

Texas DCS Hybrid Cloud Services

1 Executive Summary

The purpose of this document is to explain the technical solutions supporting the DCS Hybrid Cloud Services (HCS) options.

HCS was introduced to the DCS program to provide customers with expanded cloud and self-management options, while meeting the business, security, and regulatory requirements of Texas state government. The services include Fully Managed and self-managed options, as well as DCS private community cloud and public government cloud options. It is a hybrid cloud offering because it provides the ability to use and connect all these different cloud environments, as illustrated below:

DCS Community Cloud	✓ <i>Avail. Sept 2017</i>	✓
Public Gov't Cloud	✓	✓
	Semi- Managed	Fully- Managed

1.1 Hybrid Cloud Service Options

Some of the key features and benefits of this service are:

- **Integrated DCS private community cloud with public government cloud** options in the consolidated data centers
- **Semi-managed and fully-managed** service options
- **Automated cloud self-provisioning**
- **Next generation tools & infrastructure** automation improving service delivery and infrastructure availability
- **Agility, transparency, and control** of customer IT infrastructure and financial spend
- **TAC 202** security compliance

To enable these services and provide an ordering experience that mirrors the market, the DCS Service Providers will implement new capabilities via a number of new tools. Capgemini will continue to

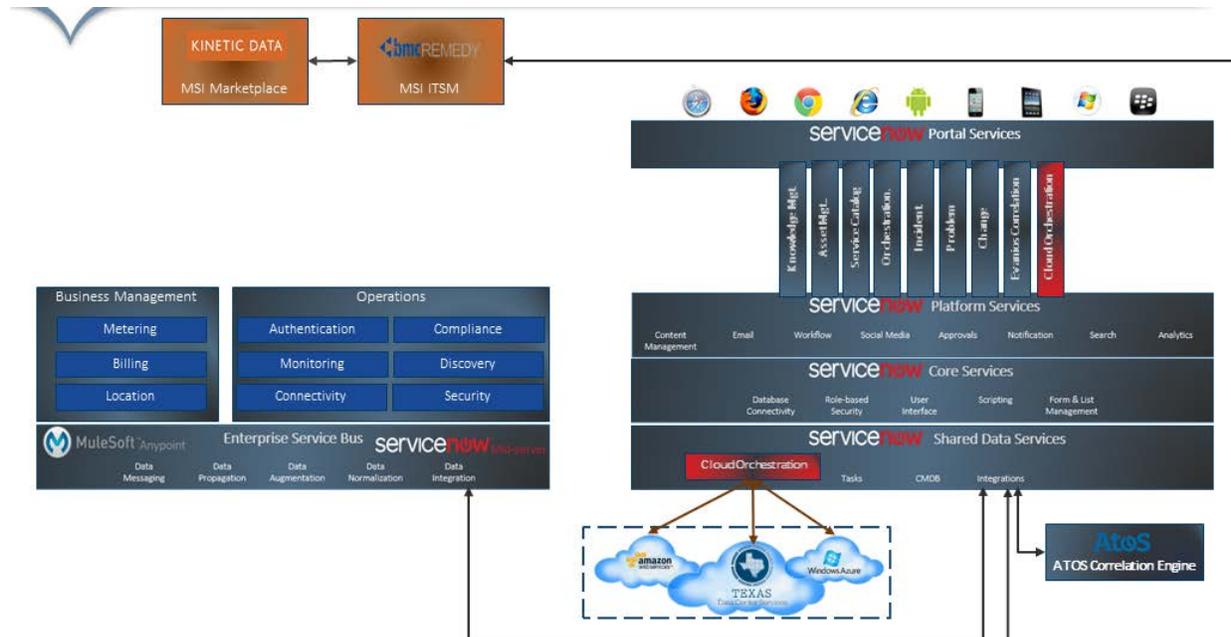
provide service integration and will enhance the user experience through a new marketplace for ordering cloud services.

- **Marketplace:** Includes service catalog for hybrid cloud services through the DCS private cloud and the public government cloud providers, enables shopping, selection and comparison of different build options, calculation of charges, review of shopping cart, and order submission
- **Data Quality Management:** Improves CMDB quality, validates data sources to create and maintain gold record

The Atos solution enables automated provisioning, which supports improved service delivery times and build quality, and automated incident management through the following tools:

- **Service Now:** Serves as the cloud resource orchestration system – acting on Marketplace requests and automatically provisioning the resources and services from the private cloud and public clouds
- **Virtual Data Center:** Allows private and public compute, storage, network, and security resources to be virtualized so provisioning and resources can be consumed more quickly, more efficiently, and in a standardized fashion
- **IPSoft:** Provides automation delivery and handling of detected incidents through its autonomic functionality
- **Enterprise Service Bus¹:** Enables interacting software applications to communicate without dependency on or knowledge of other systems on the bus

The diagram below shows key components of the logical architecture and their integration points.



¹ The ESB is a standalone project and is not part of the HCS program; however, it is included in this Overview document as the ESB is an essential component for enabling the HCS solution.

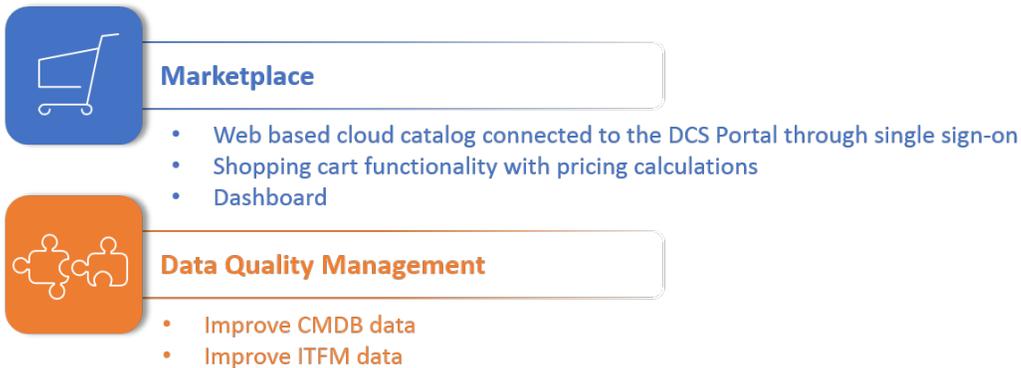
Additional detail on the solutions from Capgemini and Atos are summarized below. The full solution documents are memorialized within the Master Services Agreement as Attachment 8-B for the respective Service Provider.

2 Capgemini Solution

Capgemini's Service Integration solution enables enterprises to focus on business outcomes instead of IT service management challenges. For the DCS program, Capgemini delivers:

- Service Management and Service Desk
- Service Level Management and Service Reporting
- Security Management
- Disaster Recovery Planning
- Process, Tools, and Training
- Program and Project Management
- Service Asset and Configuration Management
- Invoice, Chargeback, Finance and Contract Management
- Agency Account Management and Communications
- Problem, Change, Availability Capacity and Major Incident Management

To enable hybrid cloud services, Capgemini is adding the Marketplace and Data Quality Management:



2.1 Marketplace

The Marketplace is a website accessed from the DCS Portal for ordering hybrid cloud services. The Marketplace enables users to:

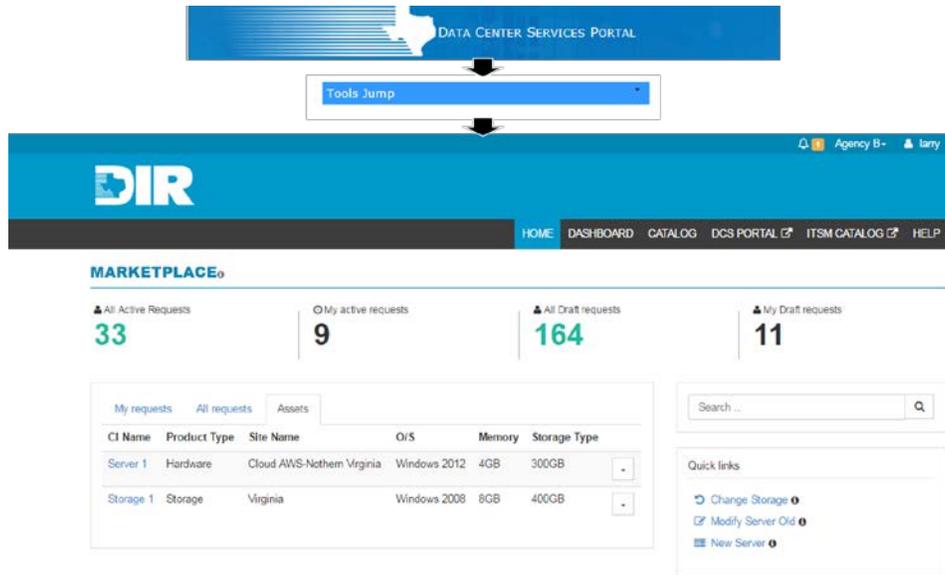
- View cloud service options
- Select and compare pricing for up to four options on one page
- Save selections to a shopping cart (draft)
- Submit the shopping cart to procure the items in the cart
- Select prior purchases to re-order, either with or without changes

Additionally, because the Marketplace is integrated with MSI and SCP tools it also:

- Displays the customer's cloud assets as recorded in the Configuration Management Data Base (CMDB)

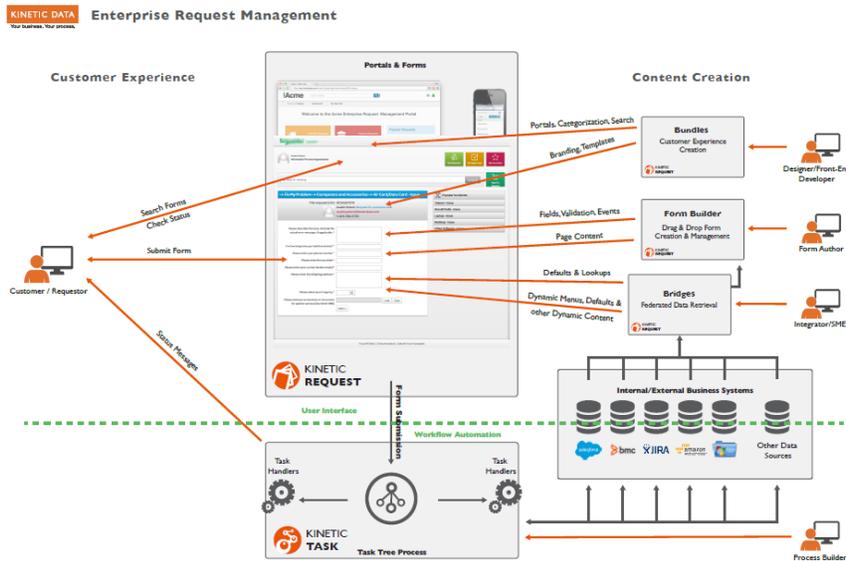
- Will start automated orchestration of the request, when Service Now is implemented (planned for January 2017 and described in the Atos solution below section below.)
- Start automated server build

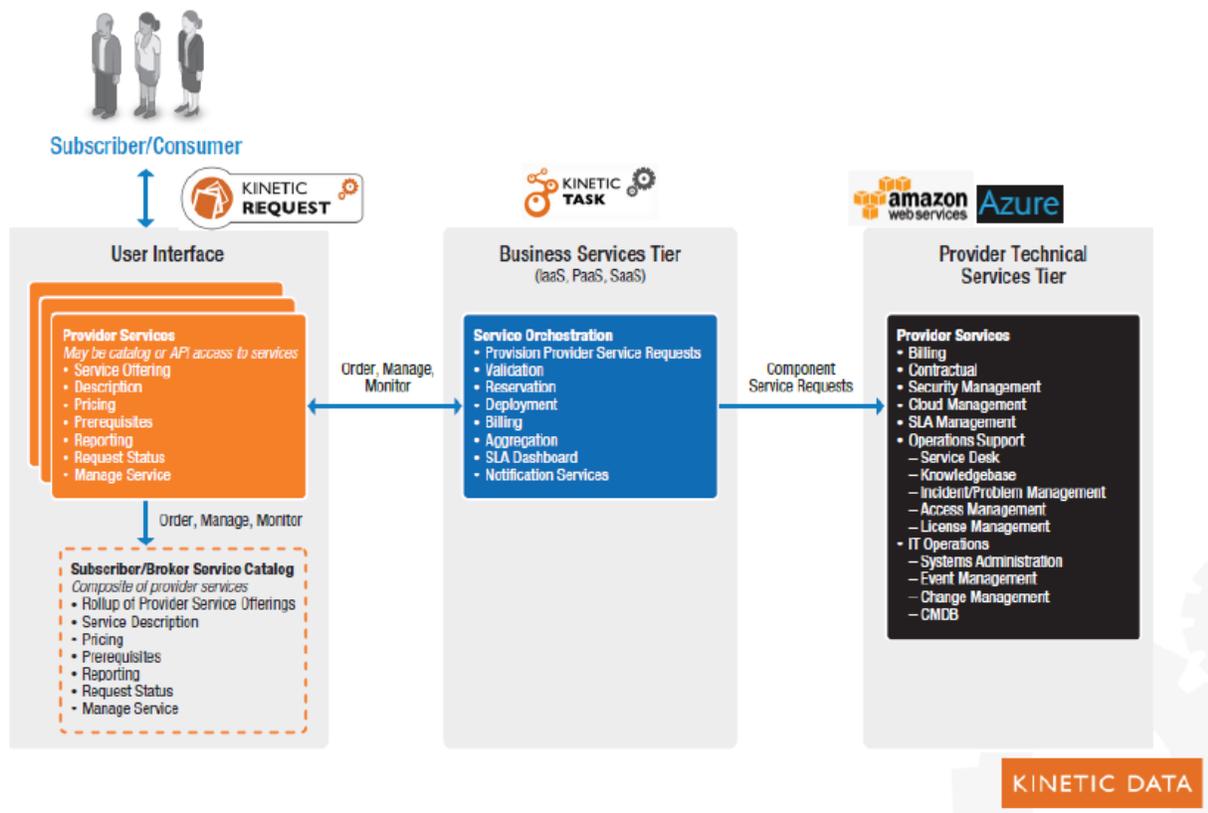
Draft screenshots of the Portal to Marketplace flow are shown below.



Kinetic Data

The Marketplace will be built using two products from Kinetic Data: Request and Task. The diagram below depicts how these two products work together and with other systems.





2.2 Data Quality Management

The Data Quality Management function will be fulfilled using Blazent tools. The Blazent Data Intelligence platform transforms and validates IT data, enabling enterprises and managed service providers to make business decisions based upon complete and accurate data. By leveraging a Data Quality Management solution, DCS will maximize IT data intelligence, while minimizing the cost and effort associated with managing data and the CMDB.

Blazent Product	Summary
Data Intelligence Platform	Provides flexibility, performance, and scalability necessary for big data processing Retains history of massive data sets while providing near real-time analytics
Data Quality Management	Reconciles multiple data sources to create user-configured Gold Records Performs identity management, relationship analysis, and purification of each CI Analyzes attributes, relationships, and status Manages all aspects of IT data quality Records and store all historical artifacts

Blazent Product	Summary
Data Explorer	At-a-glance view allows users to make fast data driven decisions for business objectives Intuitive interface enables easy configuration of role-based custom dashboards Enables ability to create analytics around custom attributes
Governance, Lifecycle Operational Validation, Expenditure (GLOVE)	Manages billing governance of assets under management for both MSI and SCPs Determine errors in lifecycle governance with continuous analytics Governs key auditable areas such as correct lifecycle status, account expenditures and assignment

3 Atos Solution

The goals of the proposed architecture are to automate key processes of server provisioning and incident management, answering the DCS Customers’ business needs of increased business velocity, agility, and process and cost efficiencies.

The Atos solution includes:



3.1 Automated Provisioning

Automated server provisioning allows customers to set up and make changes to information technology services directly, enabling a more efficient and rapid response to business requests and improving service delivery times. Automated provisioning will include self-service provisioning

Once automated provisioning has been implemented, DIR in conjunction with the Capgemini and Atos will ensure the services evolve with the needs of the business and the availability of new types of resources and services on the market.

The design and implementation of automated provisioning requires several fundamental building blocks.

3.1.1 ServiceNow

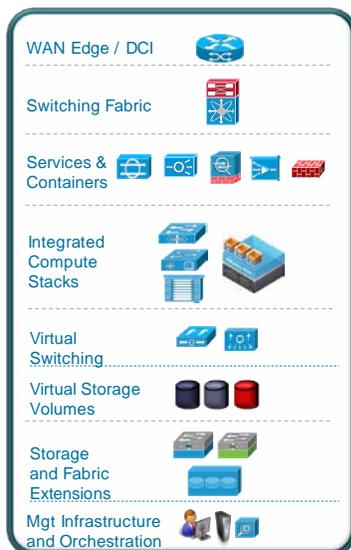
ServiceNow, also referred to as SNOW, will serve as the cloud resource orchestration system, acting on requests received from the Marketplace and provisioning the resources and services from the DCS Private Community Cloud and Public Government Clouds. The DCS Private Community Cloud will be the compute and storage resources available within the Consolidated Data Centers (CDCs). Public Government Clouds will initially include Amazon Web Services (AWS) and Azure (from Microsoft). As the Cloud landscape changes, ServiceNow provisioning allows for rapid additions of Cloud providers and Cloud resources.

When called, the ServiceNow Catalog entries launch Cloud Orchestration within ServiceNow to Provision and modify virtual servers/services as associated to the individual catalog entry in a DCS VDC. Updates back to Remedy are done via standard Web Service API to Remedy ARS and ultimately to the Atrium CMDB.

The ServiceNow interface into ITSM will maintain accurate with updates from the DCS tools in near real-time. This integration allows for an auditable flow and maintaining systems integrity.

3.1.2 Virtual Data Center (VDC)

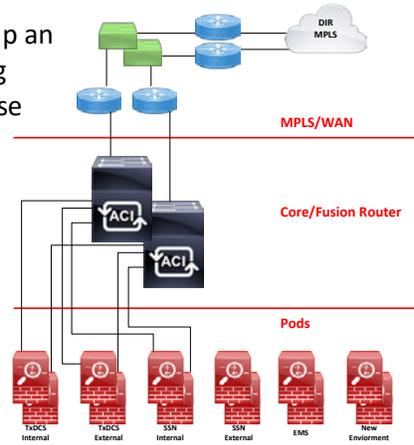
The VDC allows private and public compute, storage, network, and security resources to be virtualized so that the provisioning and use of resources can be consumed more quickly, more efficiently, and in a standardized fashion. The VDC is required to abstract the various hardware components into known, standardized, and easily consumable data center resources.



The VDC is composed of Virtual Hardware / Operating Systems, network, middleware, and storage across the State of Texas infrastructure and various Public and Private Clouds. These resources will span the CDCs as well as the public government cloud.

The Virtual Data Center allows for catalogs of cloud resources so these resources can be selected and deployed quickly. Resources may include standardized resources (e.g. network ports, firewall settings, storage types and sizes), but may also include custom settings that may spawn external manual tasks as required.

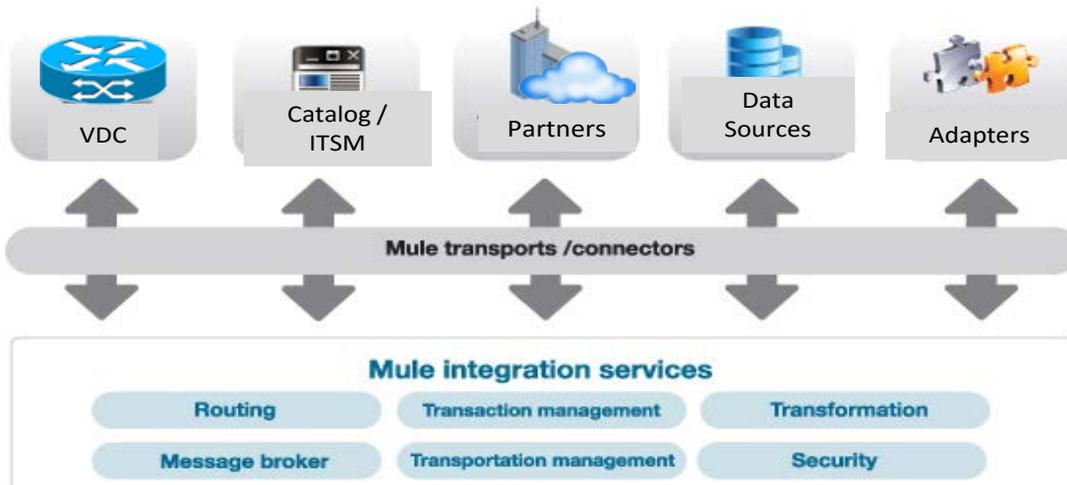
For example, with a request from a DCS Customer site to setup an environment with web servers and database servers requiring specific security settings for testing for each application release that include firewall rules. ServiceNow will interact with the VDC to automatically request and set up the necessary security settings eliminating the need for manual processes.



3.1.3 Enterprise Service Bus

The Enterprise Service Bus (ESB) is a system that enables communication between mutually interacting software applications in a service-oriented architecture (SOA). It is a set of rules and principles for integrating numerous applications together. The core concept of the ESB architecture is that different applications are integrated by putting a communication bus between them and then enable each application to talk to the bus. The ESB from MuleSoft allows all components of the Hybrid Cloud architecture to communicate with each other.

This ESB decouples applications and systems from each other, allowing them to communicate without dependency on or knowledge of other systems on the bus, thus moving away from point to point or direct interactions that are neither scalable nor manageable. For example, the ESB will enable communication between ServiceNow and the VDC.



3.2 Incident Management Automation

Incident and Problem management processes are key targets for automation, with the potential for significant improvement of service quality and performance and optimization of IT costs. To address Incident Management optimization, the SCP will deploy a solution from IPsoft.

3.2.1 IPsoft

IPsoft is an ITIL-aligned service management platform that provides automation delivery and handling of detected incidents through its autonomic functionality, thus increasing efficiency and quality of incident management.

IPsoft comes with a large knowledge base of incidents that have been collected by years of learning from hundreds of customer environments, including compute, storage, network, and security, Operating Systems, Databases, and Middleware. Associated with these recorded incidents are remediation tasks that have successfully resolved these incidents. The autonomics engine from IPsoft helps make the best choice of remediation for incidents.

4 Service Offerings

Finding a one size fits all solution for every customer's business need is nigh impossible. Customers have different sets of requirements for different types of applications; the Hybrid Cloud allows flexibility and customizable service offerings to meet differing needs. Through HCS, customers can select either Fully Managed services or Semi-Managed services. The following describes the two offerings.

4.1 Fully Managed Services

Fully Managed services are the services offered under DCS as defined in Exhibit 2.3 of the Master Services Agreement. In Fully Managed Services, the Service Provider is responsible for all aspects of the server life cycle, including the server build, ongoing operating system (OS) and hardware maintenance, and customer incident tickets, CRQs, and work orders.

4.2 Semi-Managed Services

Semi-managed services allow Customers additional flexibility in support of their systems. As part of the Hybrid Cloud Services approach, and consistent with current public cloud vendor support models whereby the end customer provides their own OS and application level support, the DCS program has added the concept of semi-managed servers. A semi-managed server is one where the customer takes on some of the responsibility the Service Provider would normally have. For semi-managed servers, the Service Provider will:

1. Build the server

2. Acquire, install, and patch the operating system
3. Install and maintain antivirus
4. Perform SIEM logging and critical watch reporting
5. Perform hardware container maintenance/reboots

Customers are responsible for all the remaining activities including:

1. OS management
2. Monitoring
3. Creating and managing incidents, changes, and work orders

NOTE: For semi-managed instances, Atos will only respond to incidents and work orders related to Hardware. Tickets related to Software, including OS, will be the responsibility of the DCS Customer. There may be some exceptions.

Services Matrix for Fully Managed vs. Semi-Managed Instances

Area	Service	Fully Managed			Semi-Managed		
		Cons	Non-Con	Cloud	Cons	Non-Con	Cloud
Application	Application Monitoring	S	S	S	NA	NA	NA
Capacity	Capacity Management, Planning, Alerting	S	S	S	NA	NA	NA
Database	Database Support, Management, and Maintenance	O	O	O	NA	NA	NA
DR	Disaster Recovery Support	S	S	S	S	S	S
DR	Disaster Recovery Services - Testing and Planning	O	O	O	NA	NA	NA
IAM	Identity and Access Management, including Authorized User support	S	S	S	NA	NA	NA
Middleware	Middleware Support, including Installation	O	O	O	NA	NA	NA
Monitoring	High Availability, OS, System Performance	S	S	S	NA	NA	NA
Operations	Batch Jobs / Processing	S	S	S	NA	NA	NA
Operations	Load Balancing	S	S	S	NA	NA	NA
Operations	Operational documentation (run books)	S	S	S	NA	NA	NA
Operations	Production Control and Scheduling	S	S	S	NA	NA	NA
Operations	Server Administration, DNS, Directory Services	S	S	S	NA	NA	NA
Operations	System Support - Reboots on HW only	S	S	S	S	S	S
Operations	System Support (Utilization, Management, Reporting)	S	S	S	NA	NA	NA
OS	OS Installation	S	S	S	S	S	S
OS	OS Management, Monitoring	S	S	S	NA	NA	NA
OS	OS Clustering	O	O	O	NA	NA	NA
Reporting	Software currency reporting, capacity reports	S	S	S	NA	NA	NA
Security	HIPS/HIDS	O	O	O	NA	NA	NA
Security	Security Certificates	S	S	S	NA	NA	NA
Service Desk	Incidents, Work Orders, Change Requests, Service Desk Support for HW and Standard Server Services as indicated by S in this table	S	S	S	S	S	S
Service Desk	Incidents, Work Orders, Change Requests, Service Desk Support for SW	S	S	S	NA	NA	NA
Software	Software support, installation, maintenance	S	S	S	NA	NA	NA