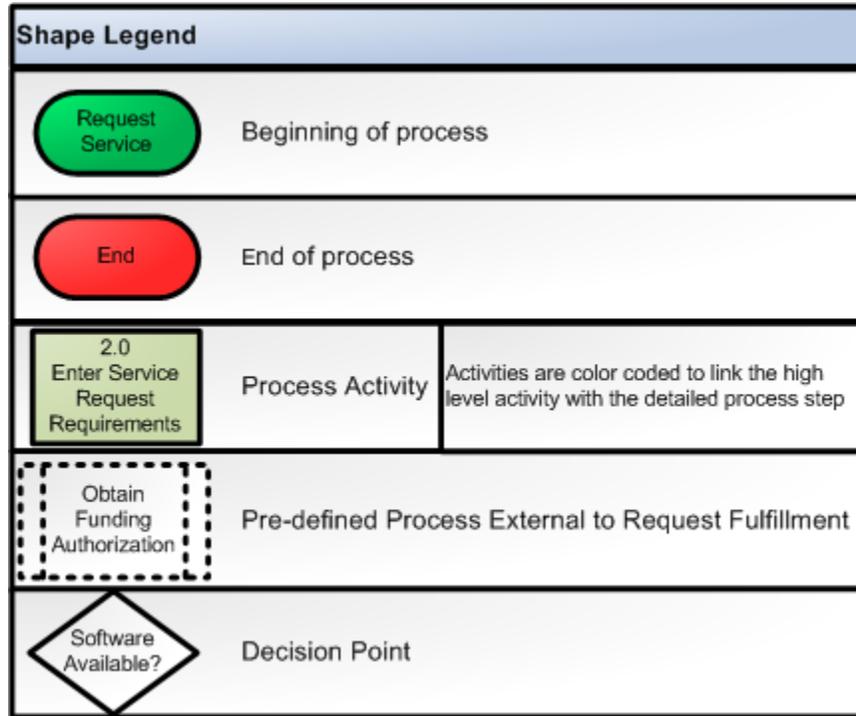


Figure 43: Diagram Legend

APPENDIX C – CONFIGURATION MANAGEMENT STANDARD OPERATING PROCEDURES



Configuration Management
Standard Operating Procedures
Version: 1.0

DATE: 08 March 2012
Program Executive Office Enterprise Information Systems
Program Manager, Next Generation Enterprise Network
1325 10th Street, SE, Suite 301
Washington, DC 20374

PREPARED

Gail Hoffman Configuration Management Process Owner Naval Enterprise Networks	Date
---	------

CONCURRENCE

Basam Hasan ITSM Lead Naval Enterprise Networks ,	Date
--	------

Dan Hickey Deputy Program Manager Naval Enterprise Networks	Date
---	------

APPROVED

Shawn P. Hendricks Captain, USN Program Manager Naval Enterprise Networks	Date
--	------

**Note: The signatures above certify this template has been approved for PMW 205 NGEN Program use. Once completed, this document and its contents are under the authority of the NGEN Process Owner, who is solely accountable for its stewardship, use, and maintenance.*

Table of Contents

1. Purpose.....1

2. Scope.....1

3. PROCESS ACTIVITIES Overview1

 3.1 Procedures2

 3.1.1 [CM-1] Establish Configuration Management Framework.....2

 3.1.2 [CM-2] Configuration Identification.....6

 3.1.3 [CM-3] Configuration Control.....10

 3.1.4 [CM-4] Configuration Status Accounting13

 3.1.5 [CM-5] Configuration Verification and Audit17

APPENDIX A: Acronyms.....1

APPENDIX B: Process Diagram Legend4

1 **17. PURPOSE**

2 This Standard Operating Procedure (SOP) is designed to provide for standard, repeatable, and
 3 measurable process for Configuration Management for government retained roles within the
 4 United States Navy (USN) Continuity of Services Contract (CoSC) environment in preparation
 5 for transitioning to the Next Generation Enterprise Network (NGEN).
 6

7 **Table 1-1 Authoritative Documents, References, Policies and Standards**

Domain	Document ID	Title
DoD	MIL-HDBK-61 A(SE)	Configuration Management Guide
DON	NAVSOP-3692	Independent Logistics Assessment (ILA) Handbook
DON	NMCI Contract N00024-00-D-6000	Attachment 9 Configuration Management
DoD	DoD Regulation 5000.02	Operation of the Defense Acquisition System

8
 9

10 **18. SCOPE**

11 The scope of this document includes the high level Configuration Management process activities
 12 performed by the current service provider-Hewlett Packard Enterprise Services (HP-ES) within
 13 the CoSC. Government touch points with HP-ES are identified within the configuration
 14 management activities. These touch points are interfaces between the Government and HP-ES
 15 operational staff and their partners which provide the Government with an increased level of
 16 Command and Control (C2). Tasks, metrics, work products, artifacts and tools that support each
 17 of the Government C2 touch points are identified if they are known. The information provided
 18 in this SOP was gathered from multiple C2 summit meetings with the HP-ES' Configuration
 19 Management Team. Additional information and details will be obtained from HP-ES during
 20 follow up C2 sessions and/or SME interactions/job shadowing. This SOP will be updated as new
 21 configuration management information is obtained.

22 This document provides process steps and tools used in supporting the CoSC Configuration
 23 Management interface (touch) points between the Government and the CoSC Service Provider
 24 (HP-ES). It documents the data exchanges between parties during the Configuration
 25 Management and other Information Technology Service Management (ITSM) processes.
 26

27 **19. PROCESS ACTIVITIES OVERVIEW**

28 In the current CoSC environment, Configuration Management activities are performed by HPES
 29 staff in their daily operational tasks. These Configuration Management tasks are identified as

30 part of the High Level process. Only Configuration Management related process activities and
31 touch points are identified within this document.

32
33 The following diagrams display the HPES high level process activities and the US Navy C2
34 touch points and the various tools used to support configuration management within CoSC.
35 Government C2 touch points are depicted by this diagram shape:

36 **19.1 Procedures**



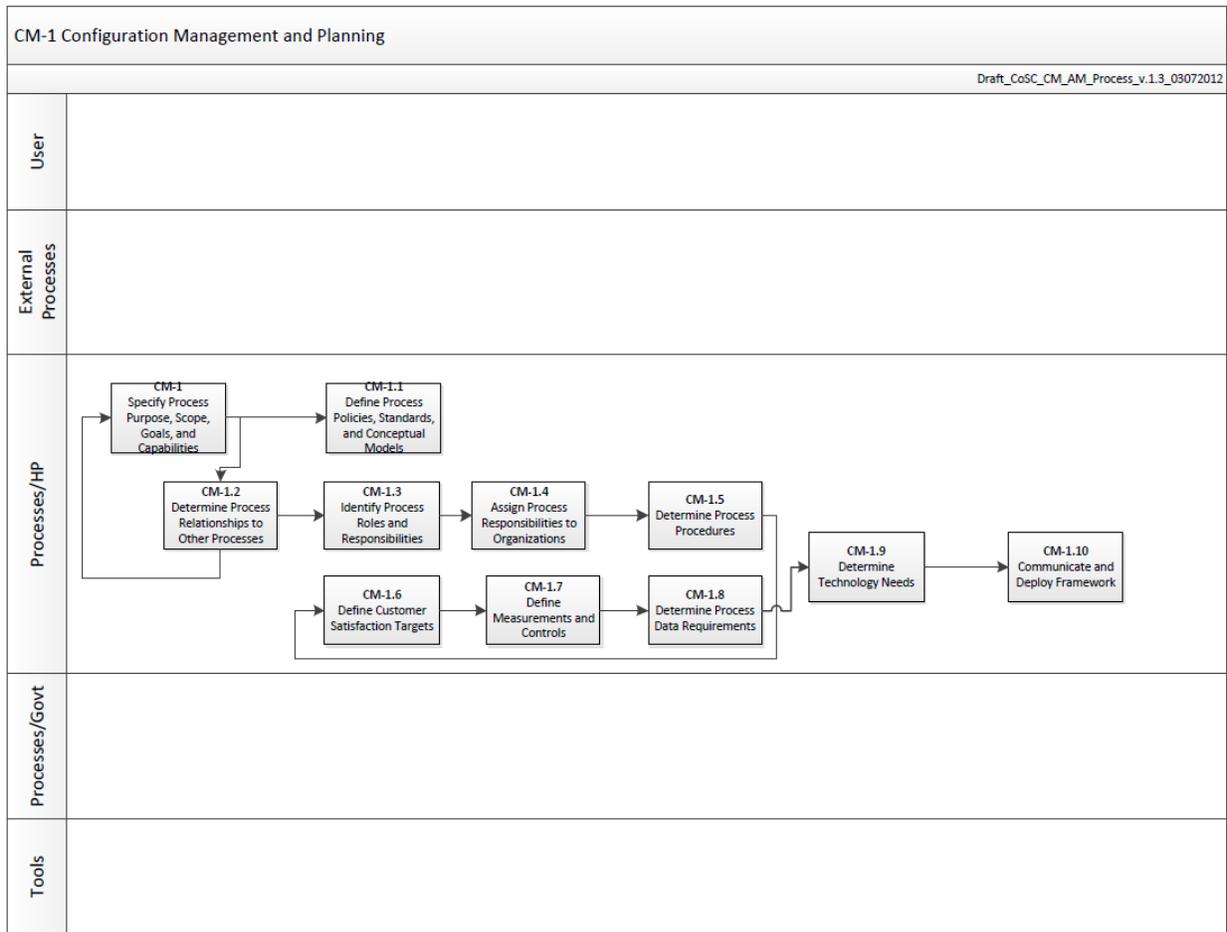
37 The following procedures provide a description of the tasks necessary to complete each
38 Configuration Management activity. A graphical representation of the tasks is provided followed
39 by a table containing additional details supporting the tasks.

40
41 **19.1.1 [CM-1] Establish Configuration Management Framework**

42 This activity defines all direction, guidance, policies, and procedures for how the process will be
43 performed. All of this is collectively referred to as the —process framework and is used as
44 reference information for all other CM activities. This information is reviewed in the Evaluate
45 Process Performance activity, which generates recommendations for making changes and
46 improvements to the process framework. The process framework is a collection of
47 information, not necessarily a single document, which includes:

- 48 • Specify CM purpose, scope, goals, and capabilities
- 49 • Define process policies, standards, and conceptual models
- 50 • Define process data requirements
- 51 • Identify roles and responsibilities
- 52 • Define relationships and interfaces with other processes
- 53 • Define measurements and controls
- 54 • Identify technology requirements
- 55 • Communicate and deploy the process framework
- 56 • Training requirements
- 57 • Do we need to call out Governance and/or Boards separately

58



59
60

1.0 CM_Establish_Process_Framework_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
21	Specify process purpose, scope, goals, and capabilities	Gather and document information from government and current contractor stakeholders	<ul style="list-style-type: none"> Contractor 	Defines the following: <ul style="list-style-type: none"> Purpose Scope Goals Capabilities
22	Define process policies, standards and conceptual models	Establish the standards required to achieve consistent, repeatable	<ul style="list-style-type: none"> Contractor 	<ul style="list-style-type: none"> Define standards that must exist Establish a concept model to validate and test standards, policies and

		practices across the enterprise		practices
23	Determine process data requirements	Define the data inputs and outputs related to the process and ensure they are properly addressed in the process	<ul style="list-style-type: none"> • Contractor 	<ul style="list-style-type: none"> • Identify inputs for each process activity • Identify outputs from process activities • Align inputs and outputs with processes and tools to ensure they are sufficiently addressed, owned and managed
24	Identify roles and responsibilities	Define the roles and their responsibilities that are required to achieve the process objectives	<ul style="list-style-type: none"> • Contractor 	<ul style="list-style-type: none"> • Define and document the process roles and their responsibilities
25	Define relationships and interfaces with other processes	Define the touch points and interfaces with other processes	<ul style="list-style-type: none"> • Contractor 	<ul style="list-style-type: none"> • Identify and document touch points • Identify and document interfaces with other processes • Identify and document tool touch points
26	Define measurements and controls	Determine and establish the controls, measurements and reports necessary to monitor the process	<ul style="list-style-type: none"> • Contractor 	<ul style="list-style-type: none"> • Define Critical Success Factors for the process • Identify Key Performance Indicators that can be measured • Define reports needed to monitor process performance
27	Identify technology requirements	Identify and document the process activities and the tool interfaces	<ul style="list-style-type: none"> • Contractor 	<ul style="list-style-type: none"> • Identify tools and their process activity touch points • Identify tool interfaces

28	Communicate and deploy the process framework	Prepare communications, training and other support for adoption of the process	<ul style="list-style-type: none"> • Contractor 	<ul style="list-style-type: none"> • Identify organizational impacts of the process • Identify training requirements • Define communication plan • Identify role touch points and need for support • Implement
-----------	--	--	--	---

61

62 **19.1.1.1 CURRENT OPERATIONS POINTS OF CONTACT**

63

Process Acronym [CM-1]Establish Configuration Management Framework						
Assumptions: Process Owner is accountable for the Configuration Management Process, but the process details are developed and implemented/monitored by the contractor.						
Constraints: Current process is defined and managed by the current contractor.						
Responsible Parties						
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
All steps in establishing the CM framework	Process Owner	SE&I				
All steps in establishing the CM framework	Contractor	HP-ES			CMS	

64

65 **19.1.1.2 DECISION TIMELINES**

66 Decision timelines have not been defined for this process activity. We hope to gain an
 67 understanding of this from HP CoSC.

68

69 **19.1.1.3 TOOLS**

70 The contractor’s Configuration Management System (CMS), which encompasses multiple
 71 Configuration Management Databases (CMDBs) and other related tools, is contained within this
 72 process activity. A specific tool (CMDB) has not been defined for this process activity.

73

74 **19.1.1.4 ROLES AND RESPONSIBILITIES**

75 The following table lists the roles and responsibilities for execution of this SOP for this process
 76 activity.

77

Role	Responsibility
Contractor	HP-ES operates and manages the Configuration Management activities on a daily basis. The current contractor develops and maintains their own Configuration Management Process framework.

78

79 **19.1.1.5 R/A/C/I**

80 This following table contains a task-level RACI chart designating which of the above roles are
 81 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process
 82 Activity task:

83

CM 1	Current Contractor	Government CM Process Owner	Government CM Process Manager
Specify process purpose, scope, goals and capabilities	RACI	I	I
Determine process relationships to other processes	RACI	I	I
Define process policies, standards and concept models	RACI	I	I
Identify process roles and responsibilities	RACI	I	I
Develop process and procedures	RACI	I	I
Define measurements and controls	RACI	I	I
Determine process data requirements	RACI	I	I
Identify tool requirements	RACI	I	I
Communicate and deploy framework	RACI	I	I

84

85 **19.1.1.6 METRICS**

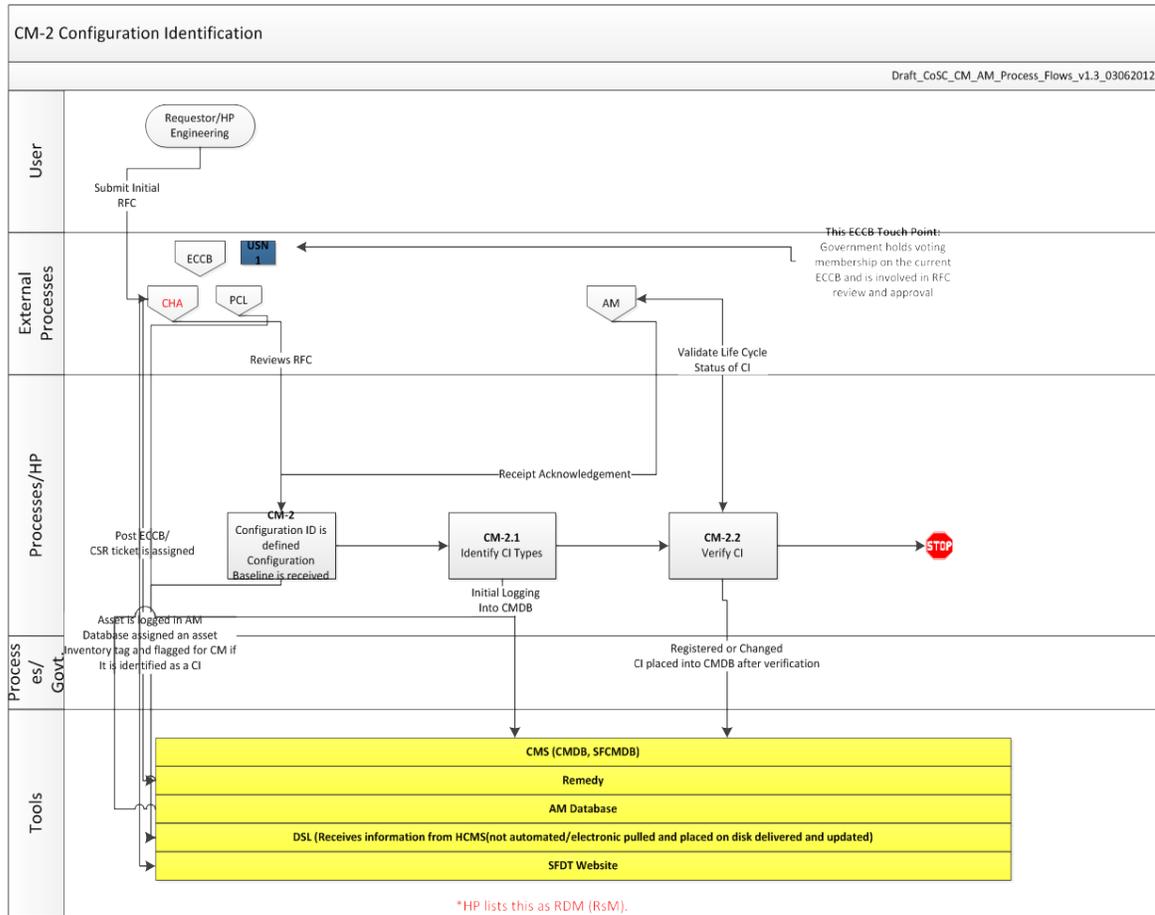
86 Metrics have not been defined for this process activity. We hope to gain this information from
 87 HP CoSC.

88

89

90 **19.1.2 [CM-2] Configuration Identification**

91 Configuration identification refers to the activities and processes dedicated to identifying and
 92 maintaining Configuration Items (CIs). The goal of configuration identification is to provide a
 93 unique identifier for each item to provide a way to track changes to that item and to understand
 94 its place in the system. Configuration identification may include processes such as item naming,
 95 drawing and document management, information management and base lining.
 96 In the diagram for this activity, note that the USN symbol indicates a touch point with the current
 97 contractor.
 98



99
 100
 101
 102
 103
 104
 105
 106
 107

Government C2 Touch Point (TP)

CM-2 ECCB Participation- The government has membership and voting rights on the CoSC Enterprise Change Control Board (ECCB) and can be involved in the Request for Change (Class I ECPs) review process. For the current state there is no Configuration Management representation on the ECCB, however, for the future state an Enterprise Configuration Control Board will be established and Configuration Management will have a presence on this board.

2.0 CM_Configuration_Identification_SOP_v1.0

Step	Process Model Task	Action	Role	Details
1	Define Configuration Items	Receive notification of new RFCs or Assets entered into CMDB, AM, DSL, or Remedy	<ul style="list-style-type: none"> Contractor 	<ul style="list-style-type: none"> Define Configuration Item (CI): RFC, Asset, Document, DSL Package (Software or Hardware), Baseline
2	Identify CI Type	Identify CI type and log into CMDB	<ul style="list-style-type: none"> Contractor 	<ul style="list-style-type: none"> Identify CI type assign CI tracking number
3	Verify CI	Verify changes to CI and package	<ul style="list-style-type: none"> Contractor 	<ul style="list-style-type: none"> Verify CI information and register in CMDB
4	ECCB	Review, approval or disapproval of changes	<ul style="list-style-type: none"> Contractor Government 	<ul style="list-style-type: none"> Review RFC's (Class I ECPs) and the government holds 3 voting memberships

108

109 **19.1.2.1 CURRENT OPERATIONS POINTS OF CONTACT**

110

Process Acronym [CM-2] Configuration Identification						
Assumptions: Contractor is accountable for the Configuration Identification Process.						
Constraints: CM processes are primarily developed and executed by the contractor. Government involvement in the development of standards has been limited to GPR IP/TDPP.						
Responsible Parties						
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
All steps in establishing the CM framework	Process Owner	SE&I			Homeport, IP Share	
All steps in establishing the CM framework	Contractor	HP-ES			CMS (CMDBs), Remedy, AM, DSL,SFDT Website	

111
 112
 113
 114
 115
 116
 117
 118
 119
 120
 121
 122
 123
 124
 125
 126
 127
 128

19.1.2.2 DECISION TIMELINES

Timelines have not been defined for this process activity. We hope to gain an understanding of these CoSC HP timelines.

19.1.2.3 TOOLS

The uCMDB is used to store all Configuration Items; post ECCB a ticket is created in Remedy for the approved Request for Change (RFC) after registration into Remedy the CM team is notified and the package information is placed under configuration control and placed into the Definitive Solution Library (DSL). Asset information is stored Asset Manager (AM) where the assets are logged and assigned an asset inventory tag, a notification is sent to the CM team when this asset is considered a CI. The DSL (Definitive Solution Library) holds all solution packages including documentation, software information, hardware information and baseline.

19.1.2.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP for this process activity.

Role	Responsibility
Contractor	HP-ES operates and manages the Configuration Management activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations

129
 130
 131
 132
 133
 134

19.1.2.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

CM 2	Current Contractor	Government CM Process Owner	Government CM Process Manager
Define Configuration Item	RACI	I	I
Identify CI Type	RACI		
Verify CI	RACI		

135

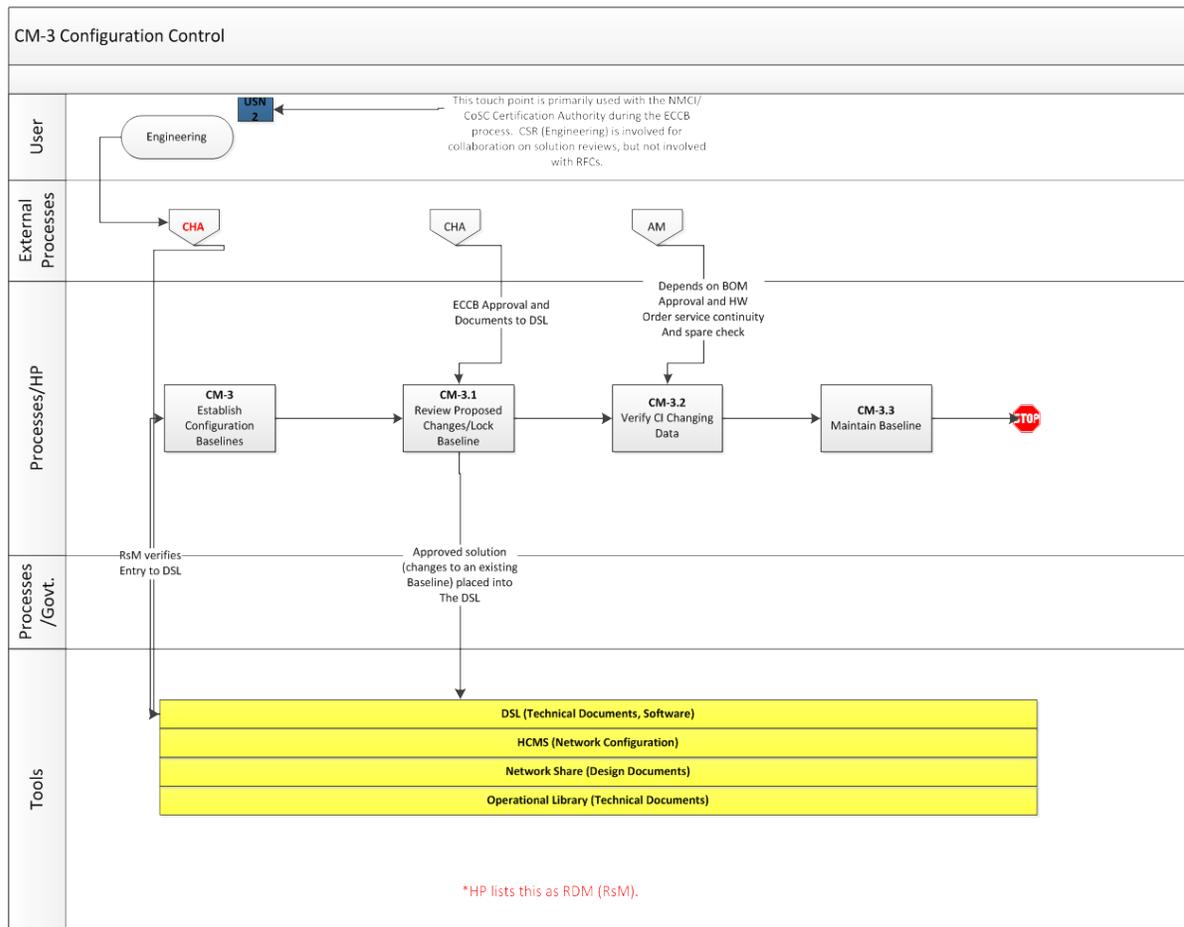
136 **19.1.2.6 METRICS**

137 The metrics for this process activity have not been defined. We hope to gain an understanding of
 138 the HP CoSC metrics for this process activity.

139
 140 **19.1.3 [CM-3] Configuration Control**

141 This activity involves control of authorized and identified Configuration Items (CIs) throughout
 142 the life-cycle. Requests for Change will contain detailed information on the proposed new
 143 baseline or solution including documentation and software.

144 In the diagram for this activity, note that the USN symbol indicates a touch point with the current
 145 contractor.



146
 147

148 **Government C2 Touch Points (TP)**

149 **CM-2 Engineering-** The government has membership and voting rights on the CoSC Enterprise
 150 Change Control Board (ECCB) and may be consulted during the CSR to collaborate on solution
 151 reviewsto include the Request for Change (Class I ECPs) review process. For the current state
 152 there is no Configuration Management representation on the ECCB, however, for the future state
 153 an Enterprise Configuration Control Board will be established and Configuration Management
 154 will have a presence on this board.

155

3.0 CM_Configuration_Control_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Establish Configuration Baselines	Gather information for changing baseline	<ul style="list-style-type: none"> Contractor 	<ul style="list-style-type: none"> Submit RFC to CSR and ECCB RFC is generated and placed into the DSL DSL sends notification to CM team of new entry
2	Maintain Baseline	Changes are made to the baseline	<ul style="list-style-type: none"> Government Contractor 	<ul style="list-style-type: none"> Changes are made to the baseline by Engineering CM places package information into DSL
3	Review Proposed Changes/Lock Baseline	Review package information	<ul style="list-style-type: none"> Contractor 	<ul style="list-style-type: none"> Change Management submits final documents to DSL CM is notified of package submitted into the DSL
4	Verify CI changing Data	Verify the CI package	<ul style="list-style-type: none"> Contractor 	<ul style="list-style-type: none"> CM verifies that the completion of the baseline package
5	ECCB	Review, approval or disapproval	<ul style="list-style-type: none"> Contractor Government 	<ul style="list-style-type: none"> Review RFC's (Class I ECPs) and the government holds 3 voting memberships

156

157 **19.1.3.1 CURRENT OPERATIONS POINTS OF CONTACT**

158

Process Acronym [CM-3]						
Assumptions: Contractor and their engineering are accountable for the Configuration Control Process. NMCI/CoSC government personnel hold voting membership on the ECCB.						
Constraints: CM processes and baseline information are primarily developed and executed by the contractor. Government may collaborate on solution reviews, but not involved with RFCs.						
Responsible Parties						
Process	Position	Org	Name	Contact Info	Tools	Tool

Point						Rqmts
All steps in establishing the CM framework	Process Owner	SE&I				
All steps in establishing the CM framework	Contractor	HP-ES			DSL, CMS(CMDB/CMDB Web Portal),AM, HCMS, Network Share	

159

160 **19.1.3.2 DECISION TIMELINES**

161 Decision timelines are currently not defined for this process activity. We hope to gain an
 162 understanding of the HP CoSC timelines for this process activity.

163

164 **19.1.3.3 TOOLS**

165 All CM baseline packages are submitted, reviewed and verified using the DSL. All asset items
 166 are submitted into Asset Manager (AM) and those assets that are identified as Configuration
 167 Items (CIs) are flagged and a notification is sent to the configuration management team. The
 168 Harris Configuration Management System (HCMS) is a tool used by HP-ES’ partner, Harris, for
 169 network configuration items. The Network Share contains all design documents.

170

171 **19.1.3.4 ROLES AND RESPONSIBILITIES**

172 The following table lists the roles and responsibilities for execution of this SOP for this process
 173 activity.

174

Role	Responsibility
Contractor	HP-ES operates and manages the Configuration Management activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations
Government	The government has membership and voting rights on the ECCB and may be consulted during CSR for solution development.
ECCB	Information Assurance (IA) has a representative participating in the ECCB. It is their responsibility to bring any impact or issues concerning IA to the ECCB meeting’s

	and boards attention.
--	-----------------------

175

176 **19.1.3.5 R/A/C/I**

177 This following table contains a task-level RACI chart designating which of the above roles are
 178 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process
 179 Activity task:

180

CM 3	Current Contractor	Government CM Process Owner	Government CM Process Manager
Establish Configuration Baselines	RACI	C/I	I
Review Proposed Changes/Lock Baseline	RACI	C/I	I
Verify CI Changing Data	RACI		
Maintain Baseline	RACI		

181

182 **19.1.3.6 METRICS**

183 Metrics for this process activity have not been defined. We hope to gain an understanding of the
 184 HP CoSC metrics for this process activity.

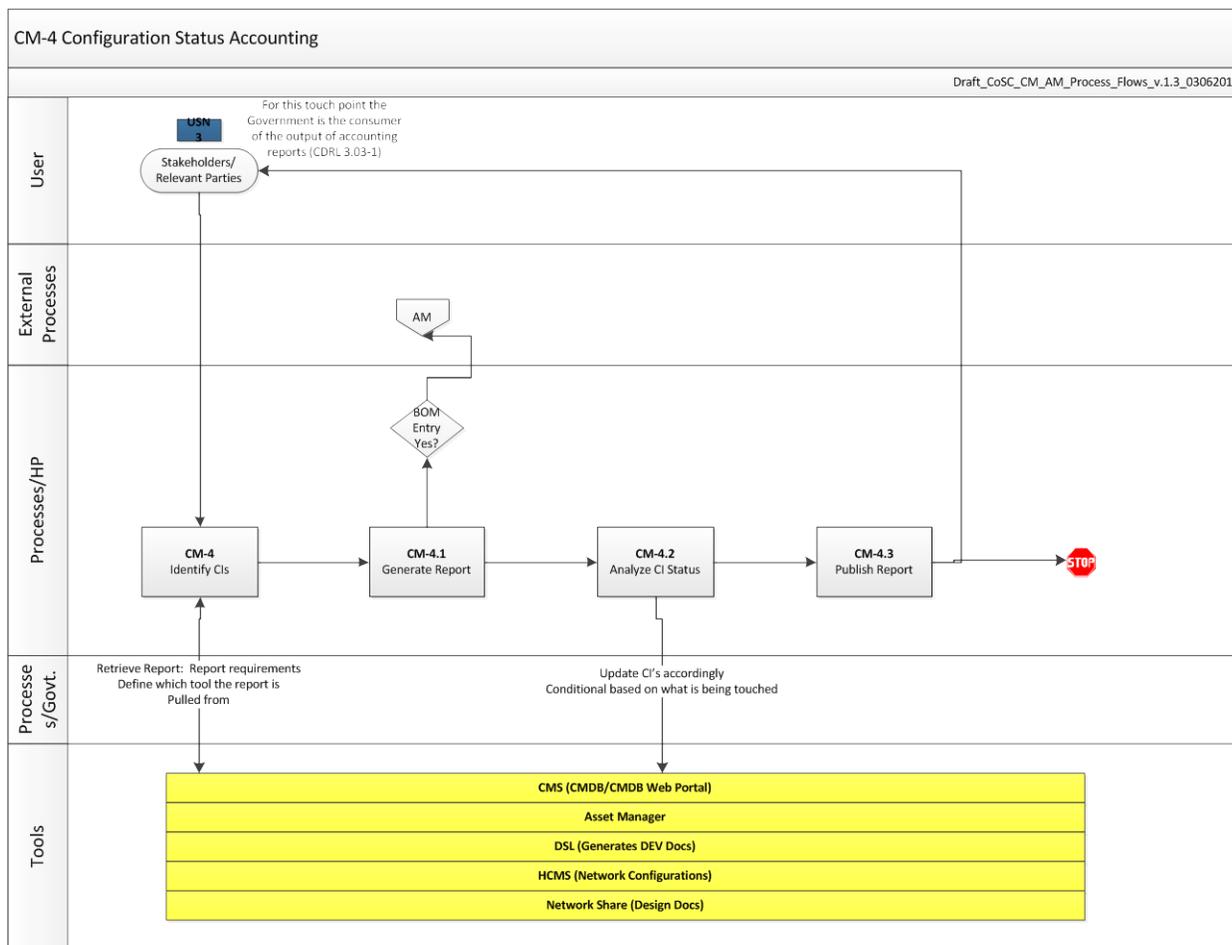
185

186 ***19.1.4 [CM-4] Configuration Status Accounting***

187 Configuration Status Accounting (CSA) is the process of ensuring that all of the relevant
 188 information about an item-documentation and change history- is up to date and as detailed as
 189 necessary. A primary goal of CSA is to repose CI information necessary to support existing and
 190 future change control efforts. A typical CSA system involves establishing and maintaining
 191 documentation for the entire life cycle of an object.

192 In the diagram for this activity, note that the USN symbol indicates a touch point with the current
 193 contractor.

194



195
 196
 197
 198
 199
 200
 201
 202
 203
 204
 205
 206
 207
 208
 209

Government C2 Touch Points (TP)

CM-3 Engineering- The government is the requestor and receives the published reports. The reports are received through CDRL 3.03-1, which contains changes to the configuration baseline. This should include the following:

- o Network architecture diagrams (both logical and physical)
- o Hardware description
- o Software version
- o System Configuration data (to include hardware device locations, software rules, ACLs, signatures, definitions, policies, protocol configurations, and scripts)
- o All systems and their currently scheduled Contractor end of support dates order to maintain state of the shelf capabilities
- o Network diagrams showing the placement of all network intrusion sensors

4.0 CM_Configuration_Status_Accounting_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Identify CI	Receive report request	• Contractor	<ul style="list-style-type: none"> • Receive request for report • Define report requirements • Determine tool to retrieve report
2	Generate Report	Gather data	• Contractor	<ul style="list-style-type: none"> • Retrieve data from appropriate tool
3	Analyze CI status	Review report information	• Contractor	<ul style="list-style-type: none"> • Update CIs based on report results in CMDB
4	Publish Report	Publish Report to Requestor	• Contractor	<ul style="list-style-type: none"> • Publish report to requestor (government) in form of CDRL 3-03.1
5	CDRL 3.3-1	Pull all requirements for CDRL	• Contractor	<ul style="list-style-type: none"> • Retrieve and publish report requirements for CDRL 3.3-1

210

211 **19.1.4.1 CURRENT OPERATIONS POINTS OF CONTACT**

212

Process Acronym [CM-4]						
Assumptions: Government is requestor of the report that is done through CDRL. The contractor controls the information and tools for the report.						
Constraints: Contractor controls input into tools that report is generated from.						
		Responsible Parties				
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
All steps in establishing the CM	Process Owner	SE&I				

framework						
All steps in establishing the CM framework	Contractor	HP- ES				CMS (CMDB/CMDB Portal), Asset Manager, DSL, HCMS, Network Share

213

214 **19.1.4.2 DECISION TIMELINES**

215 Decision timelines are currently not defined for this process activity. We hope to gain an
 216 understanding of the timelines from HP CoSC.

217

218 **19.1.4.3 TOOLS**

219 Report requirements define which tool the data will be collected from. The following tools are
 220 used for gathering report information: CMDB(s), Asset Manager, HCMS, DSL, and the
 221 Network Share. Reports once published are posted on the CMDB Web Portal for internal use by
 222 the contractor. Asset Manager is used to pull asset information that has been flagged as CIs.
 223 HCMS provides any updated network configuration information and the Network Share contains
 224 all design documents.

225

226 **19.1.4.4 ROLES AND RESPONSIBILITIES**

227 The following table lists the roles and responsibilities for execution of this SOP for this process
 228 activity.

229

Role	Responsibility
Contractor	HP-ES operates and manages the Configuration Management activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations

230

231 **19.1.4.5 R/A/C/I**

232 This following table contains a task-level RACI chart designating which of the above roles are
 233 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process
 234 Activity task:

235

CM 4	Current Contractor	Government CM Process Owner	Government CM Process Manager
Identify CIs	RACI		
Generate Report	RACI		
Analyze CI Status	RACI		
Publish Report	RACI	I	I

236

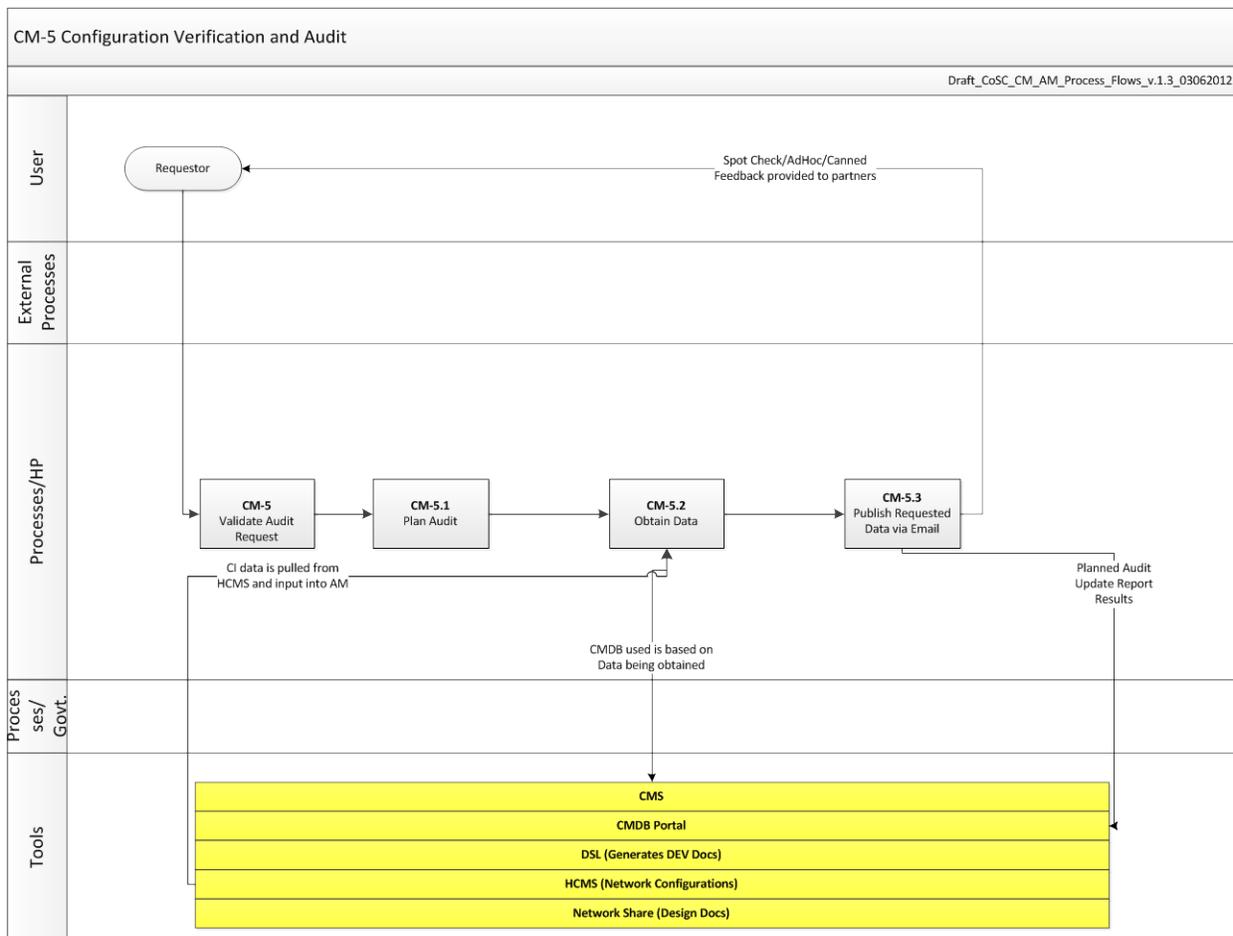
237 **19.1.4.6 METRICS**

238 Metrics for this process have not been defined for this process activity. We hope to gain an
 239 understanding of the metrics for this process activity from HP CoSC.

240

241 **19.1.5 [CM-5] Configuration Verification and Audit**

242 Configuration Verification and Audit is the process of analyzing configuration items and their
 243 respective documentation to ensure that the documentation reflects the current situation,
 244 essentially, configuration audits ensure that the change was appropriately carried out.



245

246

5.0 CM_Configuration_Verification and Audit_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Validate Audit Request	Validate Request for Audit	• Contractor	• Review audit request
2	Plan Audit	Gather requirements and plan for audit	• Contractor	• Define requirements for audit • Determine audit resources to include tools
3	Obtain Data	Gather data from resources for audit	• Contractor	• Gather data from resources • Analyze data • Verify data
4	Publish Requested Data	Publish audit results	• Contractor	• Publish audit results to requestor • Publish audit results to CMDB Portal

247

248 **19.1.5.1 CURRENT OPERATIONS POINTS OF CONTACT**

249

Process Acronym [CM-5]						
Assumptions: Contractor determines the parameters of audits (spot check, ad hoc, canned).						
Constraints: Contractor conducts all audits and sets parameters for what is to be and how it is to be audited.						
Responsible Parties						
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
All steps in establishing the CM framework	Process Owner	SE&I				
All steps in establishing the CM framework	Contractor	HP- ES			CMS, CMDB Portal, DSL, HCMS, Network	

					Share	
--	--	--	--	--	--------------	--

250

251 **19.1.5.2 DECISION TIMELINES**

252 Decision timelines have not been defined for this process activity. We hope to gain an
 253 understanding of the timelines for this process activity from HP CoSC.

254

255 **19.1.5.3 TOOLS**

256 Contractor pulls the information to be audited from different tools (may be partner tools). The
 257 data requirements determine which CMDB or tool the information is retrieved from. Once the
 258 information is retrieved, audited and verified the audit reports are sent to the requestor and
 259 published in the CMDB Portal. The DSL houses information on solution packages including
 260 software, hardware and baseline. The HCMS contains network configuration information; audits
 261 are performed by the partner (Harris) and provided to HP-ES. The Network Share contains all
 262 design document information.

263

264 **19.1.5.4 ROLES AND RESPONSIBILITIES**

265 The following table lists the roles and responsibilities for execution of this SOP for this process
 266 activity.

267

Role	Responsibility
Contractor	HP-ES operates and manages the Configuration Management activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations

268

269 **19.1.5.5 R/A/C/I**

270 This following table contains a task-level RACI chart designating which of the above roles are
 271 (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process
 272 Activity task:

273

CM 5	Current Contractor	Government CM Process Owner	Government CM Process Manager
Validate Audit Request	RACI		
Plan Audit	RACI		
Obtain Data	RACI		
Publish Requested Data	RACI	I	I

274

275 **19.1.5.6 METRICS**

276 Metrics for this process activity have not been defined. We hope to gain an understanding of the
277 metrics for this process activity from HP CoSC.

Acronyms

ACRONYM	DEFINITION
AMDB	Asset Management Database
AMIP	Asset Management Implementation Plan
AMP	Asset Management Plan
AMP	Availability Management Plan
AS	Acquisition Strategy
ASN-RDA	Office of the Assistant Secretary of the Navy (Research, Development and Acquisition)
ATO	Authority to Operate
BCP	Business Continuity Plan
C&A	Certification and Accreditation
C2	Command and Control
CAB	Change Advisory Board
CANES	Consolidated Afloat Networks and Enterprise Services
CBT	Computer-Based Training
CDRL	Contract Data Requirements List
CDS	Cross Domain Security
CI	Configuration Item
CLIN	Catalog Line Item Number
CMDB	Configuration Management Database
CMIS	Capacity Management Information System
CMP	Configuration Management Plan
CMS	Change Management System
CND	Computer Network Defense
CO/CO	Contractor Owned / Contractor Operated
COI	Communities of Interest
CONOPS	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial Off the Shelf
CYBERCOM	Fleet Cyber Command
DAA	Designated Accrediting Authority
DFS	Distributed File System
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DM	Decision Meeting
DMZ	Demilitarized Zone
DoD	Department of Defense
DON	Department of the Navy
DON CIO	Department of Navy Chief Information Officer
DR	Disaster Recovery
DV	Desktop Virtualization
ECCB	Engineering Change Control Board
ECP	Engineering Change Proposal
EDSS	Engineering Design and Support Services
EILT	Executive Integration Leadership Team
ES	Enterprise Services
ESDS	Electronic Software Delivery Services
ESL	Enterprise Software Licensing
EUHW	End-User Hardware

GFY	Government Fiscal Year
GIG	Global Information Grid
GNO	Global Network Operations
GO/CO	Government Owned / Contractor Operated
HDD	Hard Disk Drive
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alerts
IDE	Integrated Data Environment
IM/IT	Information Management / Information Technology
IPR	In Progress Review
ISOOA	Independent Security Operations Oversight and Assessment
IT-21	Information Technology for the 21st Century
LCAB	Local Change Advisory Board
MCEN	Marine Corps Enterprise Network
MD	Management Domain
NCMO	Navy Circuit Management Office
NCPDM	Navy CoSC Process Definition Model
NEN	Naval Enterprise Networks
NET	NMCI Enterprise Tool
NetOps	Network Operations
NNE	Naval Networking Enterprise
NNPDM	Navy NGEN Process Definition Model
NNWC	Naval Network Warfare Command
NSA	National Security Agency
NSA	National Security Agency
NSIB	NGEN Senior Integration Board
OCONUS	Outside the United States
OEM	Original Equipment Manufacturer
ONE-NET	OCONUS Navy Enterprise Network
QA	Quality Assurance
RAS	Remote Access Service
RFC	Requests for Change
RFP	Request for Proposal
RFQ	Request for Quote
ROM	Rough Order of Magnitude
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SECCONOPs	Security Concept of Operations
SEM	Security Event Management
SITREP	Situation Report
SLA	Service Level Agreement
SME PED	Secure Mobile Environment Portable Electronic Device
SRM	Supplier Relationship Management
SW	Software
TCB	Transition Control Board
TMP	Transition Management Plan
TRRB	Training Readiness Review Board
TXS	Transport Services
USMC	United States Marine Corps
USN	United States Navy

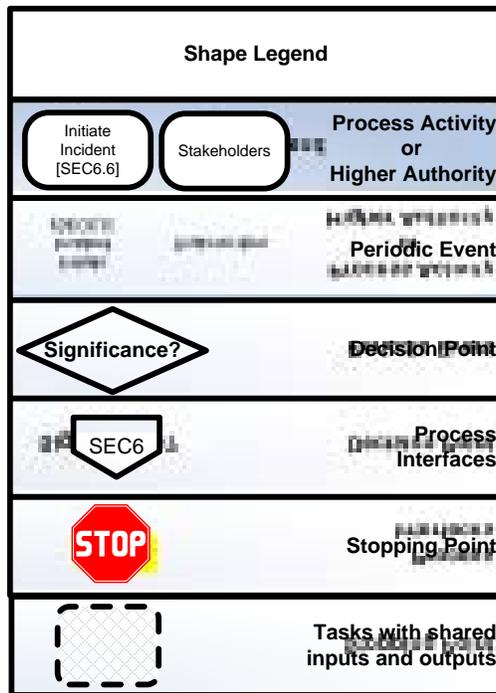
VTC	Video Teleconferencing
VV&R	Verification, Validation, and Reporting
WAN	Wide Area Network

Process Diagram Legend

The Process Activity diagrams in this document are created using a standardized Microsoft Visio template. The Process Activity Diagrams are developed in the form of a 'swim lane', which depicts sequential process tasks horizontally, with all of roles, functions, interfaces, data, and tools that interact with process activities listed vertically.

The Process Activity Diagram template is owned and maintained by the ITSM Architect and may be obtained with permission from the ITSM workspace on the PEO EIS portal.

The shape legend used to create the Process Activity Diagram is given below:



APPENDIX D – RELEASE AND DEPLOYMENT MANAGEMENT STANDARD OPERATING PROCEDURE



Release and Deployment Management
Standard Operating Procedures
Version: 1.0

DATE: 08 March 2012
Program Executive Office Enterprise Information Systems
Program Manager, Next Generation Enterprise Network
1325 10th Street, SE, Suite 301
Washington, DC 20374

PREPARED

Rajan Sharma Release and Deployment Management Process Owner Naval Enterprise Networks	Date
--	------

CONCURRENCE

Basam Hasan ITSM Lead Naval Enterprise Networks ,	Date
--	------

Dan Hickey Deputy Program Manager Naval Enterprise Networks	Date
---	------

APPROVED

Shawn P. Hendricks Captain, USN Program Manager Naval Enterprise Networks	Date
--	------

**Note: The signatures above certify this template has been approved for PMW 205 NGEN Program use. Once completed, this document and its contents are under the authority of the NGEN Process Owner, who is solely accountable for its stewardship, use, and maintenance.*

Table of Contents

1.	Purpose.....	1
2.	Scope.....	1
3.	PROCESS ACTIVITIES Overview	1
3.1	Procedures.....	1
3.1.1	[RDM1] Establish the Framework	1
3.1.2	[RDM 2] Develop Release and Deployment Plan	6
3.1.3	[RDM3] Design and Build Release.....	11
3.1.4	[RDM4] Test and Verify Release.....	16
3.1.5	[RDM5] Prepare Deployment Capabilities & Perform Transition Administration	19
3.1.6	[RDM6] Perform and Verify Deployment.....	24
3.1.7	[RDM7] Review and Close Deployment.....	28
3.1.8	[RDM8] Monitor, Manage and Report Release and Deployment	31
3.1.9	[RDM9] Evaluate Release and Deployment Management Performance	35
	APPENDIX A: Acronyms.....	1
	APPENDIX B: Process Diagram Legend	4

20. PURPOSE

This Standard Operating Procedure (SOP) is designed to provide for standard, repeatable, and measurable process for Release and Deployment Management (RDM) for government retained roles within the United States Navy (USN) Continuity of Services Contract (CoSC) environment in preparation for transitioning to the Next Generation Enterprise Network (NGEN).

Table 1-1 Authoritative Documents, References, Policies and Standards

Domain	Document ID	Title
TBD	TBD	TBD

21. SCOPE

This document describes the procedures implemented to support the government’s role in achieving command and control of the current CoSC Service Delivery contract. These procedures will define the roles and responsibilities of the Process Owner, Process Manager, and Release and Deployment Management personnel.

This document provides process steps and tools used in supporting the CoSC RDM interface (touch) points between the Government and the CoSC Service Provider (HP-ES). It documents the data exchanges between parties during the Release and Deployment Management and other Information Technology Service Management (ITSM) processes.

22. PROCESS ACTIVITIES OVERVIEW

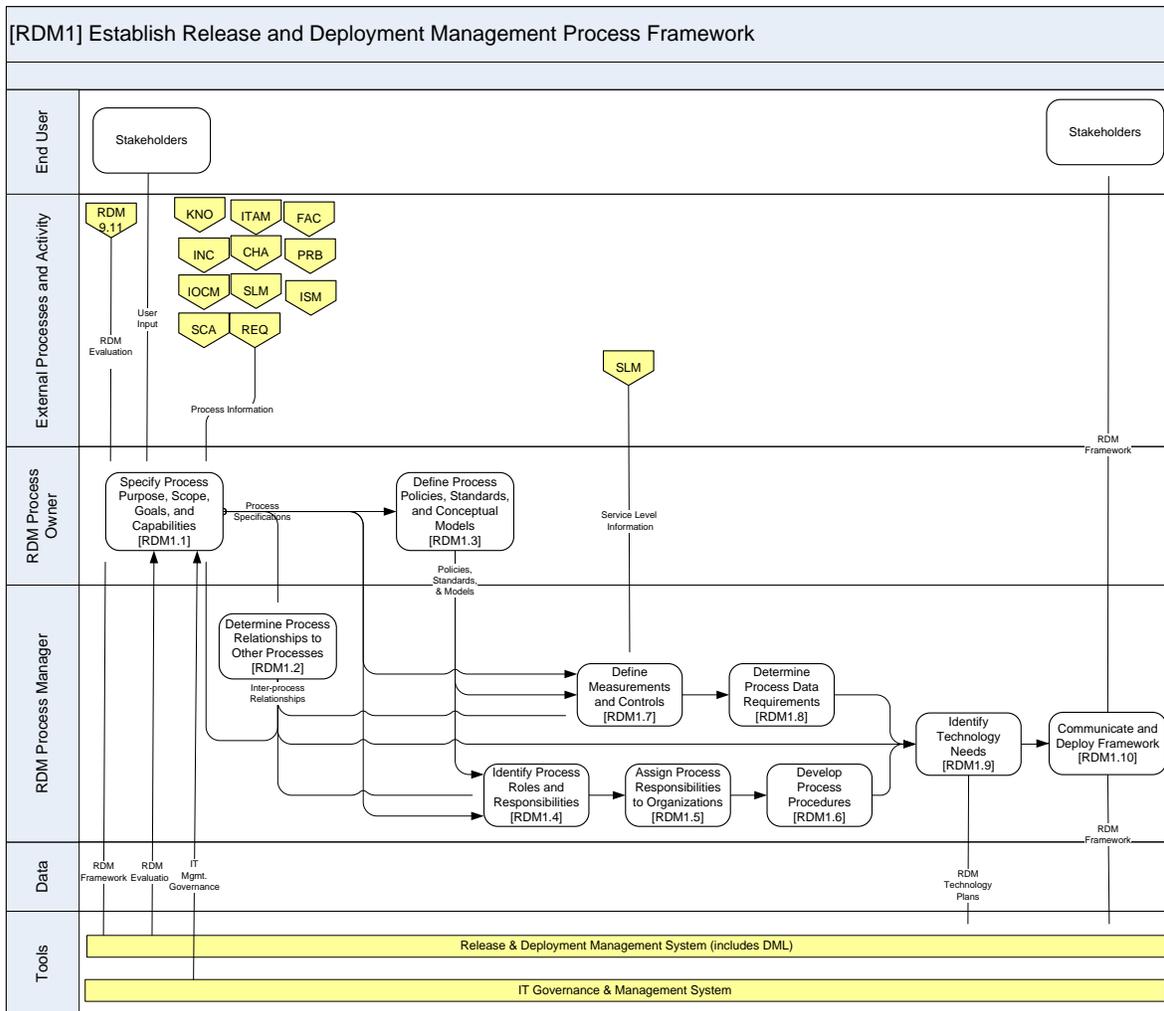
This section provides an overview of RDM activities.

22.1 Procedures

The following procedures provide a description of the tasks necessary to complete each RDM activity. A graphical representation of the tasks is provided followed by a table containing additional details supporting the tasks.

22.1.1 [RDM1] Establish the Framework

This activity defines all direction, guidance, policies, and procedures for how the RDM process will be performed taking direction from DON policies, Mission objectives and IT strategy. The RDM Management Process Framework defines the end-to-end approach of establishing the processes, procedures, roles, performance management capabilities and supporting tools needed to execute Release and Deployment Management.



1.0 RDM_Establish_Process_Framework_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
29	Specify process purpose, scope, goals and capabilities	Analyze existing process and document	RDM Process Owner	Capture the following information about the process: <ul style="list-style-type: none"> • Process flows • Tools • Metrics • Other

30	Determine process relationships to other processes	Develop process interface diagram	RDM Process Owner	<ul style="list-style-type: none"> • Process interface map detailing the nature of the interfaces (found in Process Framework document)
31	Define process policies, standards, and conceptual models	Research and gather all pertinent DOD policies	RDM Process Owner	<ul style="list-style-type: none"> • Reference all policies and store on Portal
32	Identify process rolls and responsibilities	Identify and document all pertinent rolls and responsibilities	RDM Process Owner	<ul style="list-style-type: none"> • Rolls and responsibilities document in Process Framework
33	Assign process responsibilities to organizations	Outline organizational construct	RDM Process Owner	<ul style="list-style-type: none"> • Align rolls with process activities • Align rolls with stakeholder responsibilities
34	Develop processes and procedures	Engage Contractor and stakeholders to define the process procedures	RDM Process Owner	<ul style="list-style-type: none"> • Document processes
35	Define measures and controls	Establish the controls, measurements and reports necessary to monitor process success	RDM Process Owner	<ul style="list-style-type: none"> • Define CSFs and KPIs • Define reports and other dashboard metrics needed
36	Determine process data requirements	Define the data inputs and outputs related to the process and ensure they are properly addressed in the process	RDM Process Owner	<ul style="list-style-type: none"> • Identify inputs and outputs for each process activity • Align inputs with processes and tools to ensure they are sufficiently addressed, owned and managed.

37	Identify technology needs	Identify and document the process activities that benefit from tool automation	RDM Process Owner	<ul style="list-style-type: none"> Identify opportunities where automation and tool capabilities deliver efficiencies or are required by the process Document functional tool requirements describing the required functionality
38	Communicate and deploy the process framework	Prepare communications training and other engagement to support widespread adoption of the process	RDM Process Owner	<ul style="list-style-type: none"> Identify organizational impacts of the process Identify training requirements Define communication plan Identify role touch points and need for support Implement

22.1.1.1 CURRENT OPERATIONS POINTS OF CONTACT

[RDM1] Establish Data Management Framework						
Assumptions: Process Owner is accountable for the RDM process but the process details will be developed primarily by the contractor and approved by the Government. The Government gathers its requirements and injects them into the process through collaboration with the contractor						
Constraints: Government approved RACI						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
All steps in establishing the RDM framework	RDM Process Owner	PMW 205 Engineering			TBD	Change Ticket System Management
All steps in establishing the RDM framework	RDM Manager	SPAWAR			TBD	Change Ticket Management System
All steps in establishing the RDM framework	RDM Analysts and Operators	PMW 205 and NNWC			TBD	TBD
All steps in establishing the RDM framework	RDM Administrators and Operators	Contractor			TND	TBD

22.1.1.2 DECISION TIMELINES

Discussed in regular meetings between Contractor and the Government RDM Process Owner, Manager, and stakeholders. These meeting include but are not limited to CAB, ECCB, Maintenance, PIR and others.

22.1.1.3 TOOLS

No specific tools are identified for developing the outcomes of [RDM 1].

22.1.1.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
RDM Process Owner	The RDM Process Owner is accountable for ensuring the process is Fit for Purpose. The Process Owner is the sponsor of the process, and holds the responsibility and executive authority for the overall process results across the enterprise. This authority spans across all internal and external organizations that participate in the process. Specifically the Process Owner is responsible for design, execution and continual improvement of the process. The individual filling this role ensures that the process is being carried out, but does not run the day-to-day operation of the process. The Process Owner receives regular updates concerning the performance of the process and represents this process concerning all decisions.
RDM Process Manager	The RDM Process Manager is responsible for operational management of the process, including coordination across processes, and is responsible for the overall quality of the process. The Process Manager is the main coordinator within the process. The Process Manager is responsible for all aspects of the day-to-day operational management of the process, including planning and coordinating all the activities required to perform, monitor, and report on the process. The Process Manager enables communication of preventative actions and best practices to improve service levels. The Process Manager may delegate authority to other process resources. However, the Process Manager is the single authority and point of responsibility for all issues relating to the operational command and control of the process across the enterprise.
Contractor	The Contractor operates and manages RDM activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations

Other Process Owners and Stakeholders	Process owners and Stakeholders of other ITSM or business processes that have a dependency or integration point with the RDM process
---------------------------------------	--

22.1.1.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

RDM 1	RDM Process Owner	RDM Process Manager	Other Process Owners	Contractor
Specify process purpose, scope, goals and capabilities	A/R	R	C/I	C
Determine process relationships to other processes	A/R	R	C/I	C
Define process policies, standards, and conceptual models	A/C	C	C/I	C
Identify process rolls and responsibilities	A/C	C	C/I	C
Assign process responsibilities to organizations	A/R	R	C/I	C
Develop processes and procedures	A/R	R	C/I	C
Define measures and controls	A/C	C	C/I	C
Determine process data requirements	A/R	R	C/I	C
Identify technology needs	A/R	R	C/I	C
Communicate and deploy the process framework	A/R	R	C/I	C

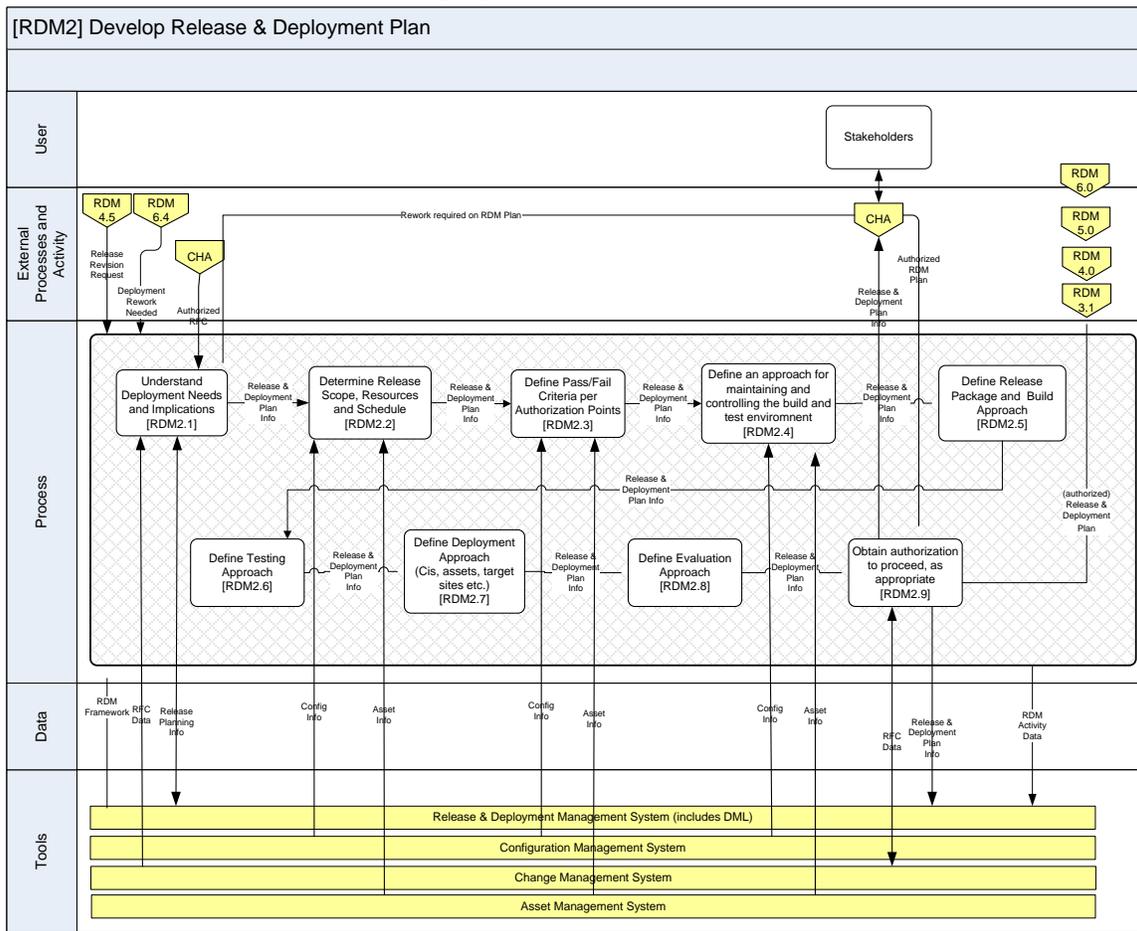
22.1.1.6 METRICS

No metrics are identified to measure performance of the RDM Framework

22.1.2 [RDM 2] Develop Release and Deployment Plan

This activity determines the approach for how each release is prepared and the type of deployment. The release planning covers the approach for building, testing and verifying the

release, including the possible need for pilot deployments, as well as establishing a model for how the finalized release should be deployed.



2.0 RDM_Develop_Release and Deployment_Plan_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Understand Deployment Needs and Implications	Contractor Owned	• Contractor	• Contractor Owned
2	Determine release scope, resources and schedule	Contractor Owned	• Contractor	• Contractor Owned

3	Define pass/fail criteria per authorization points	Contractor Owned	• Contractor	• Contractor Owned
4	Define an approach for maintaining and controlling the build and test environment	Contractor Owned	• Contractor	• Contractor Owned
5	Define release package and build approach	Contractor Owned	• Contractor	• Contractor Owned
6	Define testing approach	Contractor Owned	• Contractor	• Contractor Owned
7	Define deployment approach (CIs, assets, target sites, etc)	Contractor Owned	• Contractor	• Contractor Owned
8	Define evaluation approach	Contractor Owned	• Contractor	• Contractor Owned
9	Obtain authorization, as appropriate	If ECCB or CAB determine that authorization is they will obtain at this step	• RDM Process Owner and Manager	• ECCB • CAB

22.1.2.1 CURRENT OPERATIONS POINTS OF CONTACT

[RDM2] Develop Release and Deployment Plan
Assumptions: The government will only have a touch point in this step if the CAB or ECCB deems that

authorization to proceed with a change is required by an external organization.						
Constraints: None known at this time						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
RDM 2.9, Obtain authorization to proceed as appropriate	RDM Process Owner	PMW 205 Engineering			TBD	Change Ticket System Management
RDM 2.9, Obtain authorization to proceed as appropriate	RDM Manager	SPAWAR			TBD	Change Ticket Management System
RDM 2.9, Obtain authorization to proceed as appropriate	RDM Analysts and Operators	PMW 205 and NNWC			TBD	TBD
RDM 2.9, Obtain authorization to proceed as appropriate	RDM Administrators and Operators	Contractor			TND	TBD

22.1.2.2 DECISION TIMELINES

TBD

22.1.2.3 TOOLS

Remedy and SM7 are currently used

22.1.2.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
RDM Process Owner	The RDM Process Owner is accountable for ensuring the process is Fit for Purpose. For more detail see Section 3.1.1.4
RDM Process Manager	The RDM Process Manager is responsible for operational management of the process, including coordination across processes, and is responsible for the overall quality of the process. For more detail see Section 3.1.1.4

Contractor	The Contractor operates and manages RDM activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations
Other Process Owners and Stakeholders	Process owners and Stakeholders of other ITSM or business processes that have a dependency or integration point with the RDM process

22.1.2.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

RDM 2	RDM Process Owner	RDM Process Manager	Other Process Owners	Contractor
Understand Deployment Needs and Implications	R	C	I	A/R
Determine release scope, resources and schedule	R	C	I	A/R
Define pass/fail criteria per authorization points	R	C	I	A/R
Define an approach for maintaining and controlling the build and test environment	R	C	I	A/R
Define release package and build approach	R	C	I	A/R
Define testing approach	R	C	I	A/R
Define deployment approach (CIs, assets, target sites, etc)	R	C	I	A/R
Define evaluation approach	R	C	I	A/R
Obtain authorization, as appropriate	A	R	I	C

22.1.2.6 METRICS

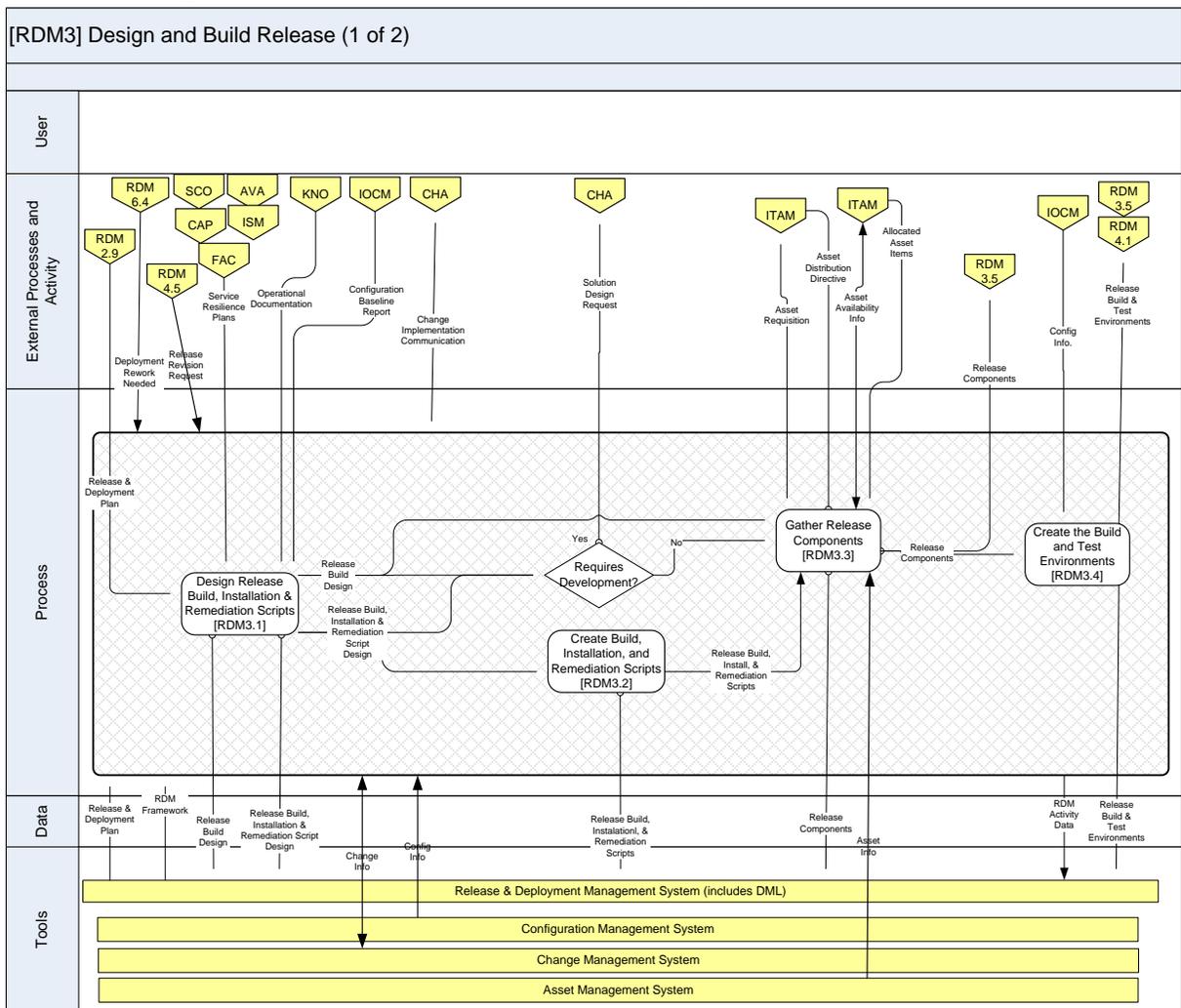
The following metrics will be captured for RDM Develop Release and Deployment Plan.

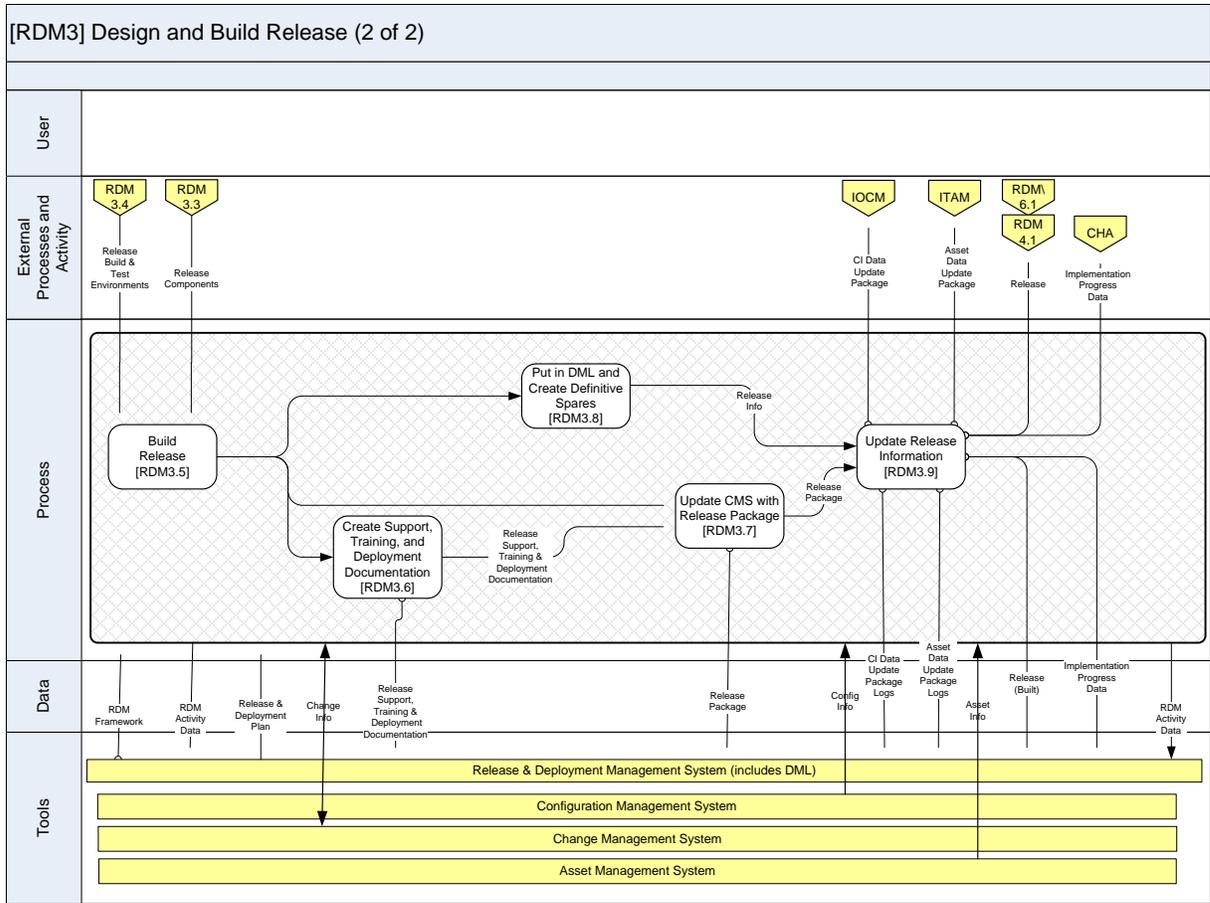
Metric: Total Releases in the pipeline

Description	Total releases in pipeline
Relevance	Assess if system is operating effectively or overtaxed and too slow
Target Values	TBD
Calculation	Total number of releases approved but not yet deployed
Notes	None

22.1.3 [RDM3] Design and Build Release

This activity determines what needs to be built for the release and how it will be assembled and deployed. Release build, installation, and rollback scripts are designed at a high level. Software and hardware components are obtained for the build activity and the test environment is created.





3.0 RDM_Design and Build_Release_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Design release build, installation & remediation scripts	Contractor owned and performed	• Contractor	• Reserved
2	Create build, installation, and remediation scripts	Contractor owned and performed	• Contractor	• Reserved

3	Gather release components	Contractor owned and performed	• Contractor	• Reserved
4	Create the build and test environments	Contractor owned and performed	• Contractor	• Reserved
5	Build release	Contractor owned and performed	• Contractor	• Reserved
6	Create support training and deployment documentation	Contractor owned and performed	• Contractor	• Reserved
7	Update CMS with release package	Contractor owned and performed	• Contractor	• Reserved
8	Put in DML and create definitive spares	Contractor owned and performed	• Contractor	• Reserved
9	Update release information	Contractor owned and performed	• Contractor	• Reserved

22.1.3.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym RDM3	
Assumptions: All aspects of this step shall be owned and performed by contractor	
Constraints: Nothing to report at this time	
	Responsible Parties

Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
All steps in design and Build release	Contractor	Contractor			Contractor owned	TBD

22.1.3.2 DECISION TIMELINES

Reserved

22.1.3.3 TOOLS

The tools for these process steps shall be determined by contractor

22.1.3.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
RDM Process Owner	N/A
RDM Process Manager	N/A
Contractor	The Contractor operates and manages all RDM3 activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operation
Other Process Owners and Stakeholders	N/A

22.1.3.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

RDM 3	RDM Process Owner	RDM Process Manager	Other Process Owners	Contractor
Design release build, installation & remediation scripts	C	C	C	A/R

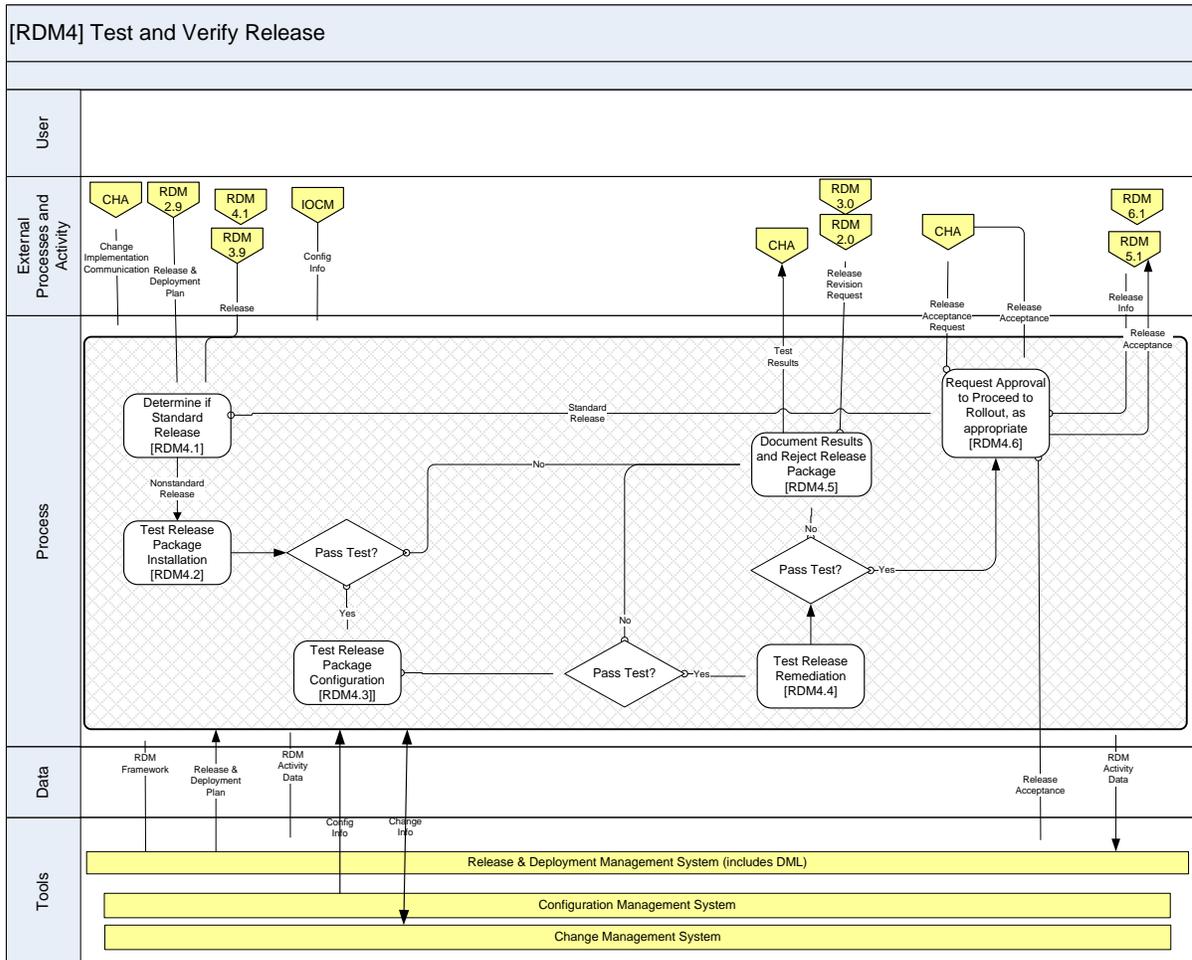
Create build, installation, and remediation scripts	C	C	C	A/R
Gather release components	C	C	C	A/R
Create the build and test environments	C	C	C	A/R
Build release	C	C	C	A/R
Create support training and deployment documentation	C	C	C	A/R
Update CMS with release package	C	C	C	A/R
Put in DML and create definitive spares	C	C	C	A/R
Update release information	C	C	C	A/R
	C	C	C	A/R

22.1.3.6 METRICS

There are no metrics discussed for this step at this time

22.1.4 [RDM4] Test and Verify Release

This activity tests the built Release Package to determine if installation, configuration, and rollback work properly.



4.0 RDM_Test and Verify_Release_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Determine if standard release	Contractor owned and performed	• Contractor	• Reserved
2	Test and release package installation	Contractor owned and performed	• Contractor	• Reserved

3	Test release package configuration	Contractor owned and performed	• Contractor	• Reserved
4	Test release remediation	Contractor owned and performed	• Contractor	• Reserved
5	Document results and reject release package	Contractor owned and performed	• Contractor	• Reserved
6	Request approval to proceed to rollout, as appropriate	NETOPS must approve release at this point	• NETOPS	• NETOPS approves release as appropriate and issues required User Communications that release is scheduled

22.1.4.1 CURRENT OPERATIONS POINTS OF CONTACT

RDM4						
Assumptions: None at this time						
Constraints: None known at this time						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
Request approval to proceed to rollout, as appropriate	RDM Process Owner	PMW 205 Engineering			TBD	Change Ticket System Management
Request approval to proceed to rollout, as	RDM Manager	SPAWAR			TBD	Change Ticket Management System
Request approval to proceed to rollout, as	RDM Analysts and Operators	PMW 205 and NNWC			TBD	TBD

Request approval to proceed to rollout, as	RDM Administrators and Operators	Contractor			TND	TBD
---	---	-------------------	--	--	------------	------------

22.1.4.2 DECISION TIMELINES

Reserved

22.1.4.3 TOOLS

Remedy and SM7 currently being used

22.1.4.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
RDM Process Owner	The RDM Process Owner is accountable for ensuring the process is Fit for Purpose. For more detail see Section 3.1.1.4
RDM Process Manager	The RDM Process Manager is responsible for operational management of the process, including coordination across processes, and is responsible for the overall quality of the process. For more detail see Section 3.1.1.4
Contractor	The Contractor operates and manages RDM activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations
Other Process Owners and Stakeholders	Process owners and Stakeholders of other ITSM or business processes that have a dependency or integration point with the RDM process

22.1.4.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

RDM 4	RDM Process Owner	RDM Process Manager	Other Process Owners	Contractor
Determine if standard release	R	C	I	A
Test and release package	R	C	I	A

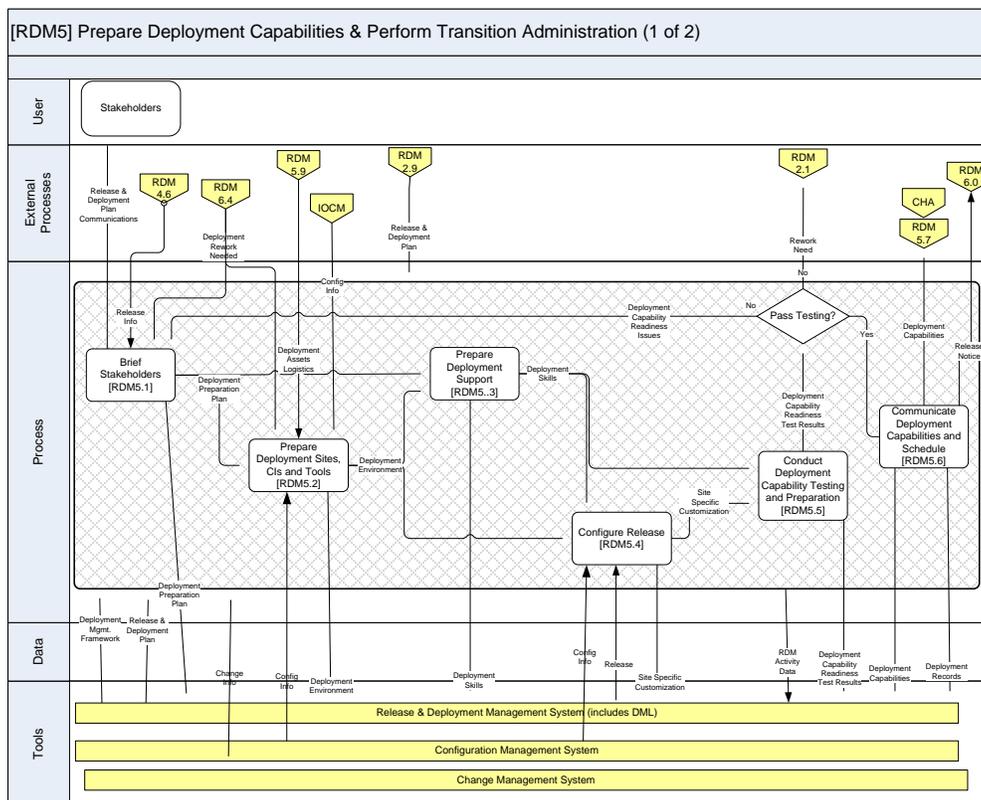
installation				
Test release package configuration	R	C	I	A
Test release remediation	R	C	I	A
Document results and reject release package	R	C	I	A
Request approval to proceed to rollout, as appropriate	A	R	C	I

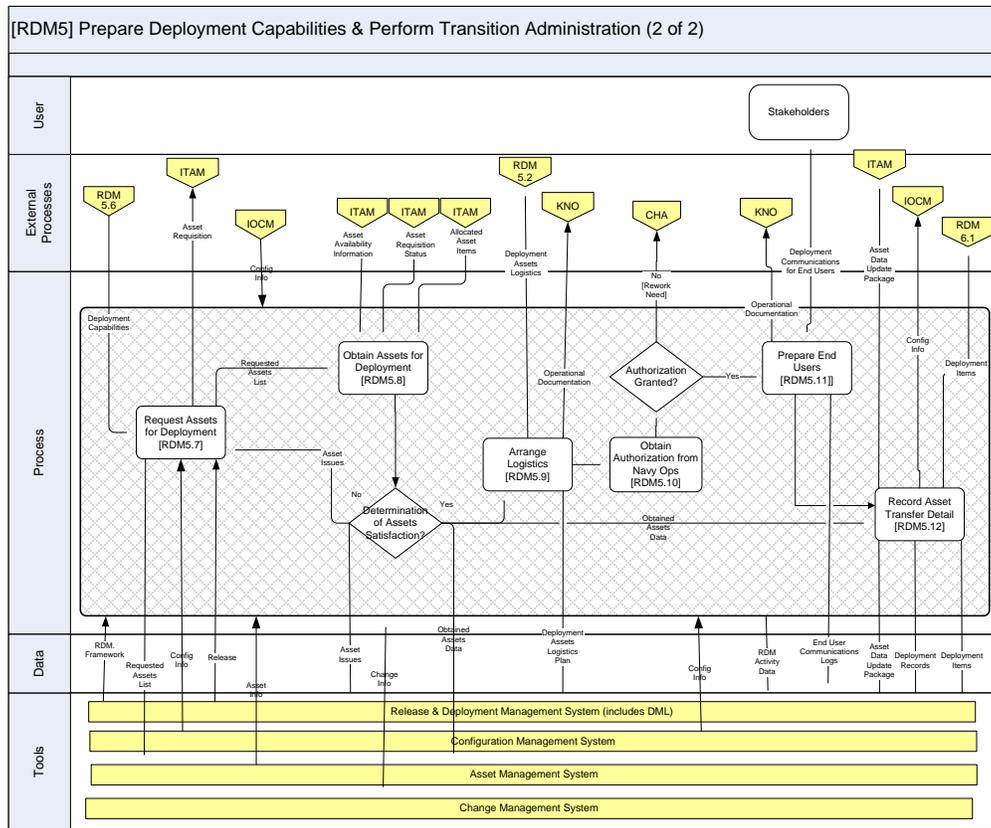
22.1.4.6 METRICS

The metrics to be captured for RDM4 have not yet been determined. They will probably be contractor internal.

22.1.5 [RDM5] Prepare Deployment Capabilities & Perform Transition Administration

In this activity, the deployment capabilities for each deployment are prepared.





5.0 RDM_Prepare_Deployment Capabilities and Perform Transition Administration_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Brief shareholders	Contractor owned and performed	• Contractor	• Reserved
2	Prepare deployment sites, CIs and tools	Contractor owned and performed	• Contractor	• Reserved
3	Prepare deployment support	Contractor owned and performed	• Contractor	• Reserved

4	Configure release	Contractor owned and performed	• Contractor	• Reserved
5	Conduct deployment capability testing and preparation	Contractor owned and performed	• Contractor	• Reserved
6	Communicate deployment capabilities and schedule	Contractor owned and performed	• Contractor	• Reserved
7	Request assets for deployment	Contractor owned and performed	• Contractor	• Reserved
8	Obtain assets for deployment	Contractor owned and performed	• Contractor	• Reserved
9	Arrange logistics	Contractor owned and performed	• Contractor	• Reserved
10	Obtain authorization from Navy Ops	The CAB presents RFCs for new solution with recommendation for what Navy Ops needs to be consulted	• NETOPS	• NETOPS obtains authorization from designated Navy Ops to do change.
11	Prepare end users	Contractor owned and performed	• Contractor	• Reserved

12	Record asset transfer detail	Contractor owned and performed	• Contractor	• Reserved
-----------	------------------------------	--------------------------------	--------------	------------

22.1.5.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym RDM5						
Assumptions: None at this time						
Constraints: None known at this time						
Responsible Parties						
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
Obtain authorization from Navy Ops	Position	Org	Name	Contact Info	Tools	Tool Rqmts
Obtain authorization from Navy Ops	RDM Process Owner	PMW 205 Engineering			TBD	Change Ticket System Management
Obtain authorization from Navy Ops	RDM Manager	SPAWAR			TBD	Change Ticket Management System
Obtain authorization from Navy Ops	RDM Analysts and Operators	PMW 205 and NNWC			TBD	TBD

22.1.5.2 DECISION TIMELINES

Reserved

22.1.5.3 TOOLS

Remedy and SM7 are currently used for processing the User Communications.

22.1.5.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
RDM Process Owner	The RDM Process Owner is accountable for ensuring the process is Fit for Purpose. For more detail see Section 3.1.1.4
RDM Process Manager	The RDM Process Manager is responsible for operational management of the process, including coordination across processes, and is responsible for the overall quality of the process. For more detail see Section 3.1.1.4
Contractor	The Contractor operates and manages RDM activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations
Other Process Owners and Stakeholders	Process owners and Stakeholders of other ITSM or business processes that have a dependency or integration point with the RDM process

22.1.5.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

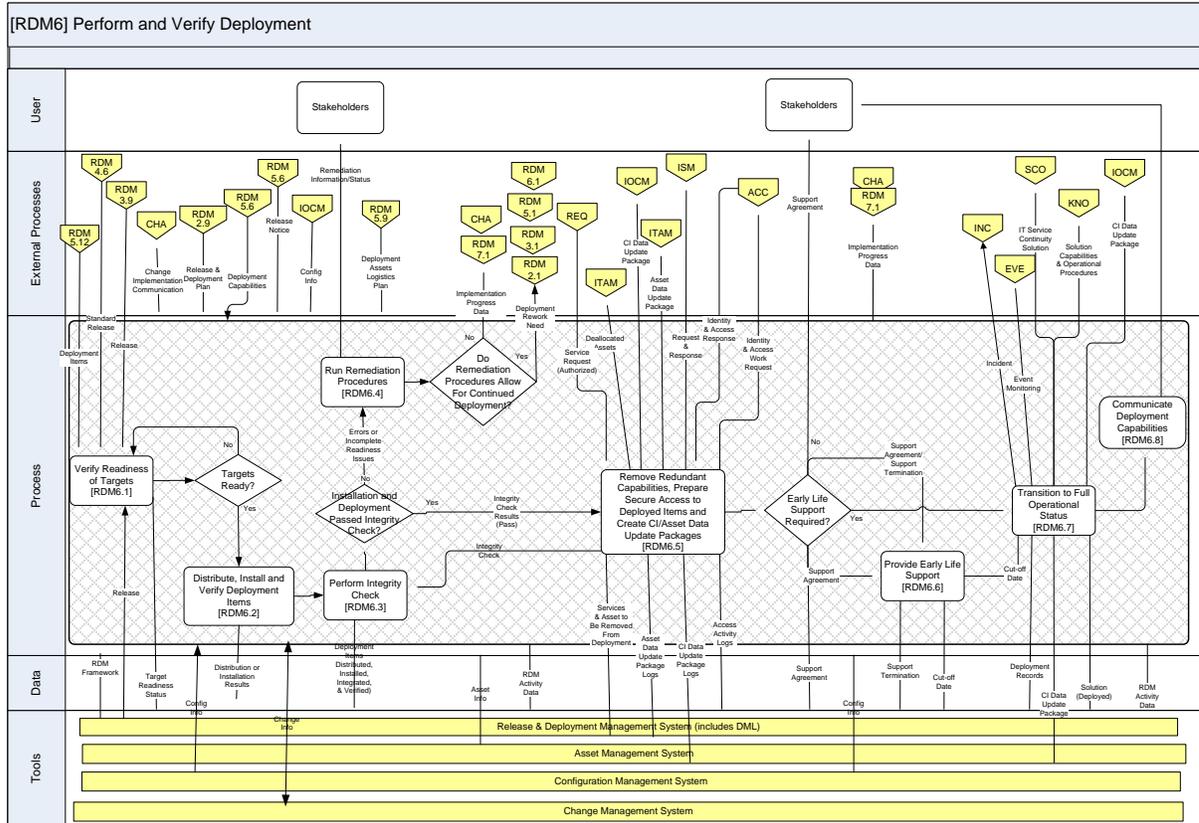
RDM 5	RDM Process Owner	RDM Process Manager	Other Process Owners	Contractor
Brief shareholders	R	C	I	A
Prepare deployment sites, CIs and tools	R	C	I	A
Prepare deployment support	R	C	I	A
Configure release	R	C	I	A
Conduct deployment capability testing and preparation	R	C	I	A
Communicate deployment capabilities and schedule	R	C	I	A
Request assets for deployment	R	C	I	A
Obtain assets for deployment	R	C	I	A
Arrange logistics	R	C	I	A
Obtain authorization from Navy Ops	A	R	I	C
Prepare end users	R	C	I	A
Record asset transfer detail	R	C	I	A

22.1.5.6 METRICS

The following metrics to be captured for RDM5 will be contractor internal and have not been determined yet.

22.1.6 [RDM6] Perform and Verify Deployment

This activity executes all tasks necessary to complete the actual deployment. In this activity, the capability status would move from “Not Deployed” to “Deployed”.



6.0 RDM_Perform and Verify_Deployment_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Verify readiness of targets	Contractor owned and performed	• Contractor	• Reserved

2	Distribute, install and verify deployment items	Contractor owned and performed	• Contractor	• Reserved
3	Perform integrity check	Contractor owned and performed	• Contractor	• Reserved
4	Run remediation procedures	Remediation procedures are ran to assess effectiveness of back out	NETOPS	• Remediation notifications are issued when back plan out has been tested and verified
5	Remove redundant capabilities, prepare secure access to deployed items and create CI/Asset data update packages	Contractor owned and performed	• Contractor	• Reserved
6	Provide early life support	Contractor owned and performed	• Contractor	• Reserved
7	Transition to full operational status	Contractor owned and performed	• Contractor	• Reserved
8	Communicate deployment capabilities	Deployment capability USER Communications drafted, approved, and issued	• NETOPS	• NETOPS issues a USER Communications stating what capabilities the new Release shall have

22.1.6.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym RDM6						
Assumptions: None at this time						
Constraints: None known at this time						
Responsible Parties						
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
RDM 6.8 and 6.6	RDM Process Owner	PMW 205 Engineering			TBD	Change Ticket System Management
RDM 6.8 and 6.6	RDM Manager	SPAWAR			TBD	Change Ticket Management System
RDM 6.8 and 6.6	RDM Analysts and Operators	PMW 205 and NNWC			TBD	TBD
RDM 6.8 and 6.6	RDM Administrators and Operators	Contractor			TND	TBD

22.1.6.2 DECISION TIMELINES

Reserved

22.1.6.3 TOOLS

Remedy and SMY are currently used by contractor

22.1.6.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
RDM Process Owner	The RDM Process Owner is accountable for ensuring the process is Fit for Purpose. For more detail see Section 3.1.1.4
RDM Process Manager	The RDM Process Manager is responsible for operational management of the process, including coordination across processes, and is responsible for the overall quality of the process. For more detail see Section 3.1.1.4
Contractor	The Contractor operates and manages RDM activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations
Other Process Owners and	Process owners and Stakeholders of other ITSM or business processes that have a dependency or integration point with the RDM process

Stakeholders	
--------------	--

22.1.6.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

RDM 6	RDM Process Owner	RDM Process Manager	Other Process Owners	Contractor
Verify readiness of targets	R	C	I	A
Distribute, install and verify deployment items	R	C	I	A
Perform integrity check	R	C	I	A
Run remediation procedures	A	R	I	C
Remove redundant capabilities, prepare secure access to deployed items and create CI/Asset data update packages	R	C	I	A
Provide early life support	R	C	I	A
Transition to full operational status	R	C	I	A
Communicate deployment capabilities	A	R	I	C

22.1.6.6 METRICS

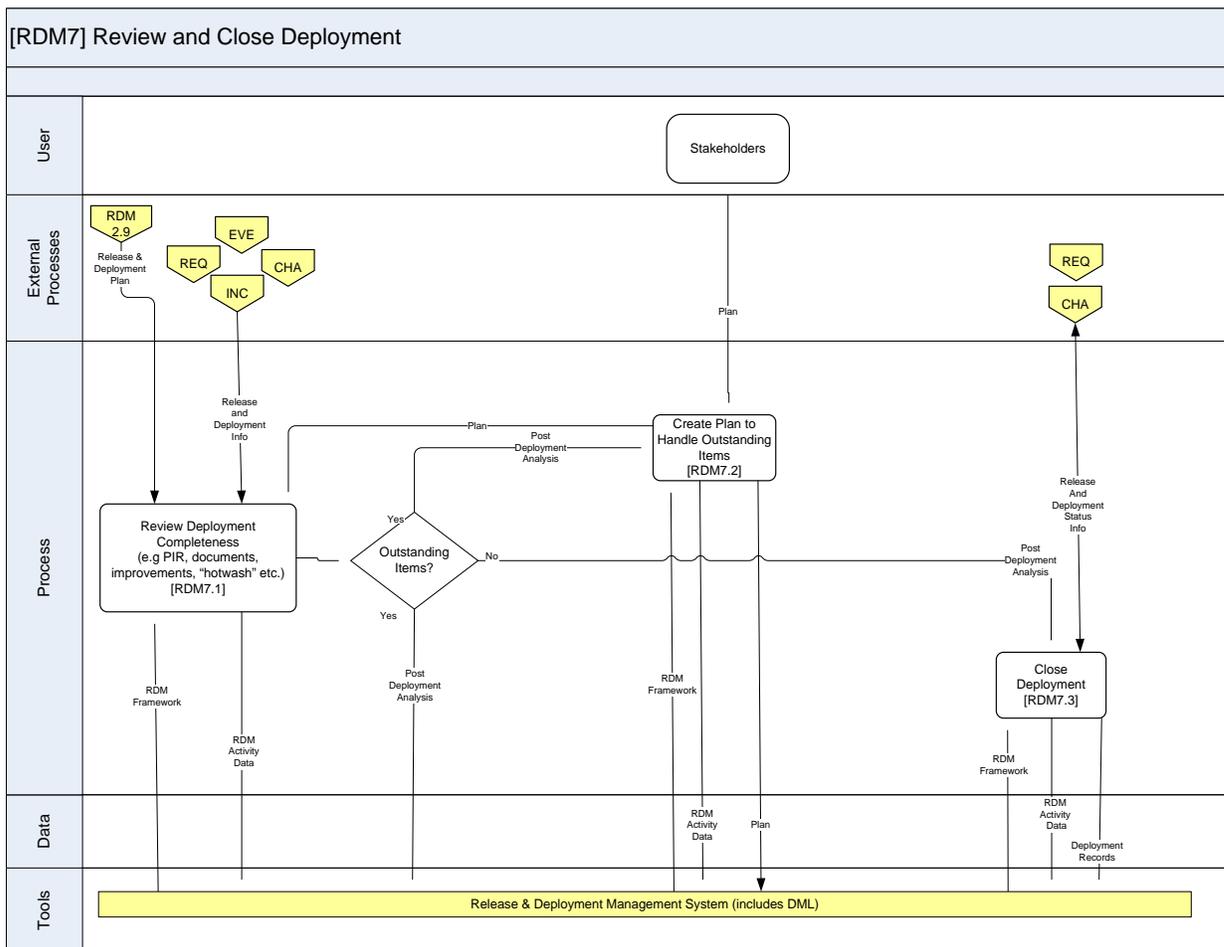
The following metrics will be captured for RDM6:

Metric Total Releases Implemented	
Description	Volume of releases deployed over time
Relevance	Overall performance indicator of the robustness of system
Target Values	TBD
Calculation	Number of release per selected period of time

Notes	None
--------------	------

22.1.7 [RDM7] Review and Close Deployment

This activity reviews the tasks completed during deployments and determines that all objectives of the deployment plan were met. A management plan is established for outstanding risks, issues, incidents and known errors before the deployment is closed. Deployment is completed with a handover of the support to Service Operations.



7.0 RDM_Review and Close_Deployment_SOP_v1.0				
Step	Process Model Task	Action	Role	Details

1	Review deployment completeness (e.g PIR, documents, improvements, “hotwash” etc.)	Contractor owned and performed	• Contractor	• Reserved
2	Create plan to handle outstanding items	Contractor owned and performed	• Contractor	• Reserved
3	Close deployment	Deployment is formally reviewed and closed	• PMW205 and NETOPS	• Situational awareness for this task with be accomplished by government participation in Post Implementation Review

22.1.7.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym RDM7						
Assumptions: None to report						
Constraints: None known at this time						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
Close Deployment	RDM Process Owner	PMW 205 Engineering			TBD	Change Ticket System Management
Close Deployment	RDM Manager	SPAWAR			TBD	Change Ticket Management System
Close Deployment	RDM Analysts and Operators	PMW 205 and NNWC			TBD	TBD
Close Deployment	RDM Administrators and Operators	Contractor			TND	TBD

22.1.7.2 DECISION TIMELINES

Reserved

22.1.7.3 TOOLS

Remedy and SM7 are currently being used by contractor.

22.1.7.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
RDM Process Owner	The RDM Process Owner is accountable for ensuring the process is Fit for Purpose. For more detail see Section 3.1.1.4
RDM Process Manager	The RDM Process Manager is responsible for operational management of the process, including coordination across processes, and is responsible for the overall quality of the process. For more detail see Section 3.1.1.4
Contractor	The Contractor operates and manages RDM activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations
Other Process Owners and Stakeholders	Process owners and Stakeholders of other ITSM or business processes that have a dependency or integration point with the RDM process

22.1.7.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

RDM 7	RDM Process Owner	RDM Process Manager	Other Process Owners	Contractor
Review deployment completeness (e.g PIR, documents, improvements, “hotwash” etc.)	R	C	I	A
Create plan to handle outstanding items	R	C	I	A
Close deployment	A	C	I	R

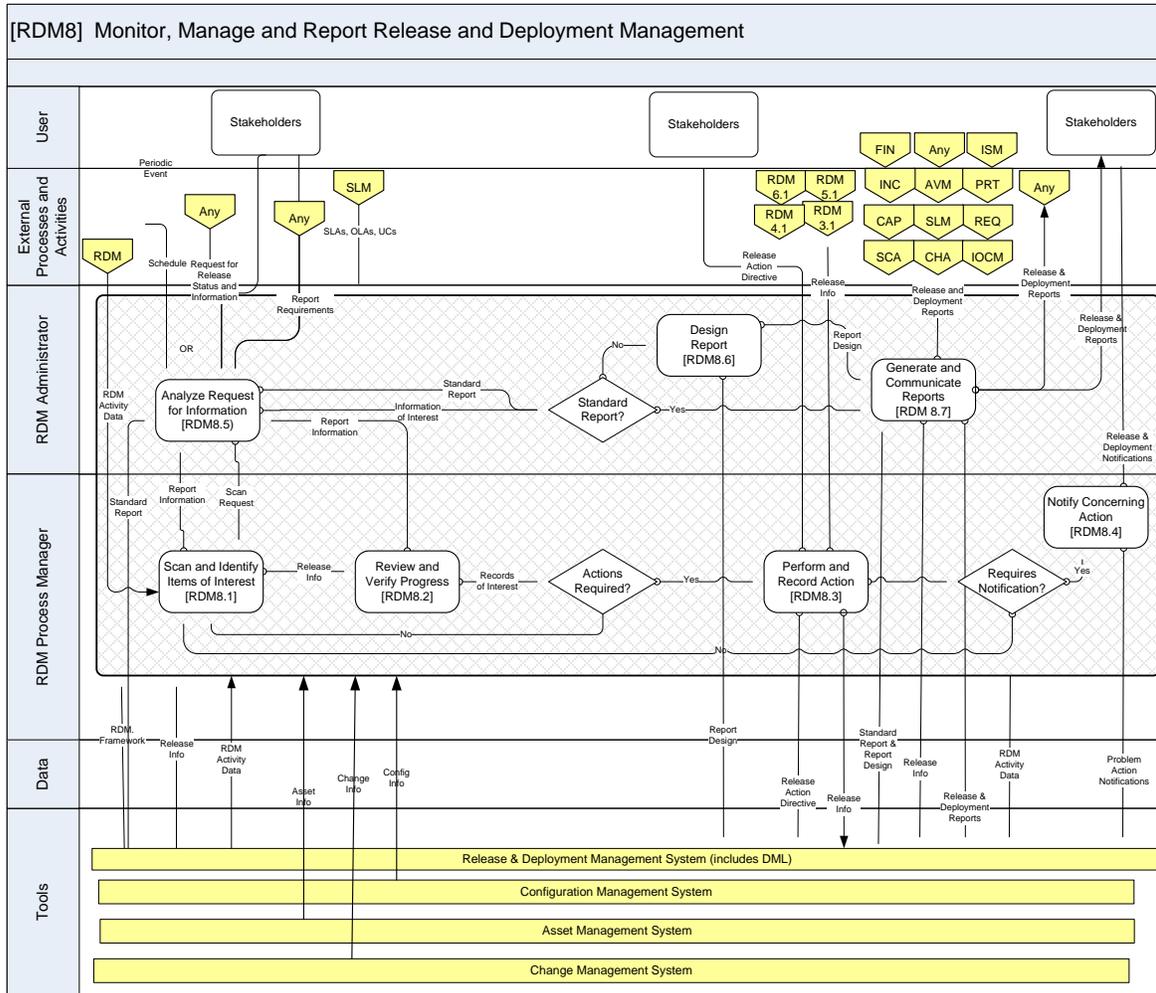
22.1.7.6 METRICS

The following metrics will be captured for RDM 7:

Metric: Number of Releases Resulting In Incidents or Problems	
Description	Releases that cause reported incidents and / or problems
Relevance	Overall efficiency of RDM (and CHA) process
Target Values	99.999%
Calculation	Inverse of number of incidences or problems caused by changes per opportunity
Notes	None

22.1.8 [RDM8] Monitor, Manage and Report Release and Deployment

This activity involves the overall monitoring of work within the process and reporting on specific items or general status to stakeholders.



8.0 RDM_Monitor_Manage_Report_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Scan and identify items of interest	Contractor owned and performed	• Contractor	• Reserved
2	Review and verify progress	Contractor owned and performed	• Contractor	• Reserved

3	Perform and record action	Contractor owned and performed	• Contractor	• Reserved
4	Notify concerning action	Notification is issued that action is being taken on issue		• The RDM Process Owner takes corrective or preventive action in response to PIR
5	Analyze request for information	Contractor owned and performed	• Contractor	• Reserved
6	Design report	Contractor owned and performed	• Contractor	• Reserved
7	Generate and communicate reports	Contractor owned and performed	• Contractor	• Reserved
8	Notify concerning action	Contractor owned and performed	• Contractor	• Reserved

22.1.8.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym RDM8						
Assumptions: None at this time						
Constraints: None known at this time						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
Notify concerning action	RDM Process Owner	PMW 205 Engineering			TBD	Change Ticket System Management

Notify concerning action	RDM Manager	SPAWAR			TBD	Change Ticket Management System
Notify concerning action	RDM Analysts and Operators	PMW 205 and NNWC			TBD	TBD
Notify concerning action	RDM Administrators and Operators	Contractor			TND	TBD

22.1.8.2 DECISION TIMELINES

Reserved

22.1.8.3 TOOLS

Remedy and SM7 being used by current contractor.

22.1.8.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
RDM Process Owner	The RDM Process Owner is accountable for ensuring the process is Fit for Purpose. For more detail see Section 3.1.1.4
RDM Process Manager	The RDM Process Manager is responsible for operational management of the process, including coordination across processes, and is responsible for the overall quality of the process. For more detail see Section 3.1.1.4
Contractor	The Contractor operates and manages RDM activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations
Other Process Owners and Stakeholders	Process owners and Stakeholders of other ITSM or business processes that have a dependency or integration point with the RDM process

22.1.8.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

RDM 8	RDM Process Owner	RDM Process Manager	Other Process Owners	Contractor
Scan and identify items of interest	R	C	I	A
Review and verify progress	R	C	I	A
Perform and record action	R	C	I	A
Notify concerning action	R	C	I	A
Analyze request for information	R	C	I	A
Design report	R	C	I	A
Generate and communicate reports	R	C	I	A
Notify concerning action	A	R	I	C

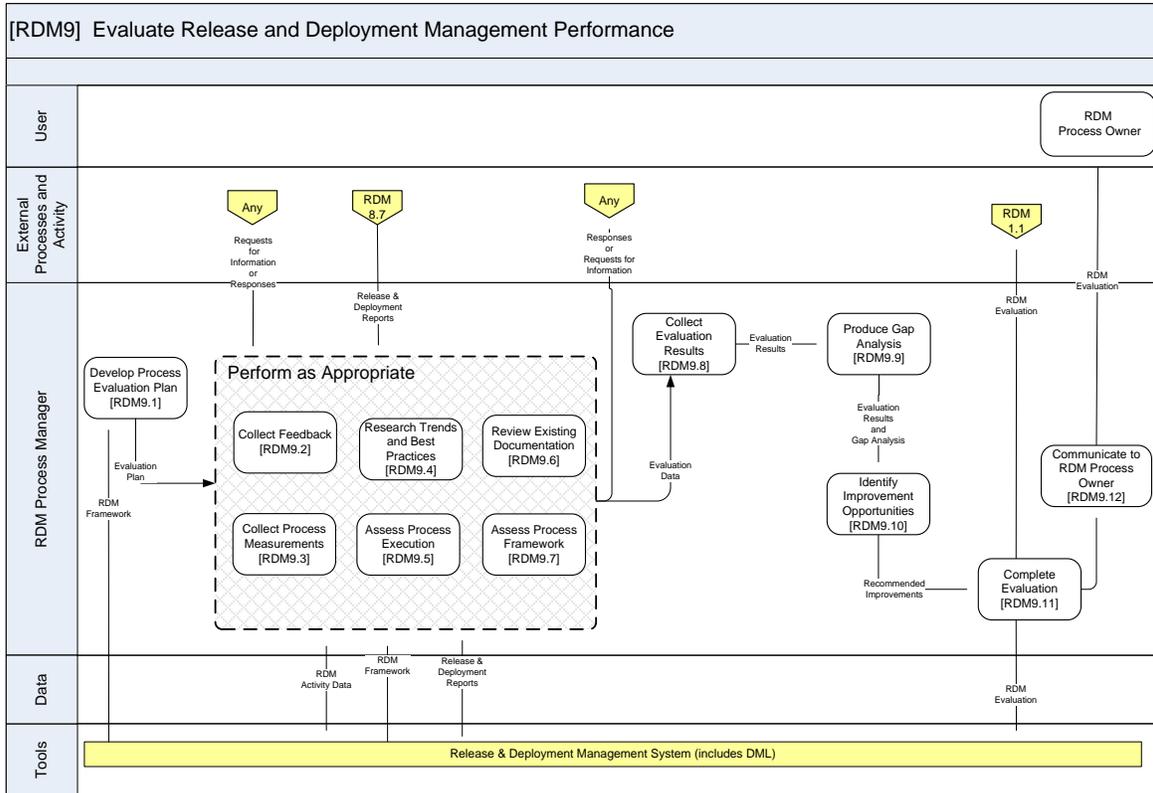
22.1.8.6 METRICS

The following metrics will be captured for RDM8:

Metric – Customer Satisfaction	
Description	Assessment of customer satisfaction
Relevance	Is service meeting end user needs
Target Values	TBD
Calculation	Customer surveys and other
Notes	None

22.1.9 [RDM9] Evaluate Release and Deployment Management Performance

Identifies what improvements can be made to the Release and Deployment Management process using information from Post Implementation Review (PIR).



9.0 RDM_Monitor_Evaluate_SOP_v1.0				
Step	Process Model Task	Action	Role	Details
1	Develop process evaluation plan	Establish the processes required to monitor and evaluate RDM process performance	<ul style="list-style-type: none"> • RDM Manager 	<ul style="list-style-type: none"> • Define the Critical Success Factors (CSFs) and Key Performance Indicators (KPIs) used to monitor process performance. • Define the periods of evaluation and expectations for process review • Define and align roles and responsibilities for performing defined tasks
2	Collect feedback	Gather data related to process performance	<ul style="list-style-type: none"> • RDM Manager 	<ul style="list-style-type: none"> • Define what data can be gathered
3	Collect process measurements	Process gathered data and perform analysis and calculate defined measurements	<ul style="list-style-type: none"> • RDM Manager 	<ul style="list-style-type: none"> • Gather, process data so that it can be analyzed
4	Research trends and best practices	Identify trends and successful practices that are or should be incorporated into the RDM process	<ul style="list-style-type: none"> • RDM Manager 	<ul style="list-style-type: none"> • Identify trends associated with the RDM process • Identify benefits and successes of the process • Identify good practices that could help improve RDM process tasks
5	Assess process execution	Analyze data gathered to assess the effectiveness and efficiency of the RDM process	<ul style="list-style-type: none"> • RDM Manager 	<ul style="list-style-type: none"> • Analyze the data gathered to determine required actions to support and improve the RDM process

6	Review existing documentation	Review the defined process to determine if changes are needed or beneficial	<ul style="list-style-type: none"> • RDM Manager 	<ul style="list-style-type: none"> • Review the documented process and compare analysis results with established practices • Identify training opportunities to better establish existing processes • Identify opportunities to improve the RDM process or the existing documentation
7	Assess the process framework	Review the process framework for opportunities to improve tasks and activities that address process gaps	<ul style="list-style-type: none"> • RDM Manager 	<ul style="list-style-type: none"> • Evaluate the process framework to identify gaps that may be causing process pain points • Identify where failure points have occurred or could occur • Establish a Continual Process Improvement practice that includes process stakeholders
8	Collect evaluation results	Evaluate all the data gathered and potential recommendations for CPI	<ul style="list-style-type: none"> • RDM Manager 	<ul style="list-style-type: none"> • Evaluate all data gathered • Review recommendations and suggestions
9	Produce gap analysis	Produce a gap analysis recommendations	<ul style="list-style-type: none"> • RDM Manger 	<ul style="list-style-type: none"> • Produce a report of the gap analysis and recommendations • Prepare to present the gathered information to stakeholders and process governance teams
10	Identify improvement opportunities	With the input of stakeholders and process governance teams, identify the actions required to better	<ul style="list-style-type: none"> • RDM Manager 	<ul style="list-style-type: none"> • Meet with stakeholders and process Governance roles to review and assess recommendations • Make decisions on recommendations to address gaps identified

		achieve process objectives		
11	Complete evaluation	Document the steps needed to complete the recommendations of the DAT leadership team	<ul style="list-style-type: none"> • RDM Manager 	<ul style="list-style-type: none"> • Document and communicate decisions and prepare for actions to support their implementation

22.1.9.1 CURRENT OPERATIONS POINTS OF CONTACT

Process Acronym RDM 9						
Assumptions: Nothing at this time						
Constraints: None known at this time						
	Responsible Parties					
Process Point	Position	Org	Name	Contact Info	Tools	Tool Rqmts
All steps in establishing evaluation of RDM	RDM Process Owner	PMW 205 Engineering			TBD	Change Ticket System Management
All steps in establishing evaluation of RDM	RDM Manager	SPAWAR			TBD	Change Ticket Management System
All steps in establishing evaluation of RDM	RDM Analysts and Operators	PMW 205 and NNWC			TBD	TBD
All steps in establishing evaluation of RDM	RDM Administrators and Operators	Contractor			TND	TBD

22.1.9.2 DECISION TIMELINES

Reserved

22.1.9.3 TOOLS

TBD

22.1.9.4 ROLES AND RESPONSIBILITIES

The following table lists the roles and responsibilities for execution of this SOP.

Role	Responsibility
RDM Process Owner	The RDM Process Owner is accountable for ensuring the process is Fit for Purpose. For more detail see Section 3.1.1.4
RDM Process Manager	The RDM Process Manager is responsible for operational management of the process, including coordination across processes, and is responsible for the overall quality of the process. For more detail see Section 3.1.1.4
Contractor	The Contractor operates and manages RDM activities on a daily basis. They receive requirements from the Government and work to establish those requirements in operations
Other Process Owners and Stakeholders	Process owners and Stakeholders of other ITSM or business processes that have a dependency or integration point with the RDM process

22.1.9.5 R/A/C/I

This following table contains a task-level RACI chart designating which of the above roles are (R)esponsible, (A)ccountable, (C)onsulted, or (I)nformed in the performance of each Process Activity task:

RDM 9	RDM Process Owner	RDM Process Manager	Other Process Owners	Contractor
Develop process evaluation plan	A	R	C/I	I
Collect feedback	A	R	C/I	I
Collect process measurements	A	R	C/I	I
Research trends and best practices	A	R	C/I	I
Assess process execution	A	R	C/I	I
Review existing documentation	A	R	C/I	I
Assess the process framework	A	R	C/I	I
Collect evaluation results	A	R	C/I	I
Produce gap analysis	A	R	C/I	I
Identify improvement opportunities	A	R	C/I	I
Complete evaluation	A	R	C/I	I

Communicate to process owner	A	R	C/I	I
------------------------------	---	---	-----	---

Metrics

A performance management plan with complete metrics control plan should be worked up for this step as part of detailed processes design.

Acronyms

ACRONYM	DEFINITION
AMDB	Asset Management Database
AMIP	Asset Management Implementation Plan
AMP	Asset Management Plan
AMP	Availability Management Plan
AS	Acquisition Strategy
ASN-RDA	Office of the Assistant Secretary of the Navy (Research, Development and Acquisition)
ATO	Authority to Operate
BCP	Business Continuity Plan
C&A	Certification and Accreditation
C2	Command and Control
CAB	Change Advisory Board
CANES	Consolidated Afloat Networks and Enterprise Services
CBT	Computer-Based Training
CDRL	Contract Data Requirements List
CDS	Cross Domain Security
CI	Configuration Item
CLIN	Catalog Line Item Number
CMDB	Configuration Management Database
CMIS	Capacity Management Information System
CMP	Configuration Management Plan
CMS	Change Management System
CND	Computer Network Defense
CO/CO	Contractor Owned / Contractor Operated
COI	Communities of Interest
CONOPS	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial Off the Shelf
CYBERCOM	Fleet Cyber Command
DAA	Designated Accrediting Authority
DFS	Distributed File System
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DM	Decision Meeting
DMZ	Demilitarized Zone
DoD	Department of Defense
DON	Department of the Navy
DON CIO	Department of Navy Chief Information Officer
DR	Disaster Recovery
DV	Desktop Virtualization
ECCB	Engineering Change Control Board
ECP	Engineering Change Proposal
EDSS	Engineering Design and Support Services
EILT	Executive Integration Leadership Team
ES	Enterprise Services
ESDS	Electronic Software Delivery Services
ESL	Enterprise Software Licensing
EUHW	End-User Hardware

GFY	Government Fiscal Year
GIG	Global Information Grid
GNO	Global Network Operations
GO/CO	Government Owned / Contractor Operated
HDD	Hard Disk Drive
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alerts
IDE	Integrated Data Environment
IM/IT	Information Management / Information Technology
IPR	In Progress Review
ISOOA	Independent Security Operations Oversight and Assessment
IT-21	Information Technology for the 21st Century
LCAB	Local Change Advisory Board
MCEN	Marine Corps Enterprise Network
MD	Management Domain
NCMO	Navy Circuit Management Office
NCPDM	Navy CoSC Process Definition Model
NEN	Naval Enterprise Networks
NET	NMCI Enterprise Tool
NetOps	Network Operations
NNE	Naval Networking Enterprise
NNPDM	Navy NGEN Process Definition Model
NNWC	Naval Network Warfare Command
NSA	National Security Agency
NSA	National Security Agency
NSIB	NGEN Senior Integration Board
OCONUS	Outside the United States
OEM	Original Equipment Manufacturer
ONE-NET	OCONUS Navy Enterprise Network
QA	Quality Assurance
RAS	Remote Access Service
RFC	Requests for Change
RFP	Request for Proposal
RFQ	Request for Quote
ROM	Rough Order of Magnitude
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SECCONOPs	Security Concept of Operations
SEM	Security Event Management
SITREP	Situation Report
SLA	Service Level Agreement
SME PED	Secure Mobile Environment Portable Electronic Device
SRM	Contractor Relationship Management
SW	Software
TCB	Transition Control Board
TMP	Transition Management Plan
TRRB	Training Readiness Review Board
TXS	Transport Services
USMC	United States Marine Corps
USN	United States Navy

VTC	Video Conferencing
VV&R	Verification, Validation, and Reporting
WAN	Wide Area Network

Process Diagram Legend

The Process Activity diagrams in this document are created using a standardized Microsoft Visio template. The Process Activity Diagrams are developed in the form of a 'swim lane', which depicts sequential process tasks horizontally, with all of roles, functions, interfaces, data, and tools that interact with process activities listed vertically.

The Process Activity Diagram template is owned and maintained by the ITSM Architect and may be obtained with permission from the ITSM workspace on the PEO EIS portal.

The shape legend used to create the Process Activity Diagram is given below:

