

[Contract Number]

**ATTACHMENT J-1,
APPENDIX A**

**CROSS FUNCTIONAL
PERFORMANCE WORK STATEMENT**

The following matrix provides a crosswalk from the Attachment J-1, *PWS*, to Attachment J-1, Appendix A, *Cross Functional Performance Work Statement*. Appendix A contains a blend of visions and goals, background and historical information, and contract requirements. The table below contains a mapping of the specific requirements between the two documents. Where sections 3.0, 4.0, and 5.0 are referenced, it includes all subsections of those sections.

MATRIX OF APPENDIX A, <i>CROSS FUNCTIONAL PERFORMANCE WORK STATEMENT</i>, TO PWS REQUIREMENTS		
APPENDIX A SECTION		PWS SECTIONS
1	I ³ P Acquisitions	1.0
2	IT Service Management: Organization and Governance within NASA	1.0
3	Service Coordination and Collaboration	1.0, 2.0, 2.10, 2.11
4	NASA IT Infrastructure Library (ITIL) Version 3 Approach	1.0, 2.1, 2.9, 2.10
5	I ³ P Common Architecture Components	1.0, 3.6, 3.8, 3.9, 3.10, 3.11, 4.0
6	Common Information Technology Security Requirements	2.6, 3.6, 3.7, 3.12, 4.0, 6.1
7.1	General Provisions	1.0, 2.1, 2.9, 2.10
7.2	Change Management	3.9, 3.10, 3.11
7.3	Incident Management	3.6, 3.8, 3.12, 4.0
7.4	Request Management	3.0, 4.0
7.5	Problem Management	3.0, 4.0
7.6	Service Level Management	3.1, 3.2, 3.4, 3.5, 3.7, 3.9, 3.10, 3.11, 3.13
7.7	Service Asset and Configuration Management	2.3, 2.4, 2.10, 3.0, 4.0, 5.3
7.8	Release and Deployment Management	3.0, 4.0, 5.0
7.9	Capacity Management	3.1, 3.2, 3.4, 3.5, 3.7, 3.9, 3.10, 3.11, 3.12, 3.13, 4.0
7.10	Availability Management	3.1, 3.2, 3.4, 3.5, 3.7, 3.9, 3.10, 3.11, 3.12, 3.13, 4.0
7.11	IT Service Continuity Management	2.6, 3.7, 3.12
7.12	Knowledge Management	3.0, 4.0, 5.3
7.13	Information Security Management	2.6, 3.6, 3.7, 3.12, 4.0, 6.1
8.0	Common Project Management Guidelines	5.0

Table of Contents

1.	I³P Acquisitions	8
1.1	Introduction and Overview	8
1.2	Concept of Operations	8
1.3	I ³ P Success Criteria.....	9
1.4	Scope and Boundaries of Contracts	9
1.5	Client Facing and Support Services Contracts.....	12
1.6	Cross Functional and Collaboration Activities	13
1.7	Service Level Agreements	14
2	IT Service Management: Organization and Governance within NASA.....	16
2.1	Introduction and Overview	16
2.2	The NASA IT Organization: Roles and Responsibilities	16
2.2.1	Agency CIO	16
2.2.2	Enterprise Service Management	17
2.2.3	Enterprise Architecture (EA)	17
2.2.4	Systems Engineering and Integration (SE&I).....	18
2.2.5	Service Executives (SEs)	19
2.2.6	Service Integration Management (SIM).....	19
2.2.7	Enterprise Service Desk.....	20
2.2.8	Service Offices	20
2.2.9	Center CIO	21
2.2.10	Mission Directorate CIOs	22
2.3	NASA IT Governance Process and Structure.....	22
2.4	Contractor Responsibilities.....	27
2.5	Relationship Management	28
3	Service Coordination and Collaboration	30
3.1	Introduction and Overview	30
3.2	Service Delivery Coordination and Collaboration.....	30
4	NASA IT Infrastructure Library (ITIL) Version 3 Approach	32
4.1	Introduction and Overview	32
4.2	Implementation Plan and Scope for I ³ P	32
4.3	NASA Defined ITIL v3 Process Requirements.....	35
5	I³P Common Architecture Components	36
5.1	Introduction and Overview	36
5.2	NASA Enterprise Architecture Repository.....	36
5.3	NASA Enterprise Service Desk	37

5.4	NASA Enterprise Service Request System.....	38
5.5	NASA Application Portfolio Management (APM)	39
6	Common Information Technology Security Requirements	41
6.1	Introduction and Overview	41
6.2	Common IT Security Requirements	41
7	Cross Functional Performance Work Statement Elements	45
7.1	General Provisions	45
7.1.1	IT Infrastructure Library® Version 3 (ITIL® v3) Support.....	45
7.1.2	Understanding and Knowledge of ITIL®	45
7.2	Change Management	45
7.2.1	High-Level Process Flow Diagram, Goal, Purpose and General.....	45
7.2.2	Create and Maintain Change Management Process.....	46
7.2.3	Create and Record Request for Change (RFC).....	47
7.2.4	Review Request for Change (RFC)	47
7.2.5	Assess and Evaluate Change.....	47
7.2.6	Authorize Change	47
7.2.7	Coordinate Change Implementation	47
7.2.8	Review and Close Change Record.....	48
7.3	Incident Management.....	48
7.3.1	High-Level Process Flow Diagram, Goal and General Provisions.....	48
7.3.2	Create and Maintain Incident Management Process	50
7.3.3	Identify Incident.....	50
7.3.4	Log Incident	50
7.3.5	Categorize Incident	50
7.3.6	Prioritize Incident.....	50
7.3.7	Conduct Initial Diagnosis.....	50
7.3.8	Escalate Incident	51
7.3.9	Investigate and Diagnose Incident	51
7.3.10	Resolve Incident and Recover Service.....	51
7.3.11	Close Incident	51
7.4	Request Fulfillment.....	52
7.4.1	High-Level Process Flow Diagram and General Provisions	52
7.4.2	Create and Maintain Request Fulfillment Process	53
7.4.3	Initiate Request	53
7.4.4	Secure Approvals	53
7.4.5	Fulfill Request.....	53
7.4.6	Close Request.....	54
7.5	Problem Management	54
7.5.1	High-Level Process Flow Diagram and General Provisions	54
7.5.2	Create and Maintain Problem Management Process	55
7.5.3	Detect and Identify Problem	55

7.5.4	Log Problem.....	55
7.5.5	Categorize Problem.....	56
7.5.6	Prioritize Problem	56
7.5.7	Investigate and Diagnose Problem.....	56
7.5.8	Resolve Problem	57
7.5.9	Close Problem	57
7.5.10	Conduct Major Problem Review.....	57
7.6	Service Level Management (SLM).....	57
7.6.1	High-Level Process Flow Diagram, Goal, Purpose and General Provisions.....	57
7.6.2	Create and Maintain SLM Process.....	58
7.6.3	Design Service Level Agreement (SLA) Frameworks	58
7.6.4	Develop Service Level Requirements (SLR).....	58
7.6.5	Develop and Negotiate Service Level Scope and Underpinning Agreements	59
7.6.6	Produce Service Level Reports	59
7.6.7	Conduct Service Reviews	59
7.6.8	Review and Revise Service Level Agreements and Underpinning Agreements	59
7.6.9	Develop Contacts and Relationships.....	59
7.6.10	Record and Manage Customer Service Level Feedback.....	59
7.7	Service Asset and Configuration Management (SACM).....	60
7.7.1	High-Level Process Flow Diagram, Goal, Purpose and General Provisions.....	60
7.7.2	Create and Maintain Service Asset and Configuration Management (SACM) Process	61
7.7.3	Develop Service Asset and Configuration Management (SACM) Plan.....	61
7.7.4	Identify CI / Asset	61
7.7.5	Control CI / Asset	61
7.7.6	Verify and Audit CI / Asset	62
7.8	Release and Deployment Management (RDM).....	62
7.8.1	High Level Process Flow Diagram, Goal, Purpose and General Provisions.....	62
7.8.2	Create and Maintain Release and Deployment Management Process	63
7.8.3	Develop Release Plan.....	63
7.8.4	Prepare for Release Build and Test.....	63
7.8.5	Build and Test Release.....	63
7.8.6	Conduct Service Rehearsal and Pilot	64
7.8.7	Plan and Prepare for Deployment	64
7.8.8	Deploy Service	64
7.8.9	Decommission and Retire Service	64
7.8.10	Review and Close Service Release Deployment	64
7.9	Capacity Management	65

7.9.1	High-Level Process Flow Diagram, Goal, Purpose and General Provisions.....	65
7.9.2	Create and Maintain Capacity Management Process.....	65
7.9.3	Manage Business Capacity	66
7.9.4	Manage Service Capacity.....	66
7.9.5	Manage Component Capacity	66
7.9.6	Establish and Manage Capacity Thresholds	67
7.9.7	Manage Demand (within existing capacity)	67
7.9.8	Develop Capacity Models and Trend Reports	67
7.9.9	Develop Sizing Estimates	67
7.10	Availability Management.....	67
7.10.1	High-Level Process Flow Diagram, Goal, Purpose and General Provisions.....	67
7.10.2	Create and Maintain Availability Management Process.....	68
7.10.3	Determine Vital Business Functions	68
7.10.4	Determine Requirements and Formulate Recovery Design Criteria.....	68
7.10.5	Determine Impact of IT Service and Component Failure	69
7.10.6	Define Availability, Reliability and Maintainability Targets	69
7.10.7	Monitor and Analyze Availability, Reliability and Maintainability	69
7.10.8	Identify and Investigate Levels of Availability Performance	69
7.10.9	Produce and Maintain Availability Management Plan	69
7.11	IT Service Continuity Management (ITSCM).....	70
7.11.1	High-Level Process Flow Diagram, Goal, Purpose and General Provisions.....	70
7.11.2	Create and Maintain IT Service Continuity Management Process	71
7.11.3	Quantify Impact on Business of Loss of IT Services.....	71
7.11.4	Identify and Assess Risks Associated with Potential Threats.....	71
7.11.5	Develop the IT Service Continuity Management (ITSCM) Plan.....	71
7.11.6	Test the IT Service Continuity Management (ITSCM) Plan	71
7.11.7	Operate and Maintain the ITSCM Plan.....	71
7.12	Knowledge Management	72
7.12.1	High-Level Process Flow Diagram, Goal, Purpose and General Provisions.....	72
7.12.2	Create and Maintain Knowledge Management Process.....	73
7.12.3	Develop and Maintain Knowledge Management System.....	73
7.12.4	Gather and Capture Information	73
7.12.5	Validate and Organize Information.....	73
7.12.6	Disseminate Information.....	73
7.13	Information Security Management (ISM)	74
7.13.1	High-Level Process Flow Diagram, Goal and Purpose	74
7.13.2	Create and Maintain Information Security Management (ISM) Process.....	74
7.13.3	Communicate, Implement and Enforce Information Security Management (ISM) Procedures	74
7.13.4	Assess and Classify Information Assets and Documentation	74

7.13.5	Monitor and Manage Security Breaches and Major Incidents.....	75
7.13.6	Analyze and Report Security Breaches and Incident Impact on Business.....	75
7.13.7	Conduct Security Reviews, Audits and Penetration Tests.....	75
7.13.8	Improve Security Controls, Risk Assessment and Responses	75
8	Common Project Management Guidelines	76
8.1	Introduction and Overview	76
8.2	Applicability of NPR 7120.7	76
9	Glossary of Terms	77
10	Acronym List	82
11	Referenced Document List	85

Table of Figures

Figure 1:	Concept of mapping current Agency and Center contracts to I ³ P contracts	11
Figure 2:	Relationship between client facing and supporting services.....	13
Figure 3:	SLA Integration Concept.....	14
Figure 4:	NASA Business and Service Architectures.....	18
Figure 5:	IT Portfolios and Governing Policies	23
Figure 6:	NASA IT Governance Structure	24
Figure 7:	I3P Governance Structure	26
Figure 8:	High-Level Change Management Process Flow Diagram	46
Figure 9:	High-Level Incident Management Process Flow Diagram	49
Figure 10:	High-Level Request Fulfillment Process Flow Diagram	52
Figure 11:	High-Level Problem Management Process Flow Diagram.....	54
Figure 12:	High-Level Service Level Management Process Flow Diagram	58
Figure 13:	High-Level Service Asset and Configuration Management Process Flow Diagram ...	60
Figure 14:	High-Level Release and Deployment Management Process Flow Diagram	62
Figure 15:	High-Level Capacity Management Process Flow Diagram.....	65
Figure 16:	High-Level Availability Management Process Flow Diagram	68
Figure 17:	High-Level IT Service Continuity Management Process Flow Diagram	70
Figure 18:	High-Level Knowledge Management Process Flow Diagram.....	72
Figure 19:	High-Level Information Security Management Process Flow Diagram.....	74

1. I³P Acquisitions

1.1 Introduction and Overview

To fulfill NASA's requirements for infrastructure improvement the Agency has directed the Office of the CIO (OCIO) to implement a program for providing more reliable and efficient Information Technology (IT) services.

As a result, NASA's OCIO established a major IT improvement initiative in 2007, the IT Infrastructure Integration Program (I³P). Through I³P, the NASA OCIO intends to partner with industry to transform the way IT services are delivered and managed across the Agency.

The I³P strategy includes consolidating service demand across the Agency and working with trusted sourcing partners to deliver standardized, stable, secure, cost effective and high quality IT infrastructure and Enterprise Applications services to the NASA user community.

Specifically, the NASA I³P strategy intends to achieve the following benefits:

- a. Enable Agency-wide collaboration through a seamless IT infrastructure;
- b. Gain efficiencies in IT infrastructure operating costs;
- c. Reduce the complexity of managing IT services across the Agency; and,
- d. Improve IT security across the Agency's mission environment.

In addition, the Agency intends to use this improvement initiative to enable a more process-aligned service delivery model across the scope of I³P. This will be accomplished in part by the adoption of the IT Infrastructure Library (ITIL) framework. NASA expects selected IT contractors to demonstrate their capabilities through the application of ITIL processes, specifically ITIL Version 3.0.

As this document is intended to be nearly identical for all I³P contracts, it frequently uses the plural terms "Contractors" and "I³P Contractors." For purposes of this {ACES/NICS// EAST/WESTPRIME/Compute Services} contract, the terms "Contractors" and "I³P Contractors," as well as "contractor" shall mean the {ACES/NICS/ EAST/WESTPRIME/Compute Services} Contractor only except where it is patently clear that a specific CF-PWS requirement is a joint responsibility of the I³P contractors (e.g., cooperation, coordination, etc.).

1.2 Concept of Operations

Central to NASA's I³P initiative is the recognition that responsibility for major elements of the Agency's 'As-Is' IT environment, which is currently supported by a variety of independent Agency- and Center-based contracts, will be consolidated into a smaller number of integrated Agency-wide I³P Contracts. Operations and service delivery must remain stable throughout phase-in periods (i.e. transition) to assure that NASA customers do not experience disruption to business operations.

I³P contractors shall work with the Agency and with each other, in a collaborative and cooperative manner as prescribed by defined processes and assigned roles and responsibilities to transform NASA's fractured IT infrastructure and enterprise applications service delivery capabilities into a highly consolidated, integrated and secure IT Service Management (ITSM) environment.

The OCIO plans to manage this transformation through the I³P acquisition strategy according to the following four key IT principles:

- a. Mission Enabling: IT at NASA serves to achieve NASA's mission;
- b. Integrated: NASA will implement IT that enables the integration of business (mission) process and information across organizational boundaries;
- c. Efficient: NASA will implement IT to achieve efficiencies and ensure that IT is efficiently implemented; and,
- d. Secure: NASA will implement and sustain secure IT solutions.

1.3 I³P Success Criteria

Successful implementation of the NASA I³P vision will result in significant benefits to the Agency. Specifically, NASA envisions a "To-be" state characterized by the following criteria:

- a. NASA systems can be seamlessly deployed, utilized and secured across Center boundaries;
- b. NASA consistently invests in the right IT solutions that provide the greatest benefit to the NASA mission;
- c. NASA information is accessible, integrated, and actionable;
- d. A reliable, efficient, secure and well-managed IT infrastructure is in place that customers rely on rather than compete with; and,
- e. CIOs are seen as credible, trusted partners in solving business problems

1.4 Scope and Boundaries of Contracts

NASA spends approximately \$1.8 billion dollars annually on IT. Today, much of the infrastructure supporting NASA is decentralized including operations at NASA Headquarters, all ten NASA field Centers, and associated component locations. There are major challenges in IT management associated with a decentralized IT organization, such as lack of sufficient visibility into IT spending, inability to achieve economies of scale, inconsistent IT governance and numerous information security challenges.

NASA is consolidating IT service demand, transforming service delivery, aligning IT management and enhancing IT security through I³P. The acquisitions making up I³P include the following enterprise services:

- a. ACES (Agency Consolidated End-user Services): End-User Services –includes NASA desktops, cell phones, Personal Digital Assistants (PDAs), a portion of NASA’s Identity, Credential, and Access Management (ICAM) services including NASA’s Consolidated Active Directory (NCAD) and issuance of Agency logical credentials, e-mail and calendaring functionality;
- b. NICS (NASA Integrated Communications Services): Communications Services – includes data, voice, video, Local Area Network (LAN) and Wide Area Network (WAN) services;
- c. Compute Services –includes application/data hosting and housing;
- d. WESTPRIME (Web Enterprise Service Technologies): Web Services – to include public-facing website hosting and applications; and,
- e. EAST (Enterprise Applications Service Technologies): Enterprise Applications Services –includes applications services associated with the NASA Enterprise Applications Competency Center, a portion of NASA’s ICAM services including authentication services and the NASA Access Management System (NAMS), Agency-wide collaboration services, and new intranet environments and applications.

Today, these services are provided under Agency-wide service contracts and additional Center IT Infrastructure contracts. The existing contracts are identified in the Tables below.

Location	Contract Name	Contract Number	Contractor
HQ/OCIO	NASA Web Portal Services	GS-35F-0627P	eTouch
MSFC	Enterprise Application Service Technologies (EAST)	NNM04AA02C	SAIC
MSFC	Agency Consolidated End-user Services (ACES)	NNX11AA01C	HP Enterprise Services
MSFC	NASA Integrated Communications Services (NICS)	NNM11AA04C	SAIC
NSSC	Enterprise Service Desk (ESD)	NNX05AA01C	CSC

Table 1: Current Agency-wide Contracts

Location	Contract Name	Contract Number	Contractor
ARC	Ames-Consolidated IT Services Task Order 2 (ACITS2)	NNA08AF13C	Dell Federal Government Services (DFGS)
DFRC	Research Facilities and Engineering Support Services (RF&ESS)	NAS4-00047	Arcata Assoc.
GRC	Professional, Administrative, Computational and Engineering Support Services (PACE III)	NNC08BA09B	DB Consulting Group, Inc
GSFC	Goddard Unified Enterprise Services and Technology (GUEST)	NNG10FE01C	ASRC Primus

HQ	Headquarters Information Technology Support Services (HITSS)	NNH12CF39C	Digital Management, Inc. (DMI)
JSC	JSC Information Technology and Multimedia Services (ITAMS)	NNJ11JA16B	DB Consulting
KSC	Information Management and Communication Support (IMCS)	NNK08OH01C	Abacus Technology
LaRC	Langley Information Technology Enhanced Services (LITES)	L70750D	Stinger Ghaffarian Technologies (SGT)
MSFC	MSFC IT Services (MITS)	NNM10AA03C	Dynetics
NSSC	NASA Shared Services Center (NSSC)	NNX11AA02C	CSC
SSC	Information Technology Services (ITS)	NNS04AB54T	CSC

Table 2: Current Center IT Infrastructure Contracts (Partial List)

The figure below represents how the remaining services under current Agency-wide and Center IT infrastructure and support services contracts map into the I³P acquisitions. The diagram is intended to represent the concept only and not specific contract scope decisions which are specified within each of the individual contracts.

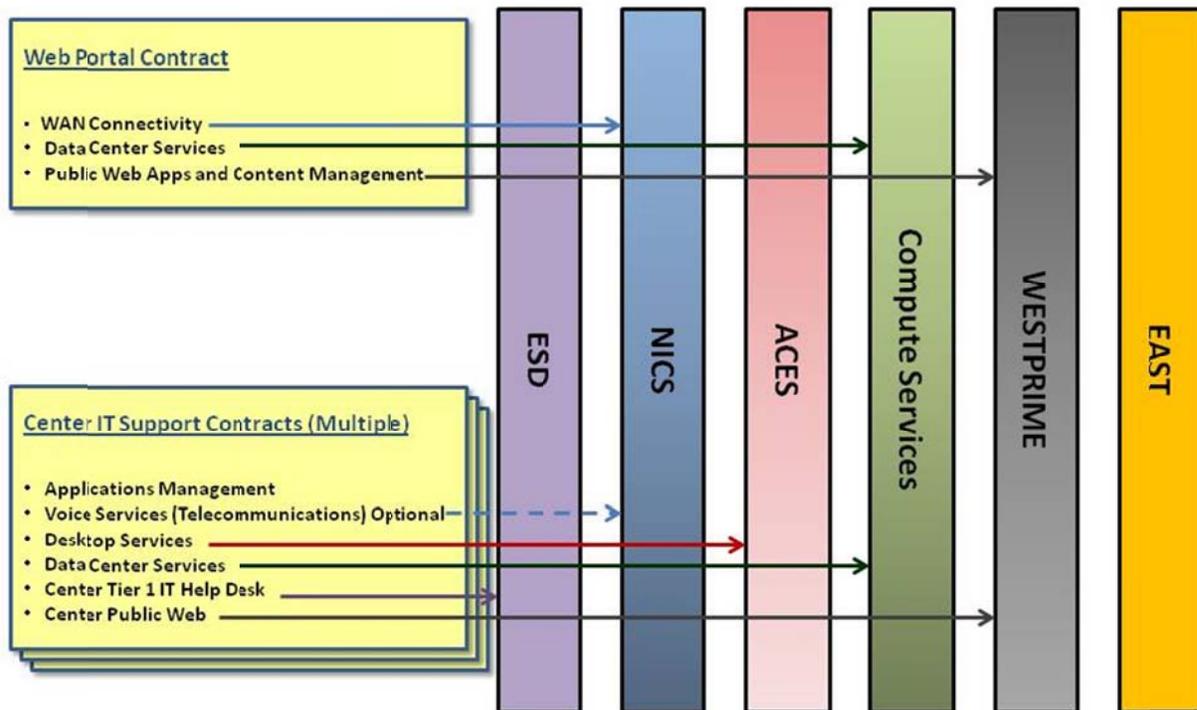


Figure 1: Concept of mapping current Agency and Center contracts to I³P contracts

Compute Services are not managed through a single Agency-wide contract, but rather through a series of existing and planned contract vehicles:

In response to the Federal Data Center Consolidation Initiative (FDCCI), NASA is reducing the overall number of data centers and focusing on “regional” consolidation, ensuring suitable data center capabilities exist at each major NASA facility. The Federal initiative imposes a moratorium on the creation or acquisition (leasing) of any new data centers. Contractors needing access to data centers to house or host NASA or Center systems, storage or data should contact the CIO at the affected or closest center to discuss the requirements and make arrangements for using an approved NASA data center.

In alignment with the FDCCI, NASA is prohibiting the creation of new “server rooms” and “server closets”, where office or other non-data center space is reallocated to house small numbers of servers and/or storage without CIO approval. NASA is in the process of consolidating the contents of all existing “server rooms” and “server closets” into approved data centers. Anyone considering creating a new “server room” or “server closet” should immediately contact the appropriate Center CIO to identify the approved data center that can accept the assets in question.

Consistent with the FDCCI and also in compliance with the 25 Point Plan for IT Reform, NASA is actively addressing the adoption of cloud computing. The NASA Office of the CIO is pursuing an enterprise cloud service offering for commercial cloud services that will allow NASA to aggregate cloud purchases to receive volume pricing and to implement compliance to IT security requirements with least impact to the end users. Anyone needing or considering the use of cloud computing services should contact the affected Center CIO or the OCIO Computing Services Service Office to discuss existing available options.

1.5 Client Facing and Support Services Contracts

ITIL defines client facing services as services that are delivered to end-users of the business (e.g., email, billing, etc.). Support services are defined as services necessary to support the operation of the delivered service (e.g., data center services, managed network service, etc.).

The relationship between Client Facing (Core) Services and Supporting Services is depicted in diagram below.

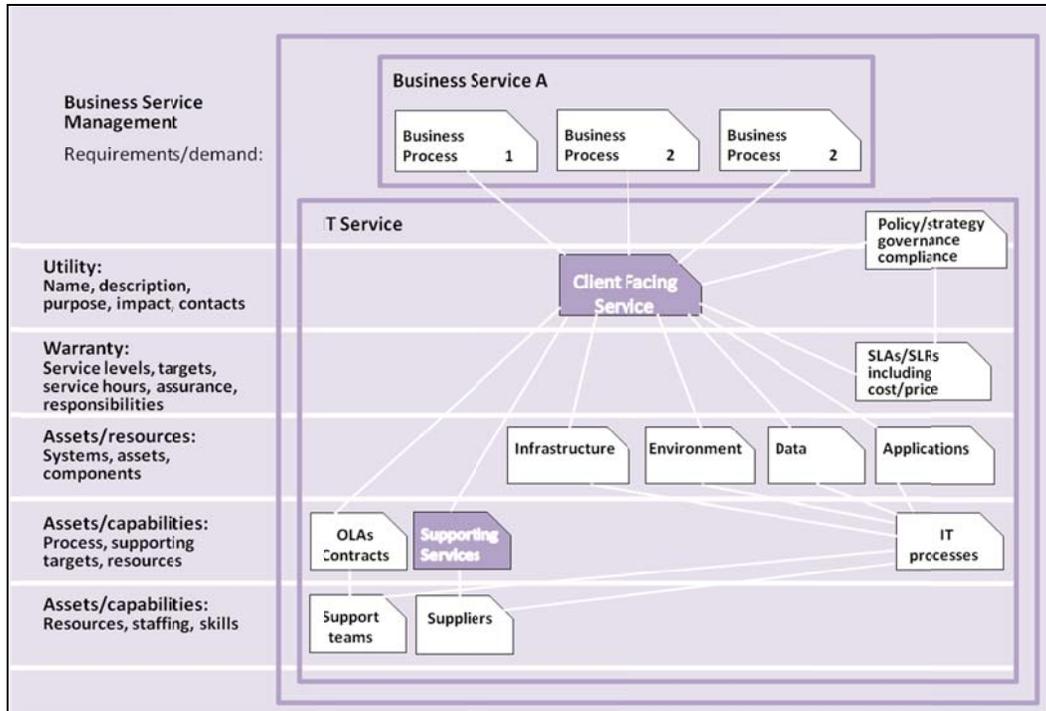


Figure 2: Relationship between client facing and supporting services

All I³P contracts will provide some level of client-facing service delivery. For the purposes of general discussion, NASA's I³P contracts are classified as client facing or support service contracts based on a significant majority of requirements being either client or support services as follows:

- a. Client Facing Contracts:
 1. ACES – End-user services
 2. EAST – Enterprise application services
 3. WESTPRIME – Web services
- b. Support Service Contracts:
 1. NICS – Communication services
 2. Compute Services (multiple contract vehicles expected)

1.6 Cross Functional and Collaboration Activities

Each of the contracts includes a Performance Work Statement (PWS) consisting of defined work activities and Contractor requirements specific to each of NASA's independent service contracts. These PWS's also define roles and responsibilities for the Contractor as they relate to NASA's requirements.

In addition to service-specific performance work statements, there are a number of contractor work activities and responsibilities that cut across all I³P contracts. These Cross-Functional Performance Work Statement (CF-PWS) requirements, contained in this document, are common to each of the contracts. The CF-PWS defines NASA’s requirements for synchronization of effort and solution integration across NASA and multiple contracts supporting the I³P initiative. NASA has taken every effort to ensure that there are no conflicts between the CF-PWS and the contract-specific PWS. If any conflicts do exist, the CF-PWS will take precedence.

Consistent application of these cross functional requirements is central to NASA’s desire to standardize processes using the ITIL Version 3.0 framework and is essential to an effective, integrated enterprise service delivery.

1.7 Service Level Agreements

Service Level Agreements (SLAs) are an important aspect of NASA’s service-based organization and the I³P contracts. An SLA specifies the level, scope and quality of a service that will be provisioned, from the business customers’ perspective. The SLA clarifies how the service provision will be measured, and the penalty to be exacted if the service is not delivered to the agreed level of service.

Service delivery under the NASA I³P program will require the involvement of multiple providers to meet the SLAs established by the NASA business customer. Providers shall work together in the best interest of NASA as described in Section 3. The diagram below depicts how an SLA will be segmented into independent Contractor service levels. Contractor-specific service levels are specified in each of the I³P contracts.

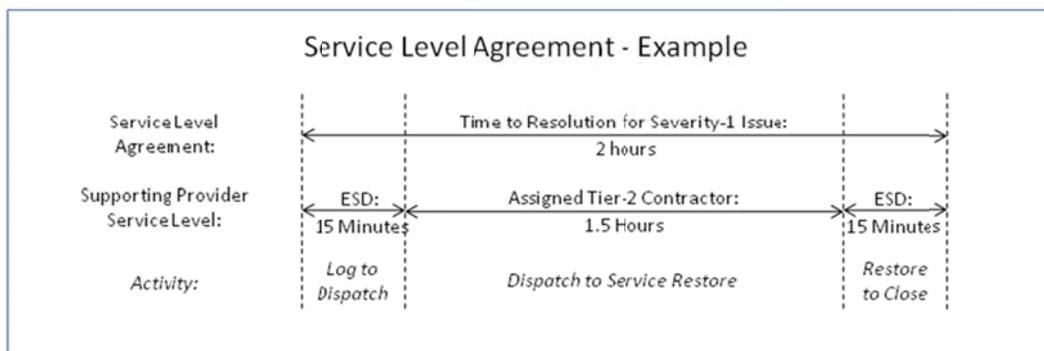


Figure 3: SLA Integration Concept

In the example diagram above, the SLA for restoration of service to the customer for a Severity 1 issue is two hours. The Enterprise Service Desk (ESD) would have a maximum time of fifteen minutes to escalate the call to the appropriate Tier 2 contractor. At that point, as specified in the Tier-2 contractor SLA, the Tier 2 contractor would have a maximum of one and a half (1.5) hours to correct the problem and restore service before assigning the incident back to the ESD

for call closure. After Tier 2 has reassigned the incident to the ESD, the ESD would again have a maximum of fifteen (15) minutes to verify service restoration with the customer and close the call. The sum of the ESD and Tier 2 contractor SLAs (15 minutes + 1.5 hours + 15 minutes) would equal the customer Service Level (2 hours). In this example, only one Tier 2 contractor is involved with the service restoration, but in some cases multiple Tier 2 providers may be involved. I³P Enterprise Service Management (ESM) leadership will coordinate service restoration efforts that span multiple providers. In all cases, Tier 2 providers are accountable only for the service level agreements specified within their individual contract.

2 IT Service Management: Organization and Governance within NASA

2.1 Introduction and Overview

NASA is transforming the Agency's IT infrastructure and applications services environment through I³P. This transformation requires changes in the way NASA manages IT across the Agency including the need to define and clarify roles and responsibilities within the NASA IT organization to assure success of the I³P initiative.

As with most organizations, the NASA IT organization is continually changing and maturing to better meet the evolving needs of the customer base it serves. This section outlines the roles and responsibilities across the IT organization within NASA. Two new elements are defined to support the transformation that is underway, including the establishment of ESM functions within the Agency CIO organization and the creation of Service Integration Management (SIM) within the Agency CIO's Enterprise Service & Integration Division (ES&ID). Contractors providing IT services to NASA shall establish appropriate roles and responsibilities in support of NASA's ITSM vision as described in this section.

2.2 The NASA IT Organization: Roles and Responsibilities

The NASA CIO established I³P and is responsible for overall direction and leadership of the program, within the larger context of NASA's IT organization. Before discussing the NASA IT Organization, it is important to understand the charter and purpose of I³P:

I³P Charter: Provide a NASA Enterprise service support environment that optimizes the ITIL best practice processes for implementing formal ITSM.

I³P Purpose: The I³P initiative seeks to standardize NASA's ITSM practices, align with industry best practices (e.g., ITIL), and yield a set of consistent, repeatable and measurable processes for service delivery to NASA OCIO customers.

The NASA IT organization is comprised of multiple elements serving Agency, Mission, and Center customers and organizations. The elements of the NASA IT organization are defined below, including an overview of the roles and responsibilities of each part of the organization.

2.2.1 Agency CIO

The NASA CIO is accountable for all aspects of IT within NASA as well as for the overall leadership of the NASA IT organization including the establishment of strategy, enterprise architecture, and operational policies and standards to support the NASA mission. To accomplish these functions, the NASA Office of the CIO is organized into 4 divisions including ES&I, IT Security, and Capital Planning and Governance, and the Chief Technology Office (CTO). Within this structure the NASA CIO has also established functions associated with Enterprise Architecture (EA), Systems Engineering and Integration (SE&I), Service Executives

(SEs), and SIM. Through integration with the SIM, the ESD provides critical integration functions in support of Agency ESM. Finally, the NASA CIO is also accountable for establishing a NASA governance model that effectively interconnects the various components of the Agency-wide IT organization and enables effective decision making at all levels within that organization. This governance spans not only the elements of the Agency CIO's office, but also Center and Mission Directorate CIO organizations; these will be described later in this document.

2.2.2 Enterprise Service Management

To support effective delivery of enterprise IT services, the ESM function is performed by ES&ID, interfacing with the other Agency CIO Divisions. ESM provides a NASA Enterprise service support environment that optimizes ITIL best practice processes for implementing formal ITSM. The purpose of ESM within NASA is to standardize NASA's ITSM practices, to align with industry best practices, and to yield a set of consistent, repeatable, and measureable processes for service delivery to NASA OCIO customers. Within the NASA IT structure, ES&ID accountable for:

- a. Service Strategy direction on how to design, develop and implement ITSM.
- b. Service Design direction for the design and development of IT services and ITSM processes.
- c. Service Operations direction on achieving effectiveness and efficiency in the delivery and support of IT services so as to ensure value for the customer and the IT service providers, including effective coordination across all service providers.
- d. Continuous Service Improvement direction in creating and maintaining value for customers through better design, transition and operation of services.

Within the NASA Office of the CIO, ES&ID is responsible for overseeing EA, SE&I, SEs, SIM, and coordination with the various I³P service offices. Each of these areas will now be further described briefly, with additional detail available in the NASA ESM Concept of Operations document.

2.2.3 Enterprise Architecture (EA)

The OCIO Enterprise Architecture Office is responsible for articulating the mission supporting technologies and operational model to accomplish the IT goals. The EA Office develops baseline architecture and target architecture and their associated sequencing. The EA Office therefore, has responsibility for ensuring that the current-state service catalog evolves to meet future customers' expectations. As part of Service Strategy, the EA Office must work in concert with the center CIOs, SIM, and SEs to ensure that customers' requests and opportunities for service improvement are effectively addressed in its service strategy efforts.

All I³P service architectures will be developed and maintained by NASA enterprise, mission and service domain architects in partnership with the I³P Contractors. These architectures shall

follow enterprise or segment architectural policy, guidance, and standards defined by NASA¹ or the Office of Management and Budget² to achieve NASA's strategic IT target state goals as stated in the NASA Information Resources Management (IRM) Strategic Plan. The outcome of this approach will ensure that IT investments are aligned with NASA's vision for the future and that technology solutions are horizontally integrated across business domains.

In order to achieve viable service architectures, it is imperative that NASA and the I³P contractors collaborate on the analysis of emerging technologies, NASA requirements, and the as-is environment. The result of this collaboration shall be an innovative to-be state, identification of gaps between the as-is and to-be states, and a transition strategy for each service area that will position NASA and the I³P contractors for success.

Each service architecture shall address the service, systems and components (see Figure 4) required to provide the specific service and ensure integration with the other service architectures and the NASA enterprise architecture.

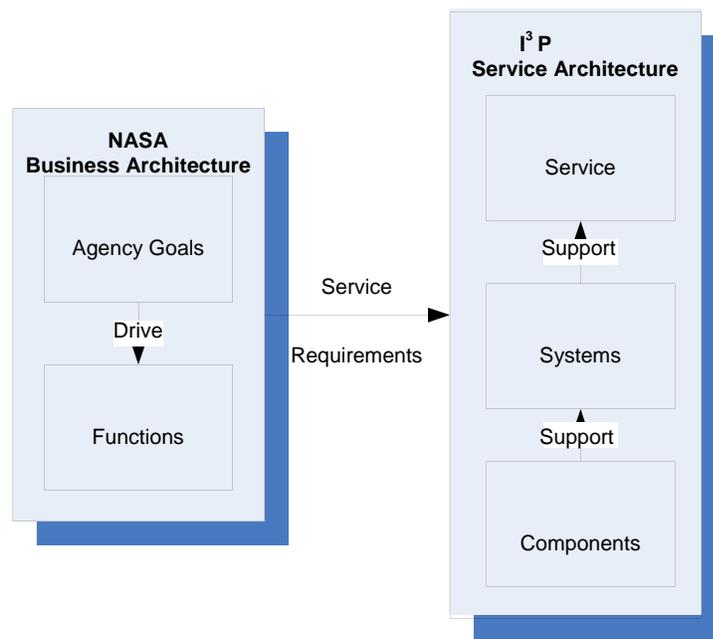


Figure 4: NASA Business and Service Architectures

2.2.4 Systems Engineering and Integration (SE&I)

The OCIO ES&ID organization's SE&I component is accountable for the design of new services including the development of cost estimates associated with these new offerings. The SE&I

¹ Examples include NASA NDP/NPR 2830.1 EA Policy, NASA-STD-2804 Minimum Interoperability Software Suite, and NASA-STD-2805 Minimum Hardware Configurations.

² Examples include the Federal Enterprise Architecture Framework (FEAF), FEA Core, Business Service, and Enterprise Service Segments, and the [Practical Guide to Federal Service Oriented Architecture \(PGFSOA\) v1.1](#)

group also ensures that new and existing services are translated into the NASA technical reference model (TRM) and that all changes to the NASA enterprise IT environment are managed through the appropriate change advisory boards (CABs). These engineering and integration functions also include the establishment of service configuration and performance expectations, reflected in appropriate performance definitions, service metrics and evaluation criteria. Under the ESM concept, the SE&I group is responsible for risk assessments and impact analyses associated with the delivery of existing and new enterprise services. Finally, the SE&I group is responsible for the coordinated deployment of new and updated services.

2.2.5 Service Executives (SEs)

Service Executives are the actual service owners for the respective I³P services for which they have responsibility. In this role as service owners, the SEs are accountable for the configuration of services and the vetting of these services through the appropriate change advisory and control boards within the Agency. SE's are responsible for the development of their specific service strategies and the budgetary requirements to implement these strategies if approved. In order to effectively carry out their responsibilities, each SE must actively engage the NASA user community. This customer relationship management function is essential in identifying issues and gaps in current service delivery to support the development of strategies that will enable continuous service improvement.

Each SE also handles contract performance escalation management in those situations where an issue cannot be resolved at the service office level, or when an issue may span multiple enterprise services and resolution requires coordination at the ESM level. In addition, managing particularly high-impact service issues that impact day-to-day performance will also be escalated to the SE for communication and possible action. Finally, the SE is responsible for collaborating with the service office(s) responsible for the day-to-day management of service delivery to define Service Office Manager (SOM) objectives and milestones.

2.2.6 Service Integration Management (SIM)

The Service Integration Manager is responsible for process architecture and design leading to the implementation of ITIL best practices across the enterprise. The SIM will provide support for designing and implementing the NASA ITIL processes and instituting formal ITSM within NASA. The purpose of the SIM is to improve the effectiveness and efficiency of NASA IT operations through the design, implementation, and operations of standardized ITSM practices. Primary functions of the SIM include:

- a. Support strategic planning associated with defining and scoping the future ITIL-aligned Service organization.
- b. Direct and coordinate implementation of the strategic plan.
- c. Provide Continuous Service Improvement and ITIL process management for NASA's IT organization.

The SIM will also provide ESD oversight and integration, along with the integration of performance metrics across all enterprise services. These metrics provided through ESD systems, Contractor deliverables, and customer surveys will be used by the SIM to obtain a ‘big-picture’ view of service performance, leading to service improvement recommendations. Additional information about the ESD is provided in the following section.

2.2.7 Enterprise Service Desk

The mission of the ESD is to be the Single Point of Contact (SPOC) for Enterprise Services support, handling incidents and requests, and providing an interface for activities such as changes, problems, configuration, releases, service levels and IT Service Continuity Management. The importance of the ESD as a SPOC is to provide a consistent interface to the end-user community, which is a critical element of the business’ determination of how well NASA IT is performing its job – one of the success criteria of the I³P program.

The primary priorities of the ESD are:

- a. To manage customer expectations by identifying and communicating I³P services to customers. Route customers to the appropriate point of contact for those services not provided directly by the ESD or an I³P service provider.
- b. To return the customer to normal operations within SLA requirements and specifications.
- c. To continuously improve service performance.
- d. To perform consistent workflow, enabling service request escalations across disparate IT infrastructure contracts.
- e. To provide reliable communications coordination for Enterprise Service outages.
- f. To collect, consolidate, analyze, and report performance metrics across the independent IT service providers for Enterprise Services provided to customers.
- g. To provide the SIM with accurate and appropriate data that enables responsible operational decisions.
- h. To leverage existing NASA infrastructure to reduce costs.
- i. To provide integrated service support interfacing to functional areas of Procurement, Finance and Human Resources.

2.2.8 Service Offices

Located at each of the sites hosting an I³P service contract, Service Offices are accountable for the day-to-day management and delivery of the enterprise services that they manage. Service Offices are expected to coordinate across SOMs, Contracting Officer’s Technical Representatives (COTRs) and Contracting Officers (COs) to ensure the effective delivery of services across the Agency. While these offices are physically located at and managed by specific Centers, they perform an Agency function.

The Service Offices are also responsible for the management and synthesis of I³P contract service performance and financial information, and communication of this information through the SIM and the appropriate SE. In terms of communication, the Service Office provides information to the Agency CIO, SEs, Center Subject Matter Experts (SMEs), SIM, and to the Center and Mission Directorate CIOs to ensure that all levels of the NASA organization remain informed regarding important performance or service delivery issues.

Service Offices manage the day-to-day financial transactions and issues associated with the services they manage, and will escalate complex contract and performance issues as required. Service Offices will work closely with the I³P service providers to manage technical issues as well as to ensure that contractual service levels are consistently being achieved.

SOMs are responsible for each specific IT service contract under the I³P services umbrella. They are the coordinator and Point of Contact (POC) for a specific service offering e.g. LAN services as opposed to WAN services. They are accountable for adherence to the day-to-day operational parameters for performance of the service as defined in the SLAs, and facilitate service operation activities. The SOM performs oversight of service supplier activities (contractor oversight) and communicates IT service performance issues to the SE. They provide customer relationship management support to the CIOs relative to Enterprise (Agency) services.

In order to provide a coordinated and consolidated technical picture of the individual I³P contracts, each Service Office will designate an Integration Lead (SOIL). The SOIL supports the SE and SIM offices ensuring contracted service providers across the Centers are working in accordance with (and to established) Agency standards, regulations, processes and procedures. SOILs work with peer SOILs and Center Integration Leads (CILs) to ensure integration across contracts for projects and processes and support service performance monitoring and reporting to SOMs, SEs and SIM in regards to individual contracts.

2.2.9 Center CIO

With the implementation of I³P and the resulting shift from local to enterprise delivery of some services, the role of the Center CIO and the staff they manage is evolving. As the roles and responsibilities shift to support the NASA IT strategy, the Center CIOs maintain significant responsibility for local service delivery, and have acquired new roles associated with enterprise service strategy and delivery. These roles and responsibilities are described in the following section.

Relative to local service delivery, Center CIOs are accountable for the day-to-day delivery of locally-provided IT services that are not provisioned as part of one of the Agency service contracts. This includes all aspects of managing these services including service design, implementation, monitoring, security, and continuous improvement. The Center CIO is also accountable for ensuring that any locally-provided services align with Agency strategy and policy. Center CIOs ensure the provisioning of local infrastructure to enable effective and efficient delivery of enterprise services while overseeing the Center's overall IT portfolio and managing demand for both local and enterprise services. The CIO is ultimately responsible for

customer relationship management across all organizations at the Center, and ensures that requirements, issues, and concerns regarding IT services are captured, understood, and addressed. In terms of strategic leadership, each CIO is a member of the Center's executive leadership team responsible for solving business problems through the application of innovative IT solutions. In a similar manner, each Center CIO is a member of the Agency IT Management Board (ITMB) and is responsible for setting the Agency's strategic direction relative to information and information technology.

Center CIOs also have significant responsibility relative to enterprise service delivery. Because the Agency has such a highly-skilled IT workforce spread across all Centers, each CIO will identify SMEs to support each of the enterprise services at their respective Center. In addition to these SMEs, a CIL will be identified to coordinate and manage issues involving integration across multiple services. These SMEs and CILs will work closely with the associated SEs, Service Offices and the SIM to effectively implement enterprise delivery of key services. As additional requirements are identified for new or improved services, Centers CIOs will also identify and provide technical experts to participate on Agency-level technical and architectural teams. Finally, the CIO will serve as the voice of the Center customers to Agency service providers while monitoring service integration and performance issues locally and participating in continuous service improvement efforts.

Those CIOs whose Centers host Service Offices have additional responsibilities including working with the Agency CIO to determine the resources required to manage and execute the project as agreed to with the Agency OCIO. Host Center CIOs also work with the appropriate SE(s) to define performance objectives for local staff members who are supporting enterprise service delivery and then manage the service office staff to ensure that the Center delivers on these Agency commitments.

2.2.10 Mission Directorate CIOs

Similar to Center CIOs, Mission Directorate CIOs represent the requirements of their respective missions, which cut across all NASA Centers. The Mission Directorate CIO has a unique understanding of the mission requirements related to information and information technology and works with Center and Agency IT Service providers to ensure that these requirements are satisfied. Each Mission Directorate CIO is a member of the ITMB and is responsible for helping to set the Agency's IT strategic direction and provides a critical customer relationship management function as the voice of the mission customer regarding all aspects of NASA IT services.

2.3 NASA IT Governance Process and Structure

Contractors shall adhere to the NASA OCIO governance strategy and framework as outlined in this section and discussed in greater detail within each respective I³P contract and associated performance work statements.

In conformance with NASA's IT governance process, contractors shall:

- a. Support NASA’s Mission via ongoing alignment and management of NASA’s IT assets and processes with its mission requirements and strategic initiatives.
- b. Identify potential areas of investment redundancy and opportunities for consolidation, rationalization and cost efficiency.
- c. Support master planning at the Agency level to increase visibility of and better prioritize investments.

NASA’s approach to IT governance is a structured, decision-oriented model that has critical linkages to NPR 7120.7 NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements and other NASA IT management processes such as capital planning and investment, IT security planning, and EA as defined in various IT-related policy documents (NPR 2800.1, Managing Information Technology, NPR 2810.1 Security of Information Technology, and NPR 2830.1 NASA Enterprise Architecture Procedures).

NASA’s IT environment is organized into three major areas, or portfolios:

- a. IT infrastructure services
- b. IT applications
- c. Highly-specialized IT, such as technology that supports real time control systems and on-board avionics

While some cross-cutting IT processes, such as IT security, apply to all portfolios, the scope of IT governance described in this section applies primarily to IT infrastructure and application services.

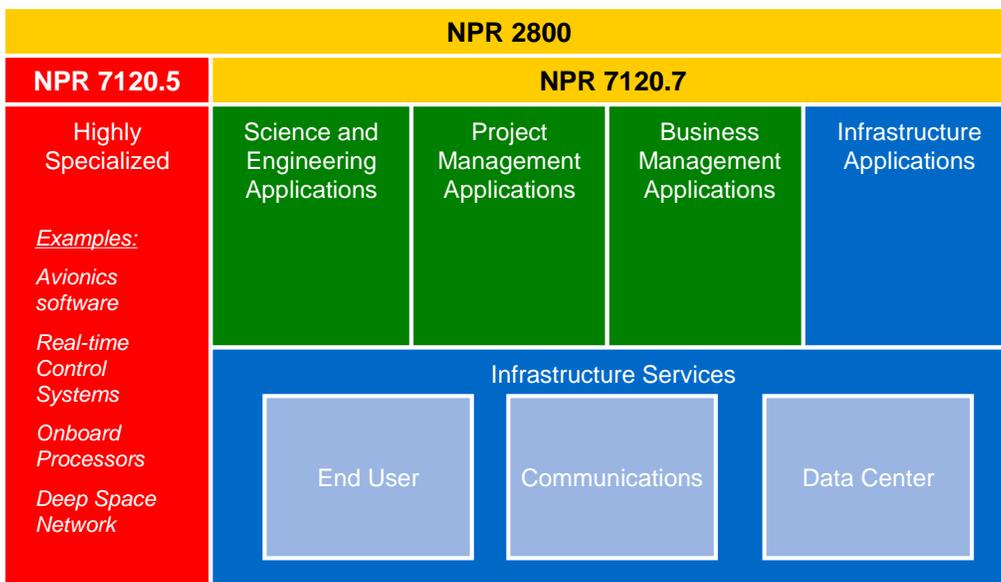


Figure 5: IT Portfolios and Governing Policies

To address the wide-ranging decisions which are likely to occur throughout the life cycle of the IP contracts, at an Agency level NASA employs a board model where each board has a clear set of responsibilities as well as interfaces to the other governing bodies. This governance model shown below provides complete coverage of the life cycle of an IT investment from the initial decision to fund a proposed investment to the oversight of its implementation and operations and subsequent decommissioning. Each of these life cycle phases has associated with it unique milestones and metrics that require different activities and therefore different board oversight.

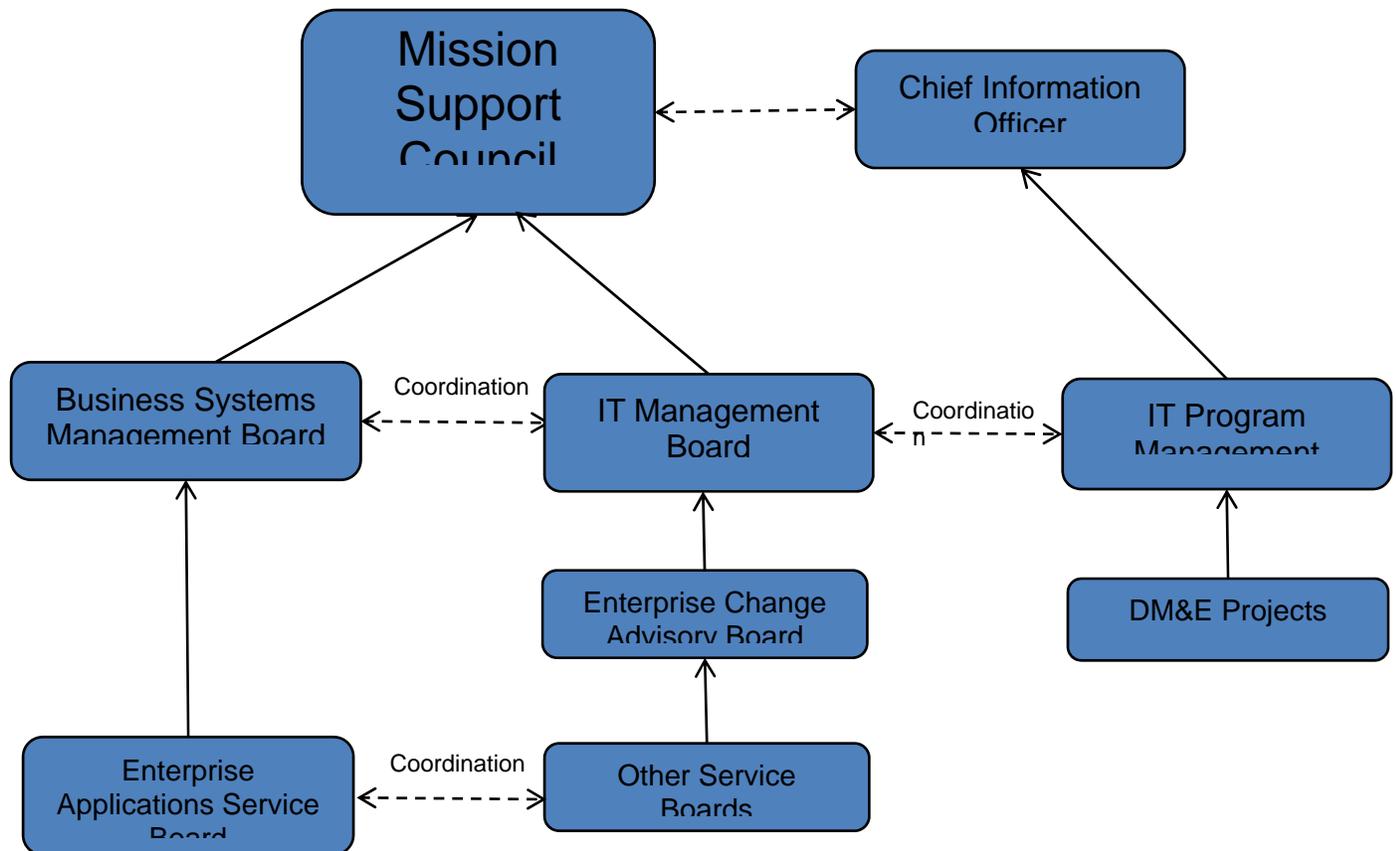


Figure 6: NASA IT Governance Structure

The scope and purview of each NASA board is further defined as follows:

- a. **Mission Support Council (MSC)** – Decisions regarding NASA strategy and related investments (prioritization and selection), and NASA-wide policies/processes. Members include senior executives from Mission Directorates, Mission Support Offices, and Centers.
- b. **Business Systems Management Board (BSMB)** – Decisions regarding strategy and related investments for the Agency Business Systems portfolio. Members include senior level stakeholders from the functional business areas.

- c. **IT Management Board (ITMB)** – Decisions regarding strategy and related investments for the I3P portfolio of services. Decisions regarding operational performance and issues related to performance. Members include the Agency OCIO Division Directors, Center and Mission Directorate CIOs.
- d. **IT Project Management Board (IT PMB)** – Decisions regarding application and infrastructure projects to ensure that investments approved by the ITMB, BSMB, or MSC stay on track during formulation, design and implementation. Members include the Deputy CIO,, Enterprise Architect, and representatives from Mission Directorates, Mission Support and Centers.
- e. **Enterprise Change Advisory Board (E-CAB)** – Decisions regarding technical integration and service integration across Service areas. Members include the Technical Integration Manager, Service Integration Manager, CTO, Enterprise Architect, and Service Executives.

The governance structure described above operates at the Agency level and addresses major IT investments that cross Center and program boundaries.

NASA’s approach to IT governance reflects the latest in industry best practices and is grounded in the strategic management principles for governing, managing, implementing, monitoring, and controlling the work of the Agency as set forth in the Strategic Management and Governance Handbook, NPD 1000.0.

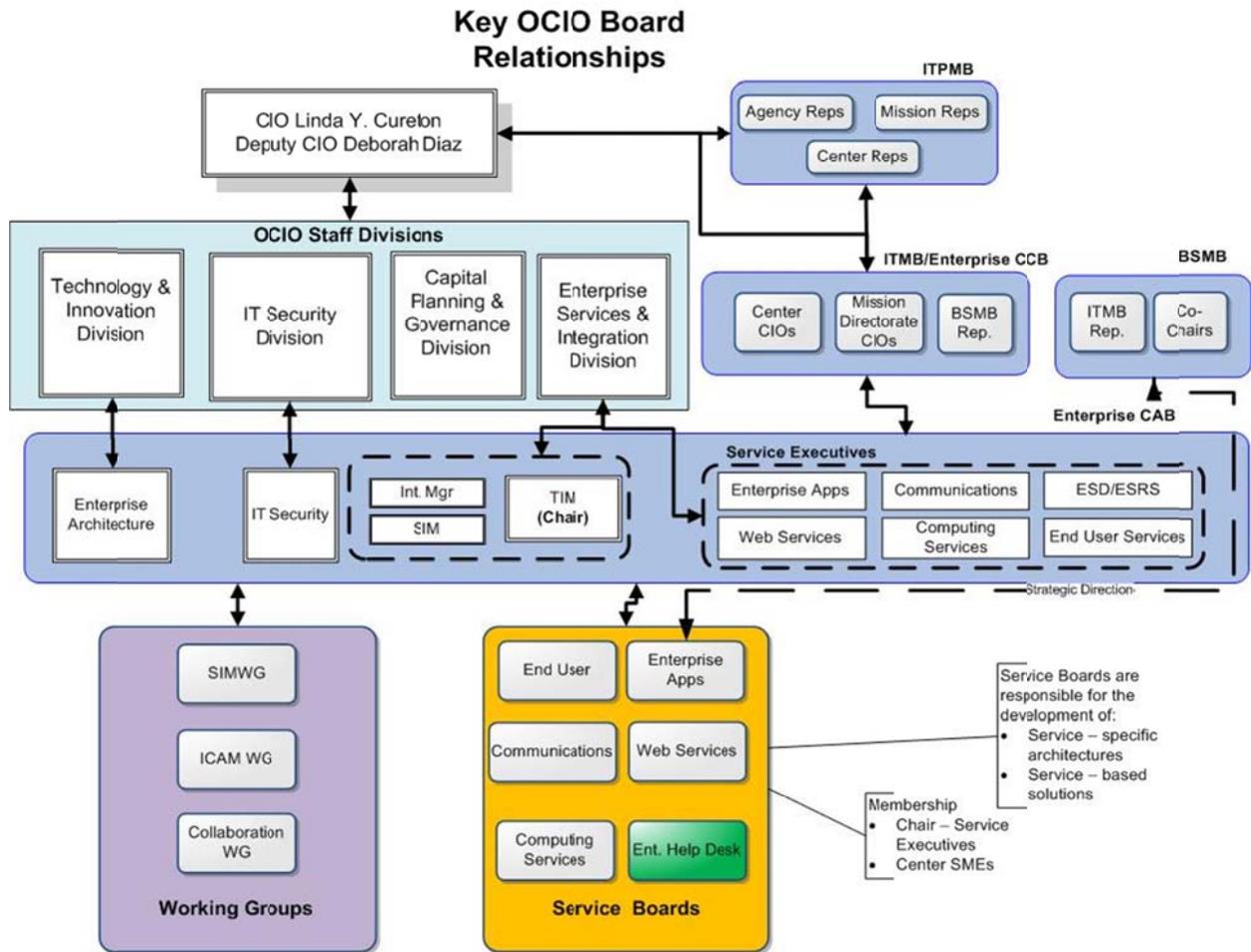


Figure 7: I3P Governance Structure

The I3P governance structure is depicted in Figure 7. Each service area has a Service Board, which is authorized to make decisions within the scope of the service. Decisions that impact multiple service areas, have a high level of risk, and/or high visibility to customers and stakeholders, are made at the E-CAB and ITMB level.

Each Service Board may have one or more working groups which are established to provide analysis and recommendations within their scope to the cognizant Service Board. Working Groups are formally chartered and approved by the E-CAB and ITMB. Communities of interest may also be established to foster the exchange of ideas. Communities of interest have no formal decisional authority. While no formal approval is required for a Community of Interest to be established, a Board or Working Group may sponsor a Community of Interest.

Centers are also implementing local governance structures that, while customized to the unique organizational environment and culture at each Center, conform in spirit to the I³P governance structure and enable Center-specific investments to be addressed. Notwithstanding the existence

of Agency or Center-specific governance structures, it is expected that changes will need to be made over the life of the I³P Acquisition to address the full IT life cycle as described in NPR 7120.7.

2.4 Contractor Responsibilities

In addition to working with NASA in concert with Agency level governance processes and structures, contractors must work within other complementary contract and relationship management mechanisms as defined within each contract.

These additional governance processes and structures relate to the Contract administration and management activities that are specific to the individual NASA Centers responsible for procuring and overseeing delivery and performance as defined in the individual I³P performance work statements. Contractors should refer to the individual contracts for details of these complementary governance processes and structures.

The I³P contractors shall work closely with the ESM and SIM organizations to ensure adherence to NASA standard IT processes, monitor compliance, drive continuous service improvement and coordinate service operations to achieve an effective and efficient multi-sourced IT environment in support of Agency requirements. I³P contractors shall work closely with Center CIOs to understand requirements and to work local service delivery issues.

While specific requirements are captured in the cross-functional ITIL process requirements, an overview of these responsibilities associated with supporting ESM and SIM activities is provided below.

- a. **Policies and Procedures:** Contractors shall support SIM identification, definition and implementation of changes to Agency IT policies and procedures that improve service delivery, streamline operations and reduce costs. Contractors shall do this through the identification and application of Industry best practices, methodologies and tools within the NASA ITSM environment.
- b. **Strategy Development:** Contractors shall participate in the Agency's annual portfolio management process by providing design, cost, benefit, risk and other information necessary for the ESM to prioritize a list of projects aligned with user requirements.
- c. **Process Development:** Contractors shall support service integration by defining and implementing service delivery processes and procedures identified in the Agency's Cross Functional Statement of Work and other contractor processes that are complementary to NASA's ITIL v3 aligned processes.

- d. **Process Interface:** Contractors shall ensure that cross-contract service integration and delivery touch-points are aligned with both Government and other I³P contractors so that seamless service delivery and management occurs.
- e. **Compliance Monitoring:** Contractors shall support the Agency in monitoring of service delivery to the end customer. Such monitoring shall include, but not necessarily be limited to, process quality assurance, escalating and resolving issues (inclusive of cross-contract/vendor), monitoring production control, and integrating actions, communications and exchanges of service supporting data activities across I³P contractors to ensure customer support requirements are met (i.e. SLAs are met).
- f. **Operations Coordination:** Contractors shall support NASA's management of the multi-sourcing environment by supporting coordination and oversight of operations.
- g. **Continuous Service Improvement:** Contractors shall identify, define and implement continuous service improvement activities. Contractors shall benchmark projects as defined by SIM's continuous improvement processes.

2.5 Relationship Management

Contractors shall follow a robust Governance model to partner with NASA and manage both services delivery and contract performance. Relationship management focuses on actively managing relationships with NASA customers, stakeholders and other contractors who are integral to the delivery of integrated ITSM under I³P. All relationship management practices are ongoing and entail the following set of activities:

- a. Managing interactions with NASA to ensure their effectiveness and to capture critical service level information.
- b. Formally managing relationships with NASA customers and contractors by establishing relationship objectives and tracking performance of those objectives.
- c. Selecting suppliers and partners based on their ability to meet NASA business requirements.
- d. Obtaining feedback from NASA stakeholders, including employees, and contractors on the nature and quality of key service and delivery relationships.
- e. Proactively identifying opportunities that will provide additional value to NASA.

The NASA IT governance structure is designed to encourage collaborative discussion of issues and ideas critical to the ongoing success of I³P and related IT transformation. As detailed in the individual I³P contracts, each party shall designate an individual to serve as a relationship manager who will be that party's SPOC for all matters relating to the outsourcing contract. The contractor's relationship manager shall:

- a. Be knowledgeable about NASA's I³P service requirements and each of the contractor's and its subcontractors/partners products and services.
- b. Be experienced at running IT systems and networks, as they relate to the provision of services for which they are contracted, of similar size to NASA's current and anticipated business requirements.
- c. Have overall responsibility for directing all of the contractor's activities.
- d. Be assigned to the NASA account for a significant portion of the contract term.

Contractors shall assist and contribute to setting the strategy and processes concerning NASA's technology and use over the life of each I³P contract. Contractors shall continually evaluate the technical environment, identifying potential enhancements that will reduce overall costs while delivering high quality and high availability services across the Agency.

3 Service Coordination and Collaboration

3.1 Introduction and Overview

The I³P acquisitions involve more than management of independent sourcing agreements. The effort will require coordination, collaboration and integrated management of key processes among contractors and across contract boundaries.

It is in the coordination of multiple contractors where the management of I³P services differs from the management of independent IT contracts. Coordination of services across these multiple contracts involves coordinated management of four sets of relationships:

- a. Between NASA end users and individual Contractors;
- b. Between NASA leadership and individual Contractors;
- c. Between NASA's internal client facing and support organizations required to deliver IT services; and,
- d. Between the I³P Contractors.

It is important that contractors work with NASA and with each other to establish and execute common management approaches and procedures to ensure that services are provided effectively and efficiently across the enterprise regardless of contractual boundaries.

3.2 Service Delivery Coordination and Collaboration

NASA recognizes the interdependencies of internal and external relationships and expects contractors to work with the Agency and among themselves to proactively manage those interdependencies to support the overall mission, vision, and objectives of the OCIO.

Contractors shall ensure that processes and procedures are established and maintained to support service coordination and collaboration with NASA and other I³P contractors in the following delivery areas.

- a. **Service Delivery Strategy** – Proactive management of NASA's service delivery strategy assumes that business conditions and customer requirements change over time requiring that initial strategies adapt to changes as they occur. By working with NASA to modify goals, priorities, policies and procedures as they affect one or more of the sourcing relationships, I³P Contractors shall continuously improve how services are delivered to meet end user needs.
- b. **Service Delivery Responsibility** – Management of service delivery can be complex when multiple contractors are responsible for IT service delivery. I³P contractors shall know and understand who is responsible for each service delivery task, where touch-points or hand-offs are and how their responsibilities change as end-to-end service delivery crosses contract boundaries. Process flows, cross-functional and

contract-specific performance work statement elements all play a part in defining roles and responsibilities where coordination is required to ensure continuity of service and operations.

- c. **Service Delivery Integration** – Coordination and collaboration across multiple contractors demands that multiple contractors work together and, as needed, shall co-develop processes that define the rules of engagement between various parties as well as how to manage the many touch-points and interface requirements between Contractors, end-users, and internal NASA organizational entities. Proactive management of delivery integration not only ensures that everything that needs to get done is accomplished, but that contractors work together to identify, create and document any new procedures necessary to ensure seamless service delivery to NASA customers over time.
- d. **Service Delivery Performance Assessment** – Proactive management of service performance processes are focused on verifying the facts of the relationship through coordination and cooperation among NASA I³P and other supporting Contractors. The contractor shall support service level evaluations, operational or security assessments, financial audits, and other assessments required by the OCIO in response to changing business conditions or governance requirements.
- e. **Delivery Communication** – Proactive management of communications and feedback requires the transmission of information generated throughout service creation and service delivery processes. Contractor reporting shall address end-to-end service delivery requirements, ensure the right information is available to the right people at the right time, facilitate operational excellence and support NASA's decision making requirements.

NASA's ESM will be the focal point to ensure seamless IT service delivery.

4 NASA IT Infrastructure Library (ITIL) Version 3 Approach

4.1 Introduction and Overview

In support of the Agency CIO's vision for I³P, various IT operational models were analyzed and the ITIL version 3.0 framework was selected. Applicable ITIL v3 processes have been identified and prioritized for development and implementation within the NASA IT environment. It is recognized by the NASA ITMB that a common and consistent Agency-wide IT organizational management structure is required to support centralized, Agency-provided IT services. The new ITIL processes will be designed to enable and support IT governance via performance metrics. The adoption of a standardized framework that includes a common terminology and process set will be an integral part of all I³P support contracts. ITIL version 3.0 focuses on Service Management and seeks to align IT with business objectives. ITIL version 3.0 outlines a set of integrated processes that encompass the full scope of the IT service lifecycle. By defining a common set of ITIL version 3.0-aligned processes that are applied across all I³P contracts, NASA strives to attain maximum efficiencies while ensuring seamless, integrated services for IT customers.

Adoption of ITIL will enable NASA's mission by:

- a. Better integrating the Agency's people, processes, and information.
- b. Improving security.
- c. Achieving efficiencies.

4.2 Implementation Plan and Scope for I³P

NASA has developed an implementation plan and roadmap based on the introduction of ITIL v3 as the Agency's process framework in support of I³P. Prospective service providers shall have documented, repeatable ITIL processes with relevant metrics reporting capabilities. NASA requires prospective service providers to engage and align with NASA's IT organization and NASA's ITIL processes.

NASA's approach is based on a phased implementation of ITIL processes. Activities in support of this implementation have been prioritized according to the following Government criteria:

- a. Processes having greater relative importance to I³P Acquisition Governance and Strategy.
- b. Processes that require extensive, multiple vendor coordination and integration.
- c. Processes that industry experience and best practice suggest should be addressed earlier in an ITIL implementation.

Twelve (12) of the ITIL v3 processes have been grouped into either Primary or Secondary implementation priorities.

Five (5) of these processes have been identified as primary implementation priorities. They include:

- a. Change Management
- b. Incident Management
- c. Request Fulfillment
- d. Problem Management
- e. IT Service Level Management and IT Service Catalog Management*

*Service level management and Service Catalog Management processes were identified early as potential process development/refinement opportunities. Although preliminary documentation for those processes was developed, it was decided that an IT Configuration Management development/refinement effort should take priority and that Service Level Management and Service Catalog Management development/refinement efforts will be conducted along with second phase of process development/refinement events.

These five (5) processes are considered primary I³P implementation priorities for the following reasons:

- a. They are foundational processes in that many of the remaining ITIL processes depend on them.
- b. They have strong ties to the ESD that was established in support of the I³P acquisition and cross all the service contracts.
- c. They tend to be ticket-management-heavy processes central to efficient and effective resolution of service interruptions and/or restoration of services to end-users.
- d. There is stronger familiarity of these processes among the NASA technology groups.
- e. There are significant opportunities associated with these processes for quick wins and/or accelerated achievement of I³P objectives.

Seven (7) of the ITIL processes have been identified by NASA as secondary I³P implementation priorities. They include:

- a. Service Asset and Configuration Management
- b. Release and Deployment Management
- c. Capacity Management
- d. Strategy Generation
- e. Service Portfolio Management
- f. Service Catalog Management
- g. Supplier Management

In addition, Access Management has been identified as a process that, while implemented as part of ICAM Services, is targeted for closer integration with the Request Fulfillment process and tools implemented by the ESD.

These seven processes were targeted as secondary implementation priorities because:

- a. Several (e.g. Release and Deployment Management and Capacity Management) require that Change Management be in place and operational prior to their implementation.
- b. Several (Service Asset & Configuration Management and Service Catalog Management) require significant set-up and coordination across the I³P contracts and delivery teams.
- c. Several (Service Portfolio Management, Supplier Management and Strategy Generation) are critical to establishing strategic direction for I³P and create momentum behind its execution.

The remaining fifteen (15) ITIL v3 processes are considered tertiary implementation priorities by NASA. Selection and prioritization of these for implementation will be evaluated and determined as the NASA ITIL framework matures. They include:

- a. Demand Management
- b. IT Financial Management
- c. Information Security Management
- d. Availability Management
- e. Service Continuity Management
- f. Validation and Testing
- g. Transition Planning and Support
- h. Knowledge Management
- i. Event Management
- j. Access Management
- k. Operations Management
- l. Service Evaluation
- m. Service Improvement
- n. Service Reporting
- o. Service Measurement

In summary, NASA's introduction of ITIL v3 processes in support of the Agency's I³P Acquisition supports the Agency's goals of transforming NASA's current environment to a more highly integrated IT Service Management environment.

4.3 NASA Defined ITIL v3 Process Requirements

I³P contractors shall define and implement service delivery processes and procedures that are consistent with both individual service provider-specific and cross-functional performance work statement elements.

I³P contractors shall implement processes and procedures that are consistent and complementary to NASA ITIL v3 aligned processes. All Contractor-developed processes and procedures necessary for the execution of the service delivery requirement are considered non-proprietary and shall be provided to the Government upon request.

I³P Contractor interfaces associated with NASA IT services shall support NASA's ITIL process requirements as detailed in the cross-functional PWS elements, as well as any standards as identified in the Government process and policy documents associated with each NASA IT process.

Contractors shall actively participate in supporting changes to NASA process and policy documents. Changes to NASA process and policy documents will be managed by the Office of the Chief Information Officer.

The Government Incident Management system operated by the ESD for tracking the status of Problems, Incidents, changes, etc. will be the primary system of record used by the Government to track the status and completion of actions associated with these processes.

5 I³P Common Architecture Components

5.1 Introduction and Overview

NASA's strategic approach to the management of IT infrastructure is to provide Enterprise-wide infrastructure services to maximize efficiency, improve IT security, and provide the best possible user experience. These infrastructure services have been defined into six (6) different portfolios:

- a. End-User Services
- b. Network and Communications Services
- c. Enterprise Compute Services
- d. Enterprise Applications
- e. Web Services
- f. Identity, Credential, and Access Management (ICAM) Services

Each of these portfolios provides a specific set of component services which comprise part of the NASA Enterprise Architecture as reflected in the NASA Enterprise Service Catalog. Common across these portfolio areas is the requirement for a TIER-0/1 ESD and an Enterprise Service Request System (ESRS). Finally, to reduce redundancy and promote interoperability and collaboration, applications within the NASA environment must be integrated through the NASA Application Portfolio Management process. Each of these elements of the NASA environment is further described below.

5.2 NASA Enterprise Architecture Repository

In support of the continual evolution of NASA EA, a knowledge base known as the NASA Enterprise Architecture Repository (NEAR) is being developed. The NEAR will support the alignment of IT goals, services, systems, components, and standards with Center, Mission Directorate, and Agency goals, while enabling more effective management of current assets and improved planning for new investments. In addition the NEAR will reduce information redundancy and improve data consistency while at the same time increasing flexibility and agility to provide a vision of the future state of the IT environment.

NASA's services are documented through a line-of-sight approach, i.e., from goals to functions to services to systems to components, with components as the lowest level of technical representation.

The NEAR will be hosted within the NASA IT environment. The NEAR will interface with repositories in IT Service areas and the Configuration Management Database (CMDB) at ESD as needed to provide authoritative data, especially at the system and component level.

Basic definitions of I3P services maintained in the Enterprise Service Request System (ESRS) will be provided to the NEAR from the NSSC via an electronic interface developed in accordance with the NEAR Interface Definition Specification (IDS).

5.3 NASA Enterprise Service Desk

The ESD is a foundational component of NASA's I³P strategy for delivery of core IT infrastructure services. The ESD is located at and administered by NASA Shared Services Center (NSSC). The ESD serves as the single point of contact for Enterprise Services support providing a unified interface between the I³P customers and the I³P service providers (i.e. I³P contracts – ACES, NICS, EAST, and WESTPRIME). The primary functions provided by the ESD include management of the IT Service Management (ITSM) software suite and ESD/ESRS CMDB, Tier 1 and Tier 0 incident management, service request processing, enterprise notification of planned/unplanned I³P infrastructure outages, I³P SLA metrics collection and reporting using the ITSM suite of tools, and integration support to the SIM and I³P contractors for service continuity.

The ESD utilizes the ITIL v3 framework and associated processes common to all I³P service providers as outlined in the cross-functional PWS elements defined in this document. ITIL processes are divided between Service Delivery and Service Support with the ESD serving as the primary point of contact between IT and users of IT services. The SIM organization in the OCIO ES&I Division is responsible for the definition and development of all NASA ITIL v3 processes. Service Support provides for implementation of operational processes and day-to-day management of the environment. Service Delivery is associated with the tactical processes and planning processes.

I³P contractors shall interface with the ESD for a number of activities. These include (but are not limited to):

- a. Building interfaces between the ESD Remedy system and the Contractor system. If the Contractor chooses to use the ESD's Remedy system, the Contractor is responsible for all integration work with the NSSC.
- b. Resolving, statusing, and closing escalated incidents that cannot be resolved at the Tier 1 or Tier 0 level.
- c. Providing and updating knowledge articles used by the ESD call agents to resolve and/or triage I3P Incidents that pertain to their specific contract service.
- d. Providing notifications and community/organization lists for dissemination of planned and unplanned notices, service configuration changes affecting customers and/or other I3P Contractors.
 1. Providing status related to incident/problem resolution for those incidents assigned to their I³P contract.
 2. Providing information as to any configuration changes related to I³P service provisioning assigned to their I³P contract.

3. Providing and updating knowledge articles for the Tier 0 self-service I³P Web site for commonly identified incidents and or user self service activities (DRD 1294CF-014).
4. Providing a POC for ESD-to-I³P-Contractor escalation processing of incidents/problem/service requests for both normal business and after hours.
5. Providing initial load of Configuration Items (CIs) to the ESD/ESRS CMDB during the transition period of the Contractor or in accordance with a specific contract Service Asset and Configuration Management Plan (DRD 1294CF-003).
6. Providing updates to the ESD/ESRS CMDB CIs e.g., for those items that were modified during the resolution of an incident or changed as a result of a scheduled refresh.

Important ESD reference information can be found in the following documents:

- a. Enterprise Service Desk Concept of Operations
- b. Enterprise Service Desk Performance Work Statement and associated Appendices
- c. ESD/ESRS Interface Definition Specification
- d. ESD/ESRS 7120.7 Program/Project Systems Requirements documents

These documents and other references are found at http://i3p.nasa.gov/document_file_home.cfm

5.4 NASA Enterprise Service Request System

To facilitate a seamless user experience, another element of the I³P common architecture is the NASA ESRS. The ESRS includes:

- a. A user-friendly, customer-facing interface to order all I³P-provided services.
- b. The ability to provide pricing for services offered.
- c. Workflows to enable purchase authorization and verification of available funding.
- d. Workflows to enable the efficient distribution of component orders to the appropriate I³P service provider(s).
- e. The ability for users to track the status of all orders via the Tier 0 web site.
- f. A reporting capability to enable NASA leadership to monitor SLA performance and continuously improve service delivery.
- g. Integration with the ESD to facilitate the aggregation of critical performance parameters with other I³P metrics.

The ESRS utilizes the same IT Service Management software as the ESD ticket system (BMC/Remedy 7.5) and will support the ITIL service request processes detailed in the cross-

functional section of this PWS. Services and their attributes offered through the ESRS are defined and obtained from a web-based user interface that initiates workflow within Remedy.

I³P contractors shall interface with the ESRS for a number of activities. These include:

- a. Building interfaces between the ESRS Remedy system and the Contractor system during the transition period. If the Contractor chooses to use the ESD's Remedy system, the Contractor is responsible for all integration work with the NSSC.
- b. Fulfilling, statusing, and closing service requests and updating CIs in the ESD/ESRS CMDB.
- c. Providing a POC for ESRS-to-I³P-Contractor interfacing/integration for both normal business and after-hours incident/problem resolution/service fulfillment.
- d. Populating and updating I³P services in the ESRS in accordance with the Remedy system requirements. The contractor shall carry this out via a web-based user interface that initiates workflow within Remedy. Contractor employees shall gain access to the system by requesting this specific role be provisioned using NAMS.

I³P contractors receive I³P service requests from the ESRS for fulfillment. The specific interface definition between the ESRS and I³P contracts are defined in the ESD/ESRS Interface Definition Specification.

The ESRS is operational and can support the phase-in of all I³P contracts. Contractors shall plan for a period of integration and testing to integrate any Contractor order fulfillment systems with the ESRS.

Important ESRS reference information can be found in the following documents:

- a. Enterprise Service Desk Concept of Operations
- b. Enterprise Service Desk Performance Work Statement and associated Appendices
- c. ESD/ESRS Interface Definitions Specification
- d. ESD/ESRS 7120.7 Program/Project Systems Requirements documents

These documents and other references are found at: http://i3p.nasa.gov/document_file_home.cfm

5.5 NASA Application Portfolio Management (APM)

Another critical element of the NASA environment is the management of NASA's Application Portfolios. NASA APM provides a framework that informs and facilitates decision making regarding application investment, development, maintenance, and decommissioning. This is accomplished by providing knowledge about available applications, application business and technical performance, and total cost of ownership.

In order to assist in effectively managing the NASA application landscape, Section 7 of this document includes process requirements associated with the NASA APM initiative.

In addition contractors shall comply with the following:

- a. Provide an annual Application Inventory Cost report as documented in DRD 1294CF-005.
- b. Review the NASA System for Tracking and Registering Applications and Websites (STRAW) to verify if an existing application will satisfactorily fulfill the stated application requirements prior to purchasing or developing a new application/capability and inform the Responsible NASA Official of said existing application(s).
- c. Utilize the documented NASA ITIL process framework to ensure that all new applications being developed and/or entered into service are documented in STRAW and all applications being decommissioned/removed from service are so documented in STRAW.

6 Common Information Technology Security Requirements

6.1 Introduction and Overview

In order to appropriately secure NASA systems and information, the following IT security requirements apply to all I³P Contractors. Where the term “information system” is used this refers to any system that physically or logically is connected to a NASA network, or that stores, processes, or transmits NASA data. Referenced NASA, federal, or IT Security policies or procedures may be downloaded from the NASA IT Security documentation website at <http://itsecurity.nasa.gov/policies/index.html>. Additional IT Security requirements may be contained in each service-specific I³P contract and shall be in addition to the requirements contained in this cross-functional section.

6.2 Common IT Security Requirements

- a. All information systems provided and/or operated under this contract are federal information systems. (A federal information system is defined in NIST SP 800-37, Rev 1 (and subsequent revisions), *Guide for the Security Authorization of Federal Information Systems* and in 40 U.S.C., Sec. 11331, as an information system used or operated by a federal agency, or by a Contractor of a federal agency or by another organization on behalf of a federal agency.) The contractor shall identify an IT Security POC for supporting IT security requirements for each I³P contract. The contractor shall demonstrate compliance with IT information system security requirements by documenting a system security plan (DRD 1294CF-002.) The contractor shall be responsible for meeting the requirements for security authorization, also known as certification and accreditation (C&A), of these information systems, consistent with FIPS 200 and NIST SP 800-37 (Rev 1). A NASA official, determined in accordance with NPR 2810.1, will perform the role of the authorizing official for all such information systems.
 1. The contractor shall use NASA processes, as specified in NASA policy and procedures, to meet the requirements for security authorization of all such information systems.
 2. For all information systems provided under this contract that store, process or transmit NASA data, NASA will determine the system’s FIPS 199 security categorization. For any other information systems provided under this contract or used in performing this contract, NASA will approve the system’s FIPS 199 security category.
 3. The contractor shall ensure that all systems institute information security controls in accordance with NIST SP 800-53.
 4. The contractor shall support all applicable security assessments of each information system. At the discretion of the NASA authorizing official, the contractor shall either perform or provide for the performance of system security assessments, or support independent system security assessments (e.g., third party certification, IG Audits, GAO audits, and self certification), as part of the security authorization and continuous monitoring process.

5. The contractor shall track identified risks and security vulnerabilities for each information system in the NASA System Assessment and Authorization Repository (NSAAR) and remediate vulnerabilities on a schedule as determined by the NASA authorizing official.
6. All required system security documentation shall be entered into the NSAAR.
- b. The contractor shall document their approach to managing information security in an Information Security Management Plan according to DRD 1294CF-001.
- c. Some work performed by the I³P contracts will require access to and/or generation of classified information, work in a secure area, or both, up to the level of Top Secret/Secure Compartmented Information (TS/SCI). See Federal Acquisition Regulation clause 52.204-2 in this contract and DD Form 254 (refer to <http://www.usaid.gov/policy/ads/500/dd254.pdf>), Contract Security Classification Specification, Attachment [Insert the attachment number of the DD Form 254].
 1. The contractor shall ensure that key Contractor IT security personnel have the appropriate security clearances, up to the level of TS/SCI, to receive classified IT security threat information, to implement security controls based on such information, or to support other activities that require access to classified information.
- d. The contractor shall configure and maintain operating system and software on all information systems provided under this contract in accordance with Federal and NASA security configuration policies and guidance.
 1. The contractor shall apply all relevant Federal system and software security configurations, for example, the Federal Desktop Core Configuration, according to NASA guidance.
 2. All information systems shall be patched with all critical patches (as determined by the product vendor or NASA) in accordance with the NASA Organization Defined Values for NIST SP 800-53 Security Controls and subsequent revisions.
 3. In some rare circumstances, the NASA Deputy CIO for IT Security or designee may determine that a particular patch must be applied more urgently. In such cases, all information systems shall be patched in the timeframe specified by the NASA Deputy CIO for IT Security or designee.
 4. System configurations and patching status for all information systems provided under and in support of this contract shall be reported using the NASA patch reporting environment. Each computer shall run up-to-date NASA reporting agent software for automated reporting. For any computers that cannot run the reporting agent software, a NASA-approved waiver must be obtained in accordance with NASA policy and procedures.
- e. All information systems shall be protected by the NASA enterprise anti-malware (including anti-virus, anti-spyware, etc.) solution, which provides automated updates of virus definitions at least once every 24 hours and automated logging and reporting. The NASA enterprise anti-malware solution for desktops and laptops is provided by the ACES contract. For any computer that cannot use the anti-malware solution or for which no anti-malware software exists, a NASA-approved waiver must be obtained in accordance with NASA policy and procedures.
 1. The contractor shall correct or mitigate detected vulnerabilities in accordance with NASA policy, unless directed otherwise by NASA for specific urgent issues.

- f. All information systems provided under this contract or used in support of this contract shall be scanned for vulnerabilities in accordance with NASA policy.
 - 1. The contractor shall make available all information systems located within the NASA network perimeter for network-based vulnerability scanning by NASA. NASA will coordinate scanning activities with the Contractor to the extent possible to ensure that vulnerability scanning creates minimal impact on operations.
 - 2. For all other information systems which process NASA data, the contractor shall report to NASA the results of vulnerability scans and remediation, in accordance with NASA guidance.
- g. For all software developed in support of this contract, the contractor shall follow software security assurance practices to ensure that the software is designed and developed to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources that it uses, controls, and protects.
 - 1. The contractor shall verify that all software developers have been successfully trained in secure programming techniques.
 - 2. The contractor shall perform application security analysis and testing according to the verification requirements of an agreed-upon standard (such as the Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS)).
 - 3. For web applications, the contractor shall ensure that the software shall not include any of the flaws described in the current "OWASP Top Ten Most Critical Web Application Vulnerabilities."
- h. The contractor shall follow NASA IT security incident management procedures in accordance with NASA policies and ensure coordination of its incident response team with the NASA Security Operations Center (SOC). The contractor shall report (DRD 1294CF-012) to the NASA SOC any suspected computer or network security incidents occurring on any systems, in accordance with Federal mandates and NASA policies and procedures. The contractor shall provide all necessary assistance and access to the affected systems so that a detailed investigation can be conducted, problems remedied, and lessons learned documented. Security logs and audit information shall be handled according to evidence preservation procedures.
 - 1. The contractor shall make available logs from any information system to the NASA common logging environment, as requested by the NASA SOC. Electronic raw log data shall be forwarded from the source device to the NASA common logging environment, in accordance with NASA policies, procedures and guidance.
 - 2. The contractor shall report the theft or loss of any device that may contain NASA information, in accordance with NASA incident reporting policy and procedures.
- i. The contractor shall provide a logging environment that centrally captures and retains logs from all information systems provided under this contract.
- j. The contractor shall provide to NASA real-time, electronic access to all asset information and configuration management information for all devices provided under this contract and in support of this contract.

- k. The contractor shall ensure that all individuals who perform tasks as a system administrator, or have authority to perform tasks normally performed by a system administrator, possess knowledge appropriate to those tasks, as demonstrated by holding industry-standard certifications. In addition, system administrators shall not be granted elevated privileges to information systems covered under this contract unless they are authorized and have met the training requirements in accordance with NASA policy.
- l. Prior to deployment of any IT security services, the contractor shall obtain approval from the NASA Deputy CIO for IT Security or designee. Any IT security services provided by the contractor shall be coordinated and integrated with the NASA SOC.
 - 1. Monitoring NASA networks (NASA IP Address space) is an IT security service performed by the NASA SOC (both security monitoring of network traffic and monitoring of system logs) and will be done only by the SOC unless otherwise agreed upon by the I³P Contractor and NASA and documented in the Contractor's Information Security Management Plan.
- m. The contractor shall support the integration of NASA SOC IT security services and technologies into systems provided under this contract and in support of this contract, in accordance with NASA guidance.
- n. The contractor shall work with the NASA OCIO and the incumbent contractor to transfer responsibility for all IT security requirements for existing information systems within the scope of the contract from the incumbent contractor to the successor contractor. The contractor will receive from NASA a list of the applicable information systems.

7 Cross Functional Performance Work Statement Elements

The NASA IT Infrastructure Integration Program (I³P) requires coordination, collaboration, and ultimately co-management of key processes across I³P Service contractors and contract boundaries. To ensure a successful integrated IT service environment across NASA, it is essential that IT service providers adhere to the NASA ITIL framework. The purpose of the following CF-PWS Elements are to consolidate the requirements that must remain consistent across contractor service agreements. The requirements contained in this section are the responsibilities of the contractor or contractors associated with the Cross Functional Services.

7.1 General Provisions

7.1.1 IT Infrastructure Library[®] Version 3 (ITIL[®] v3) Support

The contractor shall be responsible for:

- a. Defining and implementing service delivery processes and procedures that are consistent with the requirements contained in this CF-PWS. Contractor processes used to provide services shall be consistent and complimentary with Government ITIL[®] v3 aligned processes.
- b. Ensuring that interfaces with Government, I³P contractors and other contractors are consistent with Government ITIL[®] v3 aligned processes.
- c. Ensuring that changes are approved and authorized by Government in accordance with Government Change Management Process.
- d. Providing information to support maintenance of Government Enterprise Service Catalog.

7.1.2 Understanding and Knowledge of ITIL[®]

The contractor shall be responsible for:

- a. Ensuring that all contractor personnel involved in delivery of services shall possess basic knowledge, understanding, and familiarity with foundational ITIL v3 concepts and processes.
- b. Providing verification that contractor personnel, required in delivery of services, are experienced and trained in ITIL.
- c. Participating in an objective assessment of contractor ITIL maturity.

7.2 Change Management

7.2.1 High-Level Process Flow Diagram, Goal, Purpose and General

Goal: The goals of Change Management are to: Respond to the customer's changing business requirements while maximizing value and reducing incidents, disruption and re-work; and respond to business and IT requests for change that will align services to business needs.

Purpose: The purpose of Change Management is to ensure that standardized methods and procedures are used for efficient and prompt handling of changes, changes to service assets and CIs are recorded in the Configuration Management Data Base (CMDB), and overall business risk is optimized.

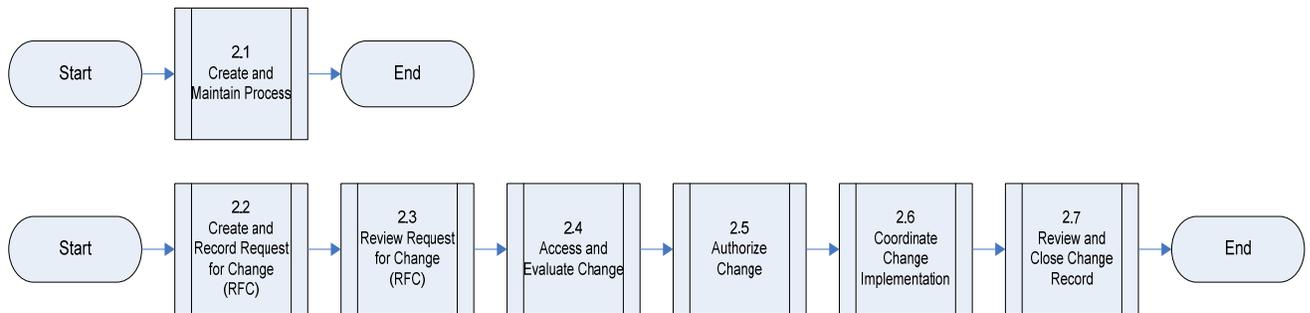


Figure 8: High-Level Change Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

- a. Designing and implementing Change Management procedures that align with Government Change Management Process.
- b. Documenting, tracking and managing all Changes using a contractor or Government provided Change Management system.
- c. (When contractors use a contractor Change Management System) Providing integration between contractor and Government Change Management systems including the integration of applicable software, e-mail and telephony in accordance with Government Change Management Process. All changes necessary to provide system integration shall be made at the contractor's expense. The contractor's solution shall provide an efficient transfer of information between systems (DRD 1294CF-011).
- d. Providing communications to users via Enterprise Service Desk and maintaining regular communications between all parties through resolution in accordance with Government Change Management Process.
- e. Providing case ownership of Change Requests that are assigned to the contractor until Change record is closed or ownership is officially recorded and subsequently reassigned.
- f. Participating in regularly scheduled Change Management meetings in accordance with Government Change Management Process.

7.2.2 Create and Maintain Change Management Process

The contractor shall be responsible for:

- a. Complying with Government Change Management Process.

- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Change Management process.

7.2.3 Create and Record Request for Change (RFC)

The contractor shall be responsible for:

- a. Determining type of change request that is required in accordance with Government Change Management Process
- b. Determining change procedures to be used in accordance with Government Change Management Process.
- c. Completing request for change form(s) (e.g. performing data entry into the government's change management system thereby creating a Change Request), with required documentation in accordance with Government Change Management Process.

7.2.4 Review Request for Change (RFC)

The contractor shall be responsible for providing information for preliminary review of requests for change.

7.2.5 Assess and Evaluate Change

The contractor shall be responsible for:

- a. Providing information to support impact assessment of requests for change.
- b. Providing information to support categorization and risk assessment of requests for change
- c. Providing information to support assessment of the benefit of implementing requests for change.

7.2.6 Authorize Change

The contractor shall be responsible for:

- a. Obtaining Government authorization for changes to services or underlying infrastructure supporting services in accordance with Government Change Management Process.
- b. Participating in Change Advisory Board(s) in accordance with Government Change Management Process.

7.2.7 Coordinate Change Implementation

The contractor shall be responsible for:

- a. Developing change implementation procedures in accordance with Government Change Management Policy.

- b. Coordinating activities with Government, I³P contractors and other contractors to implement approved changes.

7.2.8 Review and Close Change Record

- a. The contractor shall be responsible for providing information and participating in review meetings for closure of change records and capture of lessons learned.
- b. The contractor shall have responsibility for documenting in the government Change Request (CR) tracking system relevant CR closure information for which the contractor had the lead in implementation.
- c. The contractor shall be responsible for subsequent CR closure updates.

7.3 Incident Management

7.3.1 High-Level Process Flow Diagram, Goal and General Provisions

Goal: The primary goal of Incident Management is to restore normal service operation as quickly as possible and minimize adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. “Normal service operation” is defined here as service operation within Service Level Agreement (SLA) limits.

Purpose: The purpose of Incident Management is to deal with all unplanned interruptions to an IT service or a reduction in the quality of IT service. This can include failures; questions or queries reported by users via telephone, email, face to face, or automatically detected and reported by event monitoring tools.

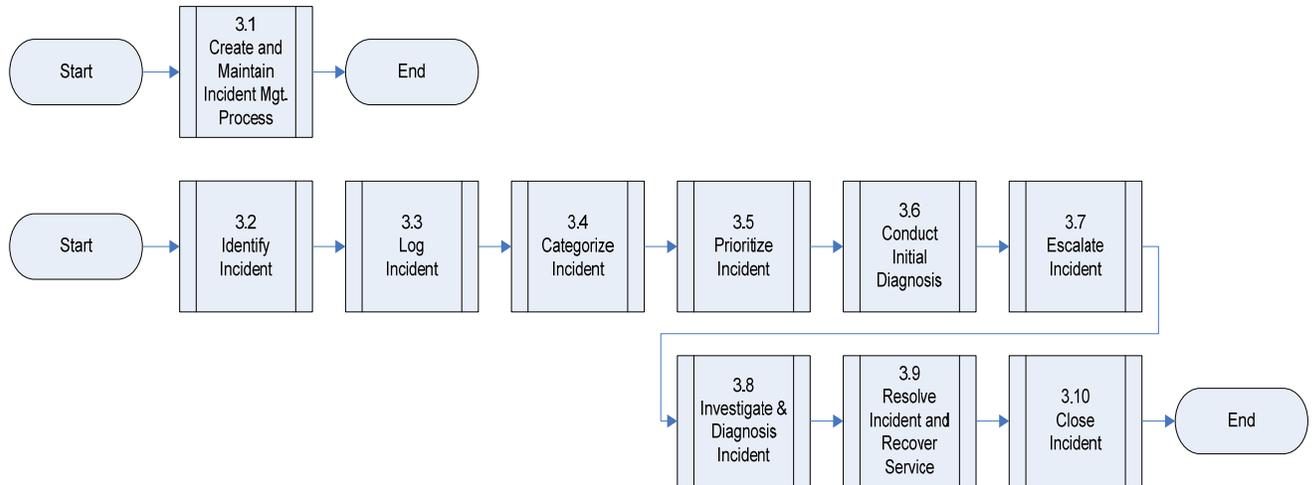


Figure 9: High-Level Incident Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

- a. Designing and implementing Incident Management procedures that align with Government Incident Management Process.
- b. Documenting, tracking and managing all Incidents using a contractor or Government provided Incident Management system.
- c. (When contractors use a contractor Incident Management System) Providing integration between contractor and Government Incident Management systems including the integration of applicable software, e-mail and telephony in accordance with Government Incident Management Process. All changes necessary to provide system integration shall be made at contractor expense. Contractor solution shall provide an efficient transfer of information between systems (DRD 1294CF-011).
- d. Providing communications to users via Enterprise Service Desk and maintaining regular communications between all parties through Incident resolution in accordance with Government Incident Management Process.
- e. Providing case ownership of Incidents that are assigned to contractor until service is restored or ownership is reassigned.
- f. Retaining ownership of each Incident assigned to contractor by the Enterprise Service Desk.
- g. Assigning end-to-end responsibility of each Incident to a single point of contact in order to facilitate communications with Government until service is restored.
- h. Resolving assigned Incidents in collaboration and coordination with Government, I³P contractors and other Contractors, and in accordance with Government Incident Management Process.
- i. Complying with Government notification and escalation procedures in accordance with Government Incident Management Process.
- j. Participating in daily Incident review meetings.

- k. Implementing and supporting continuous improvement actions to reduce frequency and severity of reported Incidents.

7.3.2 Create and Maintain Incident Management Process

The contractor shall be responsible for:

- a. Complying with Government Incident Management Process.
- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Incident Management process.

7.3.3 Identify Incident

The contractor shall be responsible for:

- a. Detecting Incidents via both manual and automated monitoring mechanisms.
- b. Notifying Enterprise Service Desk of an Incident within 15 minutes of detection.

7.3.4 Log Incident

The contractor shall be responsible for:

- a. Logging Incidents in accordance with Government Incident Management Process.
- b. Providing information to Enterprise Service Desk to ensure Incidents are logged in accordance with Government Incident Management Process.

7.3.5 Categorize Incident

The contractor shall be responsible for:

- a. Categorizing Incidents in accordance with Government Incident Management Process.
- b. Providing information to Enterprise Service Desk to ensure Incidents are categorized in accordance with Government Incident Management Process.

7.3.6 Prioritize Incident

The contractor shall be responsible for:

- a. Prioritizing Incidents in accordance with Government Incident Management Process.
- b. Providing information to Enterprise Service Desk to ensure Incidents are prioritized in accordance with Government Incident Management Process.

7.3.7 Conduct Initial Diagnosis

The contractor shall be responsible for:

- a. Conducting initial diagnosis of Incidents in accordance with Government Incident Management Process.
- b. Providing information to Enterprise Service Desk to ensure initial diagnosis of Incidents is performed in accordance with Government Incident Management Process.

7.3.8 Escalate Incident

The contractor shall be responsible for:

- a. Providing Tier 2 and Tier 3 Incident resolution and support.
- b. Accepting Incident Lead role as assigned.
- c. Providing a mechanism for expedited handling of Incidents that are of high business priority to Government in accordance with Government Incident Management Process.
- d. Opening 'Child' Incident records for other I³P Contractor(s).
- e. Providing status updates to Government Incident Management System.

7.3.9 Investigate and Diagnose Incident

The contractor shall be responsible for:

- a. Conducting incident investigation and diagnostic activities to identify root cause and develop Incident work-around(s).
- b. Executing Incident Management in accordance with Government Incident Management Procedures.

7.3.10 Resolve Incident and Recover Service

The contractor shall be responsible for:

- a. Applying resolution or work around to restore service as quickly as possible.
- b. Accomplishing resolution and recovery of all Incidents reassigned to Tier 2 and/or Tier 3 for support.
- c. Notifying Enterprise Service Desk via Incident Management System that service is restored.
- d. Recommending implementation of measures to avoid reoccurrence of Incidents relating to Services in accordance with Incident Management Procedures.

7.3.11 Close Incident

- a. The contractor shall be responsible for providing Incident closure information in accordance with Government Incident Management Process.
- b. The contractor shall have responsibility for documenting in the government Incident Management tracking system relevant incident closure information for which the contractor had the lead in implementation.
- c.

Request Fulfillment

7.4.1 High-Level Process Flow Diagram and General Provisions

Goal: The goals of Request Fulfillment are: provide a channel for users to request and receive standard services for which a pre-defined approval and qualification process exists; provide information to users and customers about the availability of services and the procedure for obtaining them; source and deliver components of requested standard services; and assist with general information, complaints or comments.

Purpose: The purpose of Request Fulfillment is to deal with Service Requests from users whether small (i.e., low risk, frequently occurring, low cost (e.g. a request to change a password, a request to install additional software onto a particular workstation, and a request to relocate some items of a desktop)) or large – higher risk, less frequently occurring, higher cost (e.g. a request to replace major infrastructure or other service components or a request to refresh major software components)).

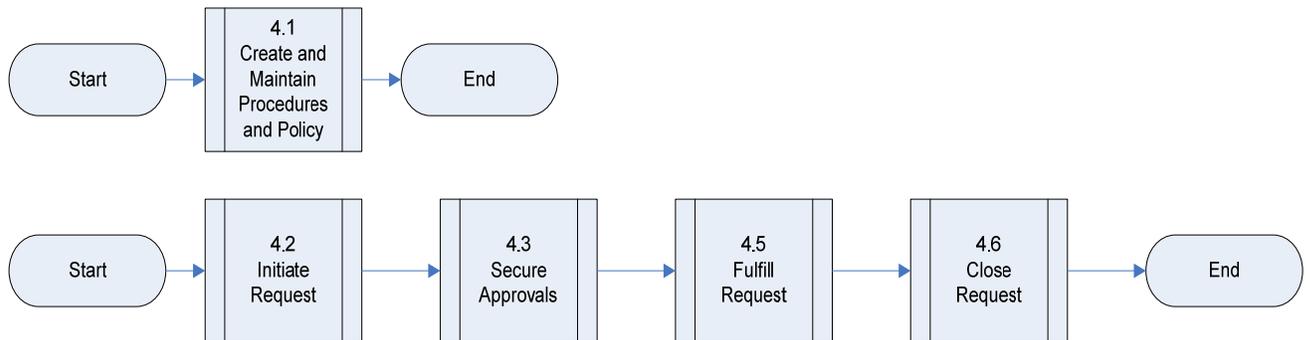


Figure 10: High-Level Request Fulfillment Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

- a. Designing and implementing Request Fulfillment procedures that align with Government Request Fulfillment Process.
- b. Documenting, tracking and managing all Requests using a contractor or Government provided Request Fulfillment system.
- c. (When contractors use a contractor Request Fulfillment System) Providing integration between contractor and Government Request Fulfillment systems including integration of applicable software, e-mail and telephony in accordance with Government Request Fulfillment Process. All changes necessary to provide system integration shall be made at the contractor's expense. The contractor's solution shall provide an efficient transfer of information between systems (DRD 1294CF-011).

- d. Maintaining communications regarding Request status with users at each status change via Enterprise Service Desk from time a Request is identified, through closure and through any follow-up communication.
- e. Providing case ownership of Requests that are assigned to Contractor until Request is closed.
- f. Participating in Request Fulfillment review meetings.
- g. Implementing and supporting continuous improvement of Request Fulfillment through self-service or other mechanisms.

7.4.2 Create and Maintain Request Fulfillment Process

The contractor shall be responsible for:

- a. Complying with Government Request Fulfillment Process.
- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Request Fulfillment process.

7.4.3 Initiate Request

The contractor shall be responsible for:

Utilizing Government-provided Enterprise Service Request System to define services that customers may request.

7.4.4 Secure Approvals

The contractor shall be responsible for providing supporting information on all Requests in support of approvals in conformance with Government Request Fulfillment Process. Supporting information includes, but is not limited to, price quotes, delivery SLAs, and dependencies.

7.4.5 Fulfill Request

The contractor shall be responsible for:

- a. Fulfilling all Requests within Government Service Level Agreements as defined for each standard Request and in conformance with Government Request Fulfillment Process.
- b. Enabling fulfillment of a Request in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government Request Fulfillment Process.
- c. Providing accurate and regular status updates for all Requests assigned to the contractor via the Enterprise Service Desk in accordance with Government Request Fulfillment Process.

7.4.6 Close Request

- a. The contractor shall be responsible for providing Request closure information in accordance with Government Request Fulfillment Process.
- b.

7.5 Problem Management

7.5.1 High-Level Process Flow Diagram and General Provisions

Goal: The primary goals of Problem Management are: to prevent problems and resulting Incidents from happening, to eliminate recurring Incidents and to minimize the impact of Incidents that cannot be prevented.

Purpose: The purpose of Problem Management is to provide a pre-defined and approved process for managing the lifecycle of all Problems to include diagnosis, determination of resolutions to those Problems, implementing solutions through appropriate control and change management procedures and preventing Problem reoccurrence.

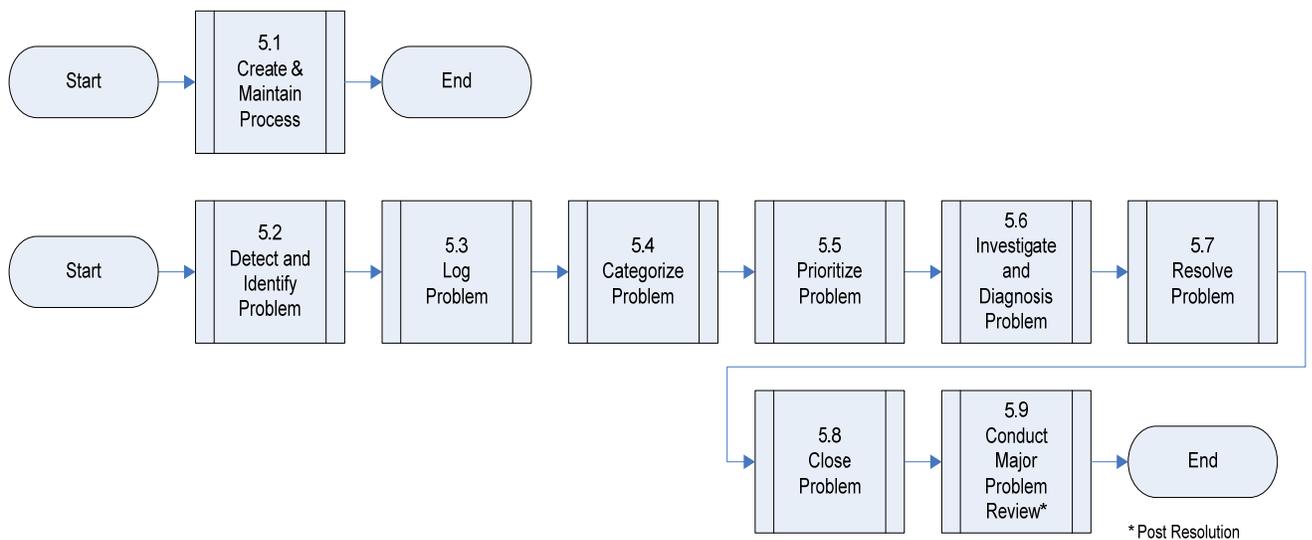


Figure 11: High-Level Problem Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

- a. Designing and implementing Problem Management procedures that align with Government Problem Management Process.

- b. Documenting, tracking and managing all Problems in a Government Problem Management System.
- c. (When contractors use a contractor Problem Management System) Providing integration between the contractor and Government Problem Management systems including integration of applicable software, e-mail and telephony in accordance with Government Problem Management Process. All changes necessary to provide system integration shall be made at the contractor's expense. Contractor solution shall provide an efficient transfer of information between systems (DRD 1294CF-011).
- d. Retaining ownership of each problem assigned to the contractor by either ESD or SIM.
 - 1. To the extent a Problem does not arise from or relate to the Contractor's Services:
 - a) The contractor shall notify ESD in accordance with Government Problem Management Procedures.
 - b) The contractor shall maintain responsibility for the Problem until the Problem is reassigned by ESD or SIM.
- e. Assigning end-to-end responsibility of each Problem to a single point of contact in order to facilitate communications with Government.
- f. Monitoring, controlling and managing each Problem assigned to contractor until it is closed by Enterprise Service Desk.
- g. Resolving assigned Problems in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government Problem Management Process.
- h. Complying with Government notification and escalation procedures in accordance with Government Problem Management Process.

7.5.2 Create and Maintain Problem Management Process

The contractor shall be responsible for:

- a. Complying with Government Problem Management Process.
- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Problem Management process.

7.5.3 Detect and Identify Problem

The contractor shall be responsible for:

- a. Identifying Problems by proactively performing on-going trend analysis on Incident information.
- b. Detecting Problems via both manual and automated monitoring mechanisms.

7.5.4 Log Problem

The contractor shall be responsible for:

- a. Logging Problems in accordance with Government Problem Management Process.

- b. Providing information to ESD to ensure Problems are logged in accordance with Government Problem Management Process.

7.5.5 Categorize Problem

The contractor shall be responsible for:

- a. Categorizing Problems in accordance with Government Problem Management Process.
- b. Providing information to Enterprise Service Desk to ensure Problems are categorized in accordance with Government Problem Management Process.

7.5.6 Prioritize Problem

The contractor shall be responsible for:

- a. Prioritizing Problems in accordance with Government Problem Management Process.
- b. Providing information to Enterprise Service Desk to ensure Problems are prioritized in accordance with Government Problem Management Process.

7.5.7 Investigate and Diagnose Problem

The contractor shall be responsible for:

- a. Conducting Problem investigation in accordance with Government Problem Management Process.
- b. Conducting Problem diagnostics in accordance with Government Problem Management Procedures.
- c. Providing status tracking information in Government Problem Management System in accordance with Government Problem Management Process.
- d. Investigating and diagnosing Problems in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government Problem Management Process.
- e. Validating Problem workarounds.
- f. Providing communications to users via Enterprise Service Desk and maintaining regular communications between all parties through Problem resolution in accordance with Government Problem Management Process.
- g. Performing Root Cause Analysis (RCA) in accordance with Government Problem Management Procedures.
- h. Updating Known Error information in accordance with Government Problem Management Process.
- i. Documenting problem resolution in accordance with Government Problem Management Process.
- j. Developing a Corrective Action Plan in accordance with Government Problem Management Process.

7.5.8 Resolve Problem

The contractor shall be responsible for:

- a. Determining if initiation of Change Management Process is required.
- b. Generating requests for change for permanent solutions and corrective action plans in accordance with Government Change Management Process.
- c. Applying resolutions across the enterprise, as applicable.
- d. Implementing the approved corrective action plan with follow-up to eliminate the fault from the operating environment.
- e. Resolving Problems in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government Problem Management Process.
- f. Developing supporting documentation, scripts, and procedures for Enterprise Service Desk to facilitate resolution of repetitive problems (DRD 1294CF-014). These supporting elements shall be fully developed, documented and tested prior to release in accordance with ITIL v3 Change, Release, and Deployment processes.

7.5.9 Close Problem

- a. The contractor shall be responsible for Providing Problem resolution and closure information in Government Problem Management System in accordance with Government Problem Management Process.
- b. The contractor is responsible for Problem Management system ticket closure and subsequent updates to the government Problem Management system regarding previously assigned and closed Problem Management tickets.

7.5.10 Conduct Major Problem Review

The contractor shall be responsible for:

- a. Participating in major Problem reviews.
- b. Providing Problem resolution details.

7.6 Service Level Management (SLM)

7.6.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Service Level Management is to ensure that an agreed-upon level of service is provided for all IT services, and that future services are delivered in accordance with Service Level Agreements. Proactive measures are also taken to seek and implement improvements to the level of service delivered.

Purpose: The purpose of SLM is to ensure that all operational services and their performance are managed in a consistent manner throughout the IT organization to meet the needs of the business and customers.

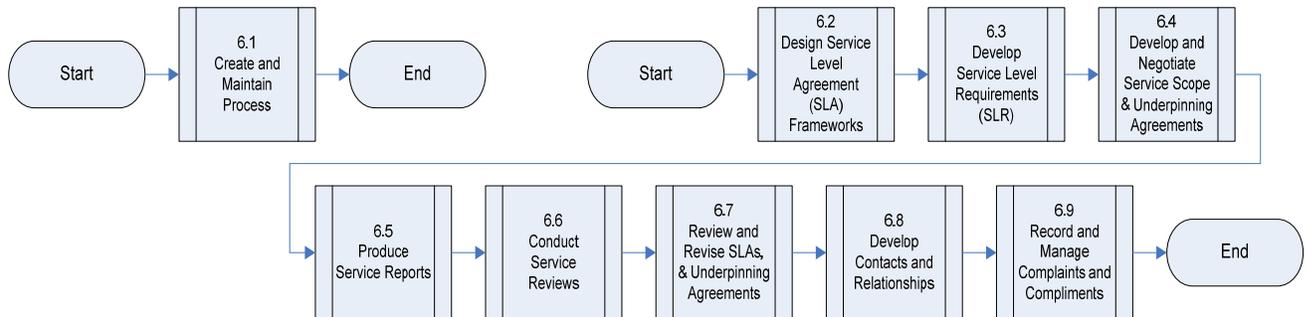


Figure 12: High-Level Service Level Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for designing and implementing SLM procedures that align with Government SLM Process.

7.6.2 Create and Maintain SLM Process

The contractor shall be responsible for:

- a. Complying with the approved Government SLM Process.
- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government SLM process.

7.6.3 Design Service Level Agreement (SLA) Frameworks

The contractor shall be responsible for providing information to support design and development of Service Level Agreement frameworks.

7.6.4 Develop Service Level Requirements (SLR)

The contractor shall be responsible for providing information to support Government with developing Service Level Requirements and gaining agreement with Government IT services customers.

7.6.5 Develop and Negotiate Service Level Scope and Underpinning Agreements

The contractor shall be responsible for providing information to support Government with developing and drafting service level scope and underpinning agreements.

7.6.6 Produce Service Level Reports

The contractor shall be responsible for providing information to support Government reporting of Service Levels in accordance with Government SLM Process.

7.6.7 Conduct Service Reviews

The contractor shall be responsible for supporting Government service reviews (e.g., meetings) in accordance with Government SLM Process.

7.6.8 Review and Revise Service Level Agreements and Underpinning Agreements

The contractor shall be responsible for providing information to support Government with reviewing and revising Service Levels and underpinning agreements.

7.6.9 Develop Contacts and Relationships

The contractor shall be responsible for providing information to support Government with developing customer relationships as it relates to IT services, service performance, and service agreements.

7.6.10 Record and Manage Customer Service Level Feedback

The contractor shall be responsible for:

- a. Providing information to support Government with assigning and dispositioning actions related to customer feedback.

7.7 Service Asset and Configuration Management (SACM)

7.7.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goals of SACM are to support the business and customer's control objectives and requirements, support efficient and effective Service Management processes by providing accurate configuration information to enable people to make decisions at the right time (e.g., to authorize change and releases and to resolve incidents and problems faster), minimize the number of quality and compliance issues caused by improper configuration of services and assets, and optimize service assets, IT configurations, capabilities and resources.

Purpose: The purpose of SACM is to identify, control, record, report, audit and verify Service Assets and CIs, including versions, baselines, constituent components, and their attributes and relationships, account for, manage, and protect the integrity of Service Assets and CIs (and where appropriate, those of their customers) throughout the service lifecycle.

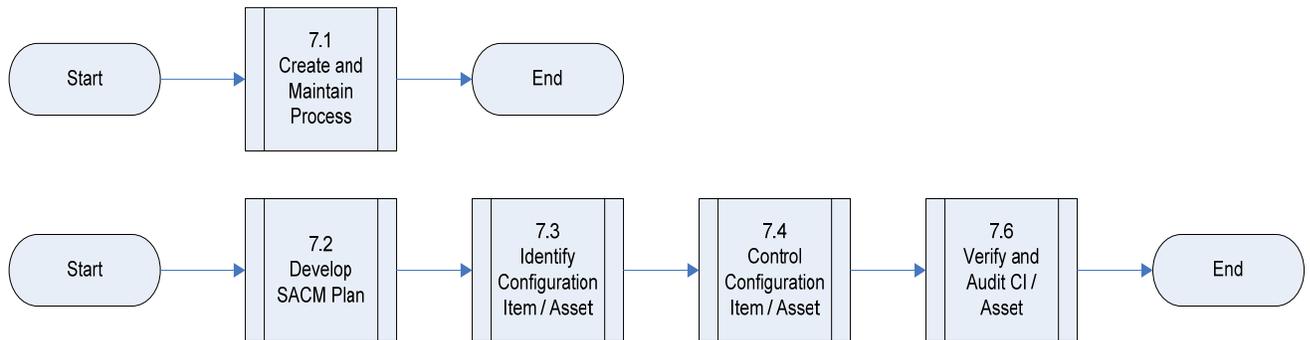


Figure 13: High-Level Service Asset and Configuration Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

- a. Defining and implementing contractor SACM procedures in accordance with Government SACM Process.
- b. Documenting, tracking and managing all Service Assets and CIs in Government CMDB in accordance with Government SACM Process.

- c. (When contractors use a contractor CMDB System) Providing integration between the contractor and Government CMDB systems including integration of applicable software, e-mail and telephony in accordance with Government SACM Process. All changes necessary to provide system integration shall be made at the contractor's expense. The contractor solution shall provide an efficient transfer of information between systems (DRD 1294CF-011).
- d. The Government CMDB is the official and authoritative system of record for all CIs (CI) where it is determined to be in the best interests of the government to track such. The contractor is responsible for creating, maintaining, and updating (to include proper removal) of CMDB records in the Government CMDB for CIs under their purview. Archival records shall be maintained for all CIs deleted from the CMDB.

7.7.2 Create and Maintain Service Asset and Configuration Management (SACM) Process

The contractor shall be responsible for:

- a. Complying with Government SACM Process.
- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government SACM process.

7.7.3 Develop Service Asset and Configuration Management (SACM) Plan

The contractor shall be responsible for developing and maintaining SACM Plan in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with DRD 1294CF-003.

7.7.4 Identify CI / Asset

The contractor shall be responsible for:

- a. Developing a strategy for ensuring identification of all CIs in accordance with Government SACM Process.
- b. Identifying and labeling, as applicable, all CIs in accordance with Government SACM Process
- c. Assigning unique identifiers to each CI in accordance with Government SACM Process.
- d. Specifying relevant attributes, relationships, owner and baselines for each CI in accordance with Government SACM Process.

7.7.5 Control CI / Asset

The contractor shall be responsible for:

- a. Identifying when a change to a CI is necessary and initiating a request for change in accordance with Government Change Management Process.

- b. Determining and reporting the root cause, impact, and actions to prevent recurrence of an unauthorized change in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government SACM Process.

7.7.6 Verify and Audit CI / Asset

The contractor shall be responsible for:

- a. Participating in Government audit activities to ensure conformity between documented CIs and actual CIs in accordance with Government SACM Process.
- b. Providing audit CI data and Release documentation in accordance with Government SACM Process.
- c. Implementing corrective actions in accordance with Government SACM Process.
- d. Providing information to support audit reporting in accordance with Government SACM Process.

7.8 Release and Deployment Management (RDM)

7.8.1 High Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Release and Deployment Management is to deploy releases into production and establish effective use of the service.

Purpose: The purpose of Release and Deployment Management is to: define and agree on release and deployment plans with customers and stakeholders; ensure that integrity of a release package and its constituent components is maintained throughout the transition activities and recorded accurately in the Configuration Management Database (CMDB); ensure that all release and deployment packages can be tracked, installed, tested, verified, and/or uninstalled or backed out if appropriate; and ensure that customers and stakeholder change is managed during Release and Deployment activities.

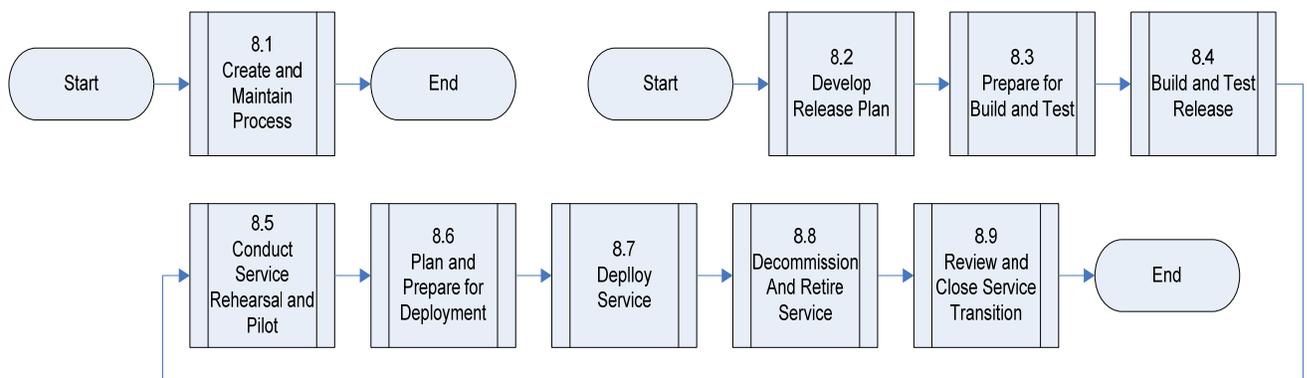


Figure 14: High-Level Release and Deployment Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for performing Releases in accordance with Government Release and Deployment Process.

7.8.2 Create and Maintain Release and Deployment Management Process

The contractor shall be responsible for:

- a. Complying with Government RDM Process.
- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government RDM Process.
- c. Conducting an annual inventory of applications being used to support NASA services, and report this data, including the cost to develop, operate, enhance and maintain applications as specified in DRD 1294CF-005.
- d. Reviewing the NASA Application Repository to verify if an existing application will satisfactorily fulfill the stated application requirements prior to purchasing or developing a new application/capability and inform the Responsible NASA Official of said existing application(s).

7.8.3 Develop Release Plan

The contractor shall be responsible for developing and maintaining RDM Plan in collaboration and coordination with Government, I³P Contractors, and other contractors and in accordance with DRD 1294CF-004.

7.8.4 Prepare for Release Build and Test

The contractor shall be responsible for preparing for release build and test in collaboration and coordination with Government, I³P contractors and other Contractors.

7.8.5 Build and Test Release

The contractor shall be responsible for:

- a. Building and testing releases in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government RDM Process.
- b. Developing release documentation in accordance with Government RDM Process.
- c. Creating test scenario and acceptance criteria and submitting them for review in accordance with Government RDM Process.
- d. Managing Release build and test environments.

7.8.6 Conduct Service Rehearsal and Pilot

The contractor shall be responsible for conducting service rehearsals and pilots in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government RDM Process.

7.8.7 Plan and Prepare for Deployment

The contractor shall be responsible for:

- a. Planning and preparing for deployment in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government RDM Process.
- b. Assessing the need for and planning for a release stabilization period in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government RDM Process.

7.8.8 Deploy Service

The contractor shall be responsible for:

- a. Deploying services in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government RDM Process.
- b. Verifying successful service deployment in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government RDM Process.
- c. Executing back-out plan, if necessary, in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government RDM Process.

7.8.9 Decommission and Retire Service

The contractor shall be responsible for decommissioning and retiring services in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with Government RDM Process.

7.8.10 Review and Close Service Release Deployment

The contractor shall be responsible for closing release deployment in accordance with Government RDM Process.

7.9 Capacity Management

7.9.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Capacity Management process is to ensure IT capacity in all areas of IT is matched to the needs of the Government's business.

Purpose: The purpose of Capacity Management is to provide a point of focus and management for all capacity and performance related issues, relating to both services and resources.

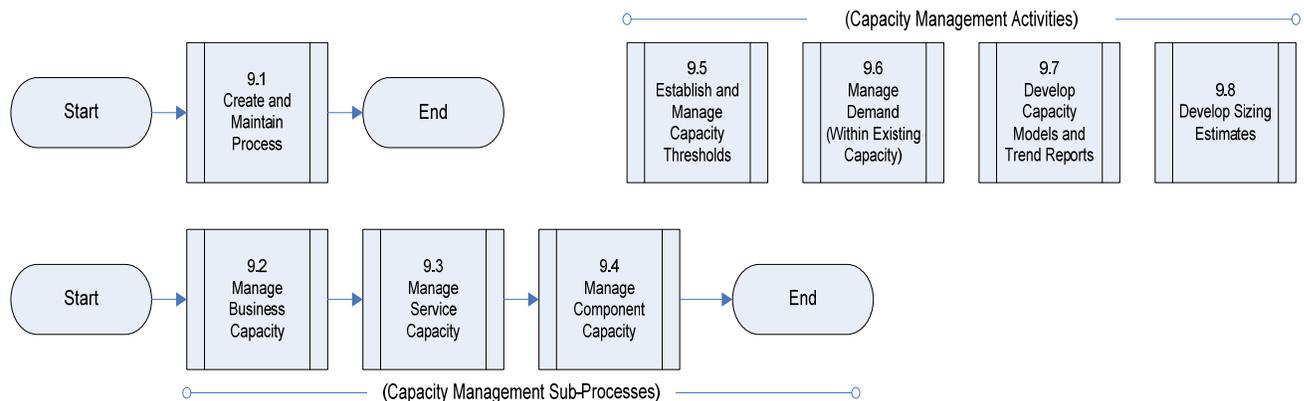


Figure 15: High-Level Capacity Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

- a. Designing and implementing Capacity Management procedures that align with Government Capacity Management Process.
- b. Developing and maintaining Capacity Management Plan in collaboration and coordination with Government, I³P Contractors, and other contractors and in accordance with DRD 1294CF-006.
- c. Conducting annual reviews of projected capacity requirements for infrastructure and related services, and providing recommendations based upon information provided by Government Portfolio Management Process as part of Government's normal business planning cycle.

7.9.2 Create and Maintain Capacity Management Process

The contractor shall be responsible for:

- a. Complying with Government Capacity Management Process.

- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Capacity Management Process.

7.9.3 Manage Business Capacity

The contractor shall be responsible for:

- a. Providing impact assessment of potential business capacity issues based on Government business direction.
- b. Prototyping and sizing capacity impact solutions, including:
 - 1. Developing and maintaining standard templates for capacity test plans in collaboration and coordination with Government, I³P contractors and other Contractors.
 - 2. Coordinating tests with Government, I³P contractors and other contractors to provide end-to-end testing.
 - 3. Testing and sizing models for capacity impacts.
- c. Developing plans for required changes to existing capacity in accordance with DRD 1294CF-006.

7.9.4 Manage Service Capacity

The contractor shall be responsible for:

- a. Providing SOM with information regarding Service Capacity and issues.
- b. Monitoring Service Capacity including:
 - 1. Collecting Service Capacity performance data, at a minimum, per the following schedule:
 - a) Daily data collection for volatile and dynamic systems.
 - b) Weekly data collection for variable and stable systems.
 - 2. Maintaining Services aligned with Government Enterprise Service Catalog.
- c. Analyzing Service Capacity, including:
 - 3. Providing service capacity performance reports in accordance with DRD 1294CF-007.
- d. Tuning Service performance, including changing capacity, to take corrective action or adjust for more effective usage.
- e. Establishing capacity thresholds and making adjustments based on Government requirements.
- f. Responding to Government requests for capacity impact statements within 30 days.

7.9.5 Manage Component Capacity

The contractor shall be responsible for:

- a. Providing SOM with information regarding component capacity and issues.
- b. Monitoring component capacity usage, including:
 - 1. Maintaining components aligned with Government CMDB.

- c. Analyzing component usage, including:
 - 1. Reviewing component capacity data.
 - 2. Determining if proactive changes are needed.
 - 3. Determining if tuning or replacing a component can provide for a more effective use of the component.
- d. Tuning or replacing components, including:
 - 1. Adjusting or balancing component capacity to provide more effective usage.
 - 2. Changing component capacity to correct utilization issues.
 - 3. Replacing components in compliance with Change Management Process.
 - 4. Collecting and providing component capacity data based on Government-specified standards and metrics.
- e. Providing component capacity reports in accordance with DRD 1294CF-007.
- f. Reviewing, validating and updating component baselines and profiles in the CMDB.

7.9.6 Establish and Manage Capacity Thresholds

The contractor shall be responsible for monitoring and generating alerts and warnings associated with capacity and performance thresholds.

7.9.7 Manage Demand (within existing capacity)

The contractor shall be responsible for providing information and support to manage demand within existing capacity levels.

7.9.8 Develop Capacity Models and Trend Reports

The contractor shall be responsible for providing capacity models and trend reports in accordance with DRD 1294CF-007.

7.9.9 Develop Sizing Estimates

The contractor shall be responsible for developing sizing estimates to support capacity planning.

7.10 Availability Management

7.10.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The Goal of Availability Management is to ensure that the level of service availability delivered in all services is matched to the requirements of the Government's business.

Purpose: The Purpose of Availability Management is to provide a point of focus and management for all availability-related issues, relating to both services and resources, ensuring that availability targets in all areas are measured and achieved.

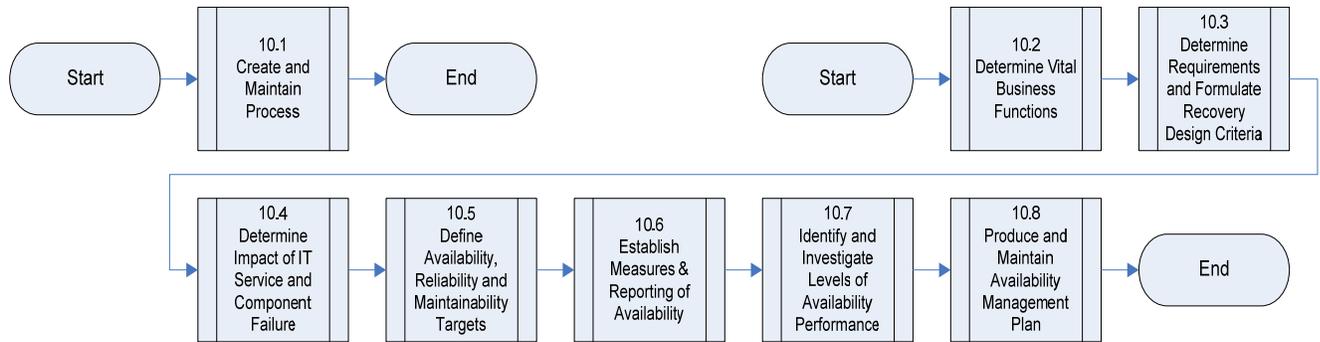


Figure 16: High-Level Availability Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for designing and implementing Availability Management procedures that align with Government Availability Management Process.

Identifying planned downtime and scheduling downtime in collaboration and coordination with Government, I³P contractors and other contractors and in alignment with Government Mission Flight Requirements.

7.10.2 Create and Maintain Availability Management Process

The contractor shall be responsible for:

- a. Complying with Government Availability Management Process.
- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Availability Management Process.

7.10.3 Determine Vital Business Functions

The contractor shall be responsible for providing information to support Government with identifying vital business functions.

7.10.4 Determine Requirements and Formulate Recovery Design Criteria

- a. The contractor shall be responsible for providing information to support Government with defining availability requirements.
- b. Providing information to support Government with formulating recovery design criteria.

7.10.5 Determine Impact of IT Service and Component Failure

The contractor shall be responsible for providing information to support Government with conducting business and service impact analysis and component failure impact analysis related to availability.

7.10.6 Define Availability, Reliability and Maintainability Targets

The contractor shall be responsible for providing information to support Government with developing and maintaining availability, reliability and maintainability targets and measures that align with applicable Service Level Agreements.

7.10.7 Monitor and Analyze Availability, Reliability and Maintainability

The contractor shall be responsible for:

- a. Establishing service metrics and tools for measuring availability, reliability and maintainability in accordance with Government Availability Management Process.
- b. Deploying tool sets and/or interfaces to permit end-to-end measurement of availability.
- c. Collecting and recording availability, reliability and maintainability data.
- d. Monitoring availability, reliability and maintainability elements with respect to Service Levels.
- e. Conducting analysis for compliance with availability, reliability and maintainability Service Levels.
- f. Reporting results of monitoring and analysis in accordance with DRD 1294CF-009.
- g. Providing information to assist in Problem analysis related to service availability.

7.10.8 Identify and Investigate Levels of Availability Performance

The contractor shall be responsible for:

- a. Identifying Availability performance that fails to meet Government Service Level Agreements.
- b. Investigating availability performance that fails to meet Government Service Level Agreements.
- c. Initiating actions to ensure availability performance complies with Government Service Level Agreements.

7.10.9 Produce and Maintain Availability Management Plan

The contractor shall be responsible for:

- a. Developing and maintaining Availability Management Plan in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with DRD 1294CF-008.

- b. Addressing end-to-end availability requirements in any designs to ensure compliance with Government design and architecture standards.
- c. Addressing end-to-end availability requirements in defining and executing any test plans.
- d. Identifying planned downtime and scheduling downtime in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with applicable Service Level Agreements.
- e. Implementing requested changes to availability metrics and Service Level Agreement in accordance with Government SLM Process.

7.11 IT Service Continuity Management (ITSCM)

7.11.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of ITSCM is to support the overall Business Continuity Management process by ensuring that required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required business timeframes.

Purpose: The purpose of ITSCM is to establish and maintain required ongoing recovery capability within required IT services and their supporting components.

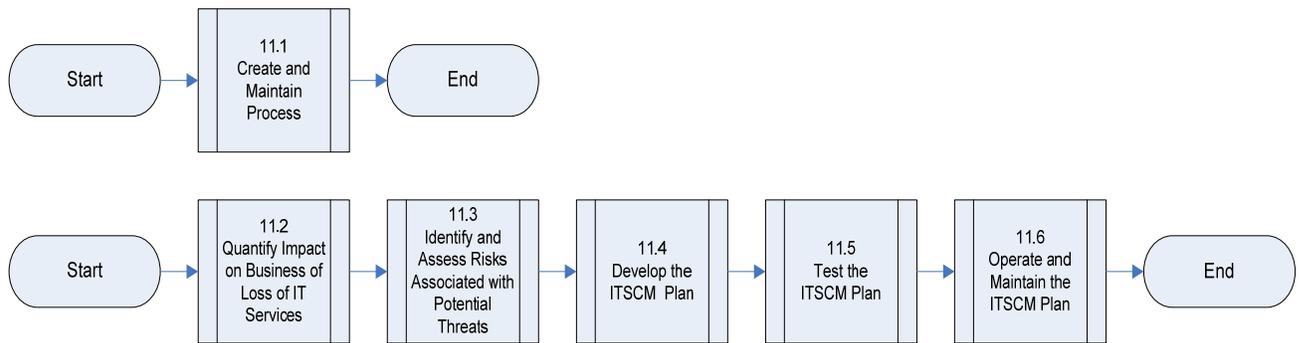


Figure 17: High-Level IT Service Continuity Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

- a. Designing and implementing ITSCM Management procedures that align with Government ITSCM Process.
- b. Providing ITSCM Services to mitigate the impact of a disaster or major failure in accordance with Government ITSCM Process.
- c. Developing, documenting and maintaining procedures (e.g., Disaster Recovery checklists) in collaboration and coordination with Government, I³P contractors and other contractors to meet Government requirements (e.g., Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)).

7.11.2 Create and Maintain IT Service Continuity Management Process

The contractor shall be responsible for:

- a. Complying with Government ITSCM Process.
- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government ITSCM process.

7.11.3 Quantify Impact on Business of Loss of IT Services

The contractor shall be responsible for:

- a. Providing information to support analysis of the impact of continuity scenarios.
- b. Providing information to support identification and impact of contingency options and mitigation actions.

7.11.4 Identify and Assess Risks Associated with Potential Threats

The contractor shall be responsible for:

- a. Providing information to support identification of risk responses and proposed countermeasures.
- b. Participating in IT risk assessment activities in order to reduce vulnerability to the business.

7.11.5 Develop the IT Service Continuity Management (ITSCM) Plan

The contractor shall be responsible for:

- a. Developing and maintaining ITSCM Plan in collaboration and coordination with Government, I³P contractors and other contractors and in accordance with DRD 1294CF-010.

7.11.6 Test the IT Service Continuity Management (ITSCM) Plan

The contractor shall be responsible for:

- a. Developing test scenarios in collaboration and coordination with Government, I³P contractors and other contractors in support of conducting testing of ITSCM Plan in accordance with Government ITSCM Process.
- b. Conducting walkthrough, full, partial and scenario tests in accordance with Government ITSCM Process.

7.11.7 Operate and Maintain the ITSCM Plan

The contractor shall be responsible for:

- a. Participating in Government ITSCM reviews in accordance with Government ITSCM Process.
- b. Invoking the ITSCM plan in accordance with Government ITSCM Process.
- c. Performing training functions including:
 1. Developing and updating the contractor ITSCM training plans and material.
 2. Training the contractor recovery team members.
- d. Maintaining local work procedures and contact lists.
- e. Performing ITSCM Plan gap analysis and response planning and updating the contractor ITSCM Plan accordingly.
- f. Documenting all contingency services provided in Government Service Level Agreements.
- g. Executing recovery plans and restoring Service to normal operation.
- h. Supporting ITSCM evaluation efforts following disaster events, including providing evaluations and lessons learned and updating the contractor ITSCM Plan as needed.

7.12 Knowledge Management

7.12.1 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Knowledge Management is to enable organizations to improve the quality of management decision making by ensuring that reliable and secure information and data is available throughout the service lifecycle.

Purpose: The purpose of Knowledge Management is to ensure that the right information is delivered to the appropriate place or person at the right time to enable informed decision making.

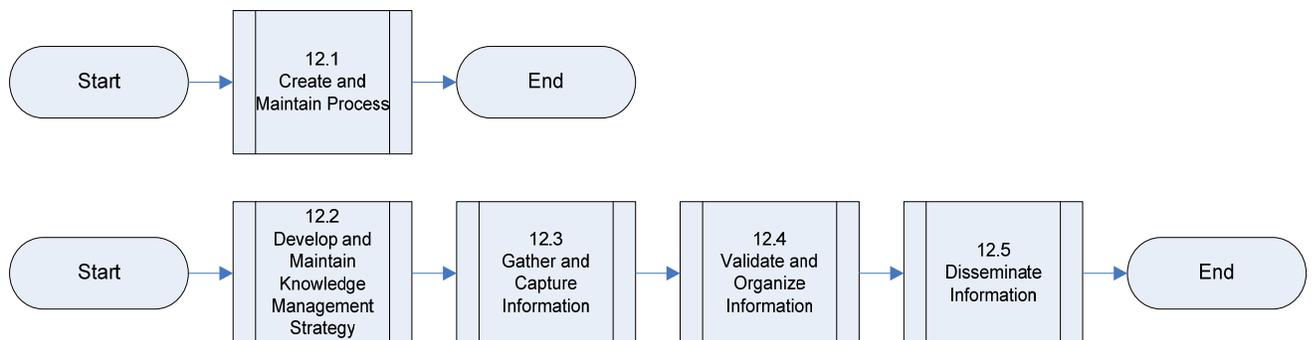


Figure 18: High-Level Knowledge Management Process Flow Diagram

General Provisions:

The contractor shall be responsible for:

- a. Designing and implementing knowledge management procedures and tools to support knowledge capture and dissemination in accordance with Government Knowledge Management Process.

- b. Managing and maintaining knowledge and information assets in collaboration and coordination with Government, I³P contractors and other Contractors, and in accordance with Government Knowledge Management Process. This captured developed, generated, and created knowledge and information and related information elements generated as a result of this process shall become the Government Knowledge Base.

7.12.2 Create and Maintain Knowledge Management Process

The contractor shall be responsible for:

- a. Complying with Government's Knowledge Management Process.
- b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Knowledge Management process.

7.12.3 Develop and Maintain Knowledge Management System

The contractor shall be responsible for providing the Government with information to support develop and maintain of the Government Knowledge Management system.

7.12.4 Gather and Capture Information

The contractor shall be responsible for gathering and capturing information in accordance with Government Knowledge Management Process.

7.12.5 Validate and Organize Information

The contractor shall be responsible for validating and organizing information in accordance with Government Knowledge Management Process.

7.12.6 Disseminate Information

- a. The contractor shall be responsible for disseminating information in accordance with Government Knowledge Management Process.
- b. The contractor shall make all Knowledge Base information developed, gathered, generated, and or otherwise created under this contract available to the NASA OCIO and ESD in electronic form compliant with the Remedy system requirements and specifications.

7.13 Information Security Management (ISM)

7.13.1 High-Level Process Flow Diagram, Goal and Purpose

Goal: The goal of ISM is to align IT security with business security and ensure that information security is effectively managed across all service management and service delivery activities.

Purpose: The purpose of ISM is to provide a point of focus and management for all aspects of IT security.

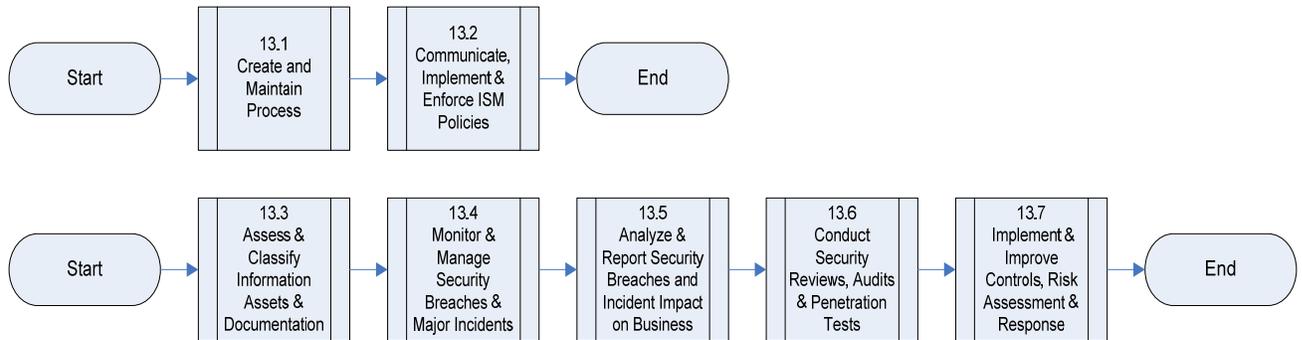


Figure 19: High-Level Information Security Management Process Flow Diagram

7.13.2 Create and Maintain Information Security Management (ISM) Process

The contractor shall be responsible for:

- a. Complying with Government's ISM policies and procedures. Examples include Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST). See Section 6, Common Information Technology Security Requirements, in this document.
- b. Performing continuous analysis of industry best practices or trends and informing Government of changes that could impact or improve Government ISM process.

7.13.3 Communicate, Implement and Enforce Information Security Management (ISM) Procedures

The contractor shall be responsible for:

- a. Implementing Government ISM policies (e.g., FISMA) for all contractor services provided.
- b. Supporting Government's ISM policy enforcement efforts and providing details of Information security practices to Government.

7.13.4 Assess and Classify Information Assets and Documentation

The contractor shall be responsible for:

- a. Providing information to Government to support information asset identification and documentation in accordance with Government's ISM policy.
- b. Providing information to Government to support information asset review activities regarding completeness, accuracy, and vulnerability.
- c. Providing information to Government to support classification of information assets in accordance with Government's ISM policy.

7.13.5 Monitor and Manage Security Breaches and Major Incidents

The contractor shall be responsible for:

- a. Monitoring and reporting security breaches and security incidents in accordance with Government's ISM procedures.
- b. Providing information to Government to support investigation of any security breach and/or security Incident.
- c. Providing information to Government to support resolution of any security breach and/or security Incident (DRD 1294CF-012).

7.13.6 Analyze and Report Security Breaches and Incident Impact on Business

The contractor shall be responsible for participating in review and analysis of security breaches and security Incidents and providing detailed information to Government to support analysis of business impact and creation of security breach and security Incident report.

7.13.7 Conduct Security Reviews, Audits and Penetration Tests

The contractor shall be responsible for:

- a. Conducting security reviews and regular audits of information and technology assets under Contractor's control in accordance with Government's ISM policy.
- b. Participating in periodic Government security audits as requested by Government and coordinating audit activities of Third Parties as required or requested by Government.
- c. Conducting and supporting security penetration testing as required or when requested by Government in accordance with Government's ISM policy.

7.13.8 Improve Security Controls, Risk Assessment and Responses

The contractor shall be responsible for:

- a. Providing information to Government to support the assessment of security risks.
- b. Participating in development and maintenance of security improvement plans in accordance with Government's ISM policy.

8 Common Project Management Guidelines

8.1 Introduction and Overview

I³P work includes projects that have been approved by the NASA IT governance process to transform elements of the NASA infrastructure. NASA's strategic approach to the management of IT projects is documented in NPR 7120.7, *NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements*. The contractor shall perform approved projects in compliance with the requirements of the NPR 7120.7 life cycle which includes formulation, implementation, and transition to operation.

8.2 Applicability of NPR 7120.7

The scope of IT projects that are subject to NPR 7120.7 is as follows:

- a. The project includes the development of new IT systems or capabilities and is \$500K or greater for the total development and implementation cost or affects more than one Center.
- b. The project includes the modification to or enhancement of existing IT systems or capabilities and is \$500K or greater for the total modification/enhancement cost, regardless of how many Centers are affected.

Some NASA Centers have developed frameworks for the management of projects of smaller scope or size. These frameworks specify a subset of NPR 7120.7 reviews and requirements that are suitable for these smaller projects as determined by the NASA CIO or the CIO of the implementing Center. Such a decision may be made, for example, for reasons related to risk, importance, or visibility of the program or project. For these projects, the Contractor's project and technical management methodology shall ensure compliance with the applicable elements of 7120.7.

9 Glossary of Terms

Activity	A set of actions designed to achieve a particular result. Activities are usually defined as part of Processes or plans, and are documented in procedures.
Asset	Any resource or capability. Assets of a contractor include anything that could contribute to the delivery of a service. Assets can be one of the following types: Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.
Asset Management	Asset Management is the Process responsible for tracking and reporting the value and ownership of financial Assets throughout their Lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process.
Availability	The ability of a CI or IT Service to perform its agreed function when required.
Availability Management	The Process responsible for defining, analyzing, planning, measuring and improving all aspects of the availability of IT Services. Availability Management is responsible for ensuring that all IT infrastructure, Processes, tools, roles etc are appropriate for the agreed Service Level Targets for availability.
Capacity	The maximum throughput that a CI or IT Service can deliver while meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.
Capacity Management	The Process responsible for ensuring that the capacity of IT Services and the IT infrastructure is able to deliver agreed Service Level Targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT Service and plans for short, medium and long term business requirements.
Change	The addition, modification or removal of anything that could have an effect on IT Services. The scope of any Change should include all IT Services, CIs, Processes, documentation etc.
Change Management	The Process responsible for controlling the Lifecycle of all changes. The primary objective of Change Management is to enable beneficial changes to be made with minimum disruption to IT Services.
Component	A general term used to mean one part of something more complex. For example, a computer system may be a Component of an IT Service; an Application may be a Component of a Release unit. Components that are managed as part of an IT Service should be CIs and managed as part of the enterprise Configuration Management Process.

Configuration Item (CI)	Any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a configuration record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people and formal documentation such as Process documentation and SLAs.
Configuration Management	The Process responsible for maintaining information about CIs required to deliver an IT Service, including their relationships. This information is managed throughout the Lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.
Continual Service Improvement	A stage in the Lifecycle of an IT Service. Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services.
Contractor Management	The Process responsible for ensuring that all Contracts with contractors support the needs of the business, and that all contractors meet their contractual commitments.
Customer	Someone who buys goods or services. The Customer of an IT Service contractor is the person or group that defines and agrees the Service Level Targets.
Deployment	The Activity responsible for movement of new or changed hardware, software, documentation, Process, etc., to the live environment. Deployment is part of the Release and Deployment Management Process.
Enterprise Service Desk	The Single Point of Contact (SPOC) between Users and contractors responsible for receiving, logging, escalating, monitoring and closing tickets associated with managing Incidents and Service Requests. Also responsible for communicating with Users regarding the status of Incidents and Service Requests and on-going measurement of Customer satisfaction.
Government	The National Aeronautics and Space Administration (NASA) enterprise along with the collective business units making up the IT Infrastructure and Service delivery environment defined to be in-scope for purposes of the IT Infrastructure Integration Program (I ³ P) Acquisition.
Incident	An unplanned interruption to an IT Service or a reduction in the quality of an IT Service. Failure of a CI that has not yet impacted service is also an Incident. For example failure of one disk from a mirror set.
Incident Management	The Process responsible for managing the Lifecycle of all Incidents. The primary objective of Incident Management is to return the IT Service to Users as quickly as possible.

Information Security Management	The Process that ensures the confidentiality, integrity and availability of an organization's assets, information, data and IT Services. Information Security Management usually forms part of an organizational approach to security management which has a wider scope than the IT Service Contractor, and includes handling of paper, building access, phone calls etc., for the entire Organization.
IT Infrastructure	All of the hardware, software, networks, facilities, etc., that are required to develop, test, deliver, monitor, control or support IT Services. The term IT Infrastructure includes all of the information technology but not the associated people, Processes and documentation in support of IT Services.
IT Service	A service provided to one or more Customers by an IT Service Contractor. An IT Service is based on the use of information technology and supports the Customer's business Processes. An IT Service is made up from a combination of people, Processes, and technology and should be defined in a Service Level Agreement.
IT Service Contractor	A Service Provider/Supplier responsible for supplying goods or services that are required to deliver IT Services. These may include commodity hardware and software vendors, network and telecom suppliers and IT outsourcing service providers.
IT Service Continuity Management	The Process responsible for managing risks that could seriously impact IT Services. ITSCM ensures that the IT Service contractor can always provide minimum agreed Service Levels, by reducing the risk to an acceptable level and planning for the recovery of IT Services. ITSCM should be designed to support business continuity management.
IT Service Management (ITSM)	The implementation and management of quality IT Services that meet the needs of the business. IT Service Management is performed by contractors in concert with the client enterprise through an appropriate mix of people, Process and information technology.
Knowledge Management	The Process responsible for gathering, analyzing, storing and sharing knowledge and information within an organization. The primary purpose of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge.
Known Error	A Problem that has a documented root cause and a workaround. Known Errors are created and managed throughout their Lifecycle by Problem Management. Known Errors may be identified by Users, Customers or IT Service Contractors.

Lifecycle	<p>The various stages in the life of an IT Service, CI, Incident, Problem, Change etc. The Lifecycle defines the categories for status and the status transitions that are permitted. For example:</p> <ul style="list-style-type: none"> • The Lifecycle of an application includes requirements, design, build, deploy, operate, and optimize. • The expanded Incident Lifecycle includes detect, respond, diagnose, repair, recover, restore. • The lifecycle of a server may include: ordered, received, in test, live, disposed etc.
Operational Level Agreement (OLA)	<p>An agreement between an enterprise IT organization and another part of the same organization. An OLA supports the enterprise IT organization's delivery of IT Services to Customers through IT Service Contractors. The OLA defines the goods and services to be provided and the responsibilities of both parties. Performance expectations are documented in SLAs and other Underpinning Contracts.</p>
Performance Work Statement (PWS)	<p>A document containing all requirements for a product purchase, or a new or changed IT Service.</p>
Problem	<p>A cause of one or more Incidents. The cause is not usually known at the time a problem record is created. The Problem Management Process is responsible for further investigation of the Problem.</p>
Problem Management	<p>The Process responsible for managing the Lifecycle of all Problems. The primary objectives of Problem Management are to prevent Incidents from happening and to minimize the impact of Incidents that cannot be prevented.</p>
Process	<p>A structured set of Activities designed to accomplish a specific objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A Process may define policies, standards, guidelines, Activities, and work instructions if they are needed.</p>
Recovery Point Objective (RPO)	<p>The maximum amount of data that may be lost when an IT Service is restored after an interruption. Recovery Point Objective is expressed as a length of time before the failure.</p>
Recovery Time Objective (RTO)	<p>The maximum time allowed for recovery of an IT Service following an interruption. Recovery Time Objective is expressed as a length of time from the failure to restoration of the IT Service.</p>
Relationship Manager	<p>Relationship Manager is the person responsible for managing the interaction between the contractor service provider and NASA customers.</p>

Release	A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, tested and deployed as a single entity.
Release and Deployment Management	The Process responsible for both Release Management and Deployment.
Release Management	The Process responsible for planning, scheduling and controlling the movement of releases to test and live environments. The primary objective of Release Management is to ensure that the integrity of the live environment is protected and that the correct components are released. Release Management is part of the Release and Deployment Management Process.
Request For Change (RFC)	A formal proposal for a Change to be made. An RFC includes details of the proposed Change, and may be recorded on paper or electronically.
Request Fulfillment	The Process responsible for managing the Lifecycle of all Service Requests.
Service Asset & Configuration Management	The Process responsible for both Configuration Management and Asset Management.
Service Level	Measured and reported achievement against one or more Service Level Targets.
Service Level Agreement (SLA)	An agreement between a contractor and a Customer. The Service Level Agreement describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service contractor and Customer. A single SLA may cover multiple IT Services or multiple Customers
Service Level Management	The Process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular Customer reviews.
Service Level Targets	Service Level Targets are performance commitments documented in a Service Level Agreement. Service Level Targets are based on Service Level Requirements agreed to with the business and ensure IT Service design is aligned with results.

Service Request	A request from a user for information, advice, a standard Change or for access to an IT Service. For example - to reset a password, or to provide standard IT Services for a new user. Service Requests are usually handled by a Service Desk and do not require an RFC (Request For Change) to be submitted.
Single Point of Contact (SPOC)	A designated single, consistent way to communicate with an individual, business entity or enterprise.
Tier 0 (Self Help)	A level of support provided to users via a web-based portal. This Self-Help level of support assists Users resolve lower level of difficulty Incidents and/or Service Requests. The Incidents and/or Service Requests handled at this level of support typically can be resolved through the direct effort of Users, rather than through the effort of resources associated with the Enterprise Service Desk.
Tier 1 Support	The first level in a hierarchy of support groups involved in the resolution of Incidents. Each level contains a more specialized skill, knowledge, time or resource in support of their responsibilities. Tier 1 is typically defined as the Enterprise Service Desk (ESD).
Tier 2 Support	The second level in a hierarchy of support groups involved in the resolution of Incidents and investigation of Problems. Each level contains a more specialized skill, knowledge, time or resource in support of their responsibilities. Tier 2 would be the next level of dispatch/escalation from Tier 1 (ESD) support.
Tier 3 Support	The third level in a hierarchy of support groups involved in the resolution of Incidents and investigation of Problems. Each level contains a more specialized skill, knowledge, time or resource in support of their responsibilities. Tier 3 would be the next level of dispatch/escalation from Tier 2 support.
Touch-point	The point or points in the execution of a NASA ITIL process where communication or exchange of information between service providers, customers, and end-users occur.
Underpinning Contract	A Contract between an IT Service contractor and a third party. The third party provides goods or services that support the delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.
Users	A person who uses the IT Service on a day-to-day basis. Users are distinct from Customers, as some Customers do not use the IT Service directly.

10 Acronym List

ACES	Agency Consolidated End-user Services
------	---------------------------------------

APM	Application Portfolio Management
BSMB	Business Systems Management Board
CAB	Change Advisory Board
CF-PWS	Cross-Functional Performance Work Statement
CI	Configuration ItemCI
CIL	Center Integration Lead
CIO	Chief Information Officer
CMDB	Configuration Management Database
CO	Contracting Officer
COTR	Contracting Officer's Technical Representative
CR	Change Request
EA	Enterprise Architecture
EAST	Enterprise Applications Service Technologies
ES&ID	Enterprise Service & Integration Division
ESD	Enterprise Service Desk
ESM	Enterprise Service Management
ESRS	Enterprise Service Request System
FDCCI	Federal Data Center Consolidation Initiative
I ³ P	IT Infrastructure Integration Program
ICAM	Identity, Credential, and Access Management
IRM	Information Resources Management
IT	Information Technology
IT PMB	IT Project Management Board
ITIL	IT Infrastructure Library
ITMB	IT Management Board
ITSCM	IT Service Continuity Management
ITSM	IT Service Management
LAN	Local Area Network
MSC	Mission Support Council

NAMS	NASA Access Management System
NCAD	NASA's Consolidated Active Directory
NEAR	NASA EA Repository
NICS	NASA Integrated Communications Services
OCIO	Office of the Chief Information Officer
PDA	Personal Digital Assistant
POC	Point of Contact
PWS	Performance Work Statement
RCA	Root Cause Analysis
RFC	Request for Change
SACM	Service Asset and Configuration Management
SE	Service Executive
SE&I	Systems Engineering & Integration
SIM	Service Integration Management
SLA	Service Level Agreement
SLM	Service Level Management
SLR	Service Level Requirements
SME	Subject Matter Expert
SOIL	Service Office Integration Lead
SOM	Service Office Manager
SPOC	Single Point of Contact
STRAW	System for Tracking and Registering Applications and Websites
TIM	Technical Integration Manager
TRM	Technical Reference Model
WAN	Wide Area Network
WESTPRIME	Web Enterprise Service Technologies

11 Referenced Document List

The following documents are applicable to the cross functional requirements:

- a. NASA Enterprise Service Management Concept of Operations
- b. NPR 7120.7 NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements
- c. NPR 2800.1, Managing Information Technology
- d. NPR 2810.1 Security of Information Technology
- e. NPR 2830.1 NASA Enterprise Architecture Procedures
- f. NPD 1000.0 NASA Strategic Management and Governance Handbook
- g. NASA Enterprise Service Desk Concept of Operations
- h. NASA Enterprise Service Desk Performance Work Statement
- i. NASA Enterprise Architecture Repository (NEAR) Interface Definition Specification (Not valid)
- j. Government Availability Management Process
- k. Government Capacity Management Process
- l. Government Change Management Process
- m. Government Incident Management Process
- n. Government Information Security Management procedures and policy
- o. Government IT Service Continuity Management Process
- p. Government Knowledge Management Process
- q. Government Problem Management Process
- r. Government Release and Deployment Management (RDM) procedures
- s. Government Release Plan (part of Government's Release and Deployment Management (RDM) procedures and policy)
- t. Government Request Fulfillment Process
- u. Government Service Asset and Configuration Management (SACM) Process
- v. Government Service Level Management Process
- w. Government Supplier Management Process