VIRGINIA IT AGENCY

Exhibit 2.3.1 MOD 23

Solution – MSI Services

VA-170822-SAIC

COMMONWEALTH OF VIRGINIA
VIRGINIA IT AGENCY (VITA)
SUPPLIER STRATEGY AND PERFORMANCE DIVISION

7325 BEAUFONT SPRINGS DRIVE
RICHMOND, VA 23225

This Page Intentionally Left Blank

TABLE OF CONTENTS

LIST OF FIGURES

1.0 INTRODUCTION

The SAIC Multisourcing Service Integrator (MSI) team brings strong Virginia-based capabilities that will continually deliver innovative Information Technology (IT) services to the Virginia Information Technologies Agency (VITA) and the Commonwealth of Virginia (COVA). These IT services will enable Virginia's citizens to improve their lives and Customers to create growth and enhance the personal security of those citizens. Our MSI solution, in close collaboration with the Service Tower Suppliers (STSs), will deliver those vital IT services by implementing and managing modern integrated technologies using mature standards-based processes that fulfill VITA's IT Infrastructure Services Program (ITISP) goals and objectives. Our solution accomplishes this by delivering the following:

1. A **Marketplace of Choices** that gives Customers an "easy to use" Service Catalog of purpose-built, flexible, cost-effective, and evolvable IT capabilities and that allows STSs to be changed based on their performance in bringing their best, most innovative, and cost-effective services to the Commonwealth
2. **Responsive Service Delivery** through implementation of highly automated Service Management Systems (SMS)
3. **Access to New Technology** driven by our implementation of Continual Service Improvement (CSI) linked with technology assessment and currency analysis, backed by experienced and efficient risk management techniques that implement effective security controls
4. A **Focus on Virginia's Mission** that pervades all our work through integration of our Business Relationship Management best practices that feed Customer information into key work areas (e.g., IT Service Strategy, Availability, Capacity, and Demand Management) to enhance their mission delivery
5. **Innovative Service Design** leading to **Efficient and Effective Service Operation** that is enabled and automated using our United Solutions™ Process Asset Library (PAL), which we have perfected over our 40 years of experience in IT service design and delivery. Our PAL incorporates and improves upon Information Technology Infrastructure Library (ITIL) v2011 best practices and executed by our highly qualified and experienced staff

We *maintain and improve service quality* by instilling a Virginia mission focus throughout all our efforts, through our Marketplace of Choices that enables innovative, efficient, effective service operation and delivery. We *ensure cost competitiveness* through our supplier management methods that result in the Marketplace of Choices and by providing access to newer and more cost-effective technologies. Finally, we provide a *highly visible, transparent, and accountable service delivery platform* through our automated and responsive SMS.

In the following sections, we detail our solution. The following table summarizes our offered past performance references and their relevance to the description of services as captured in VITA's MSI Exhibit 2.1

Description of Services	1.1	1.2	1.3	1.4	2.0	3.0	4.0	5.0	6.0	7.0
Vanguard 2.2.1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
USDA RMA Mission Support Integration Services (RMA III)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
USARC Data Center	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1.1 Service Management Practices

Our solution to provide MSI Services (**Figure 1.1-1**) centers on the implementation of mature processes highly aligned to the ITIL process framework. The ITIL Process Lifecycle captures each required process in a continuous flow from strategy, through design, transition, and operations, and into continual improvement, which is a key source for new service strategy initiatives.

Starting from the innermost area of **Figure 1.1-1**, the foundation of our solution is the ITIL life cycle, which includes our implementations of the ITIL life cycle functions. Moving out one level, we have integrated our ITIL life–cycle-based processes with our proven program management practices based on the Project Management Institute's (PMI's) Project Management Body of Knowledge (PMBOK®). This allows SAIC to provide Customers with comprehensive Project and Project Portfolio Management fully integrated with the operation and continual improvement of all IT services. For example, this integration permits the ITIL-based processes for managing change to use artifacts that we have extended to include program, portfolio, and Project Management best practices that assess the impact of changes in process and technology within the program, Portfolio, and Project domains.

SAIC has developed a set of highly mature processes, our United Solutions PAL, through more than four decades of engineering, IT service, and program management support of clients at every level of government. We have proven the value of our skilled personnel and management practices for state governments—including California, Hawaii, Utah, Tennessee, and Texas—and local governments—including the County of Orange, CA, and the District of Columbia. We have also successfully supported numerous U.S. federal government agencies, including ongoing programs for the worldwide requirements of National Aeronautics and Space Administration (NASA), the Department of State (DOS), and the Department of Defense (DoD) (e.g., U.S. Central Command [CENTCOM]). The mission-critical nature of these federal customers has driven our processes to be more complete than typical civilian work would require. This depth of experience provides us with direct, detailed, and intimate insight into our clients' needs, along with the knowledge and lessons learned to exceed the performance objectives for the COVA.
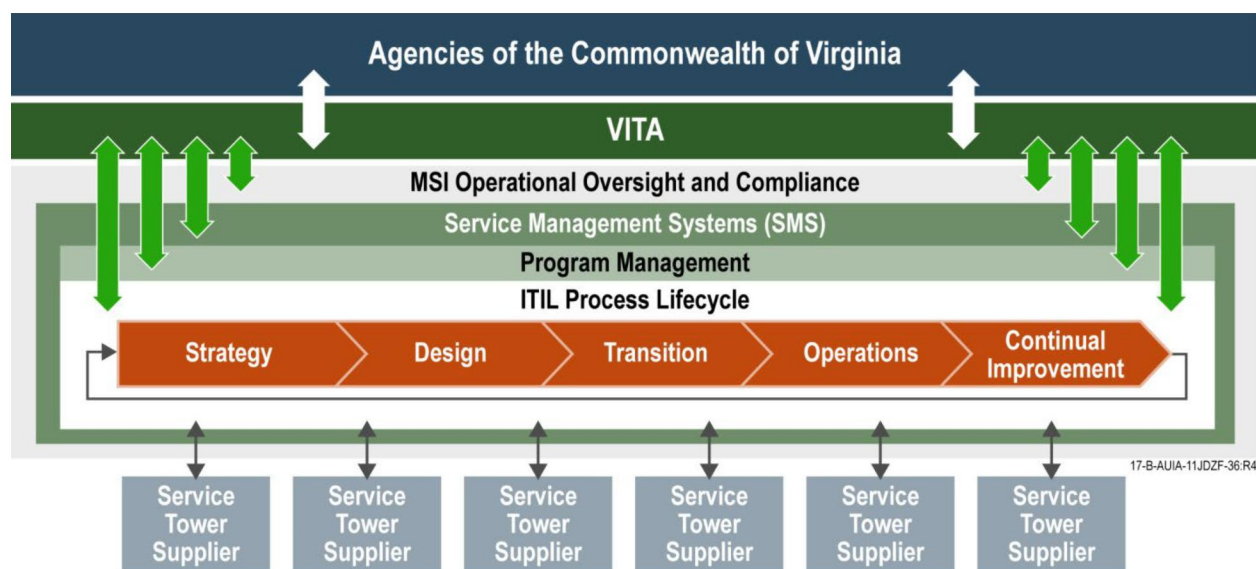
Figure 1.1-1. SAIC MSI Management Approach

Our proposed SMS provides VITA, Customers, and all service suppliers with a holistic workflow automation capability that enables fast, responsive service delivery. We have learned that a fully integrated process automation capability is necessary for the success of a multi-vendor service delivery program. One key element of SMS is our Keystone Edge™ service offering that integrates and provides the automated platform for ITIL-aligned processes and PMBOK-based program and Service Management. Our Keystone Edge service offering provides VITA with over 100 configuration and workflow customizations that provide comprehensive, efficient, and effective Project, portfolio, and IT Service Management within a central and common system and database. These configuration and workflow customizations allow us to rapidly bring new capabilities to VITA and the Commonwealth. The central database facilitates and enables direct analysis and reporting to correlate service and resource capacity

needs with Project scheduling, to relate Incidents to changes in the environment, and to document and forecast service consumption trends for each component of the Service Catalog and overall services portfolio.

Our structured IT management processes and automation are essential for providing the Commonwealth with a marketplace of service choices, founded upon new technology and focused on the Commonwealth's mission. This marketplace makes it easier to add and drop service suppliers based on new technology, improved or more cost-effective performance, or for inclusion of new services. The automated nature of the marketplace makes it easy for service suppliers to update their service offerings and provide them with the necessary data to help them evolve their services to the Commonwealth's needs.

The next layer of our solution (**Figure 1.1-1**) provides the comprehensive operational oversight and continuous compliance validation of all processes and Integrated Suppliers. Our SMS, through automation, enhances the expert oversight and ongoing collaboration and validation to ensure continued optimal service availability for the Commonwealth by providing the central source of "truth" (i.e., the central database of service delivery performance.) This comprehensive operational oversight is fully detailed in Exhibit 2.3.2. Key highlights of this aspect of our solution include the following:

◆ *Service Tower Supplier Integration.* The individual Service Tower Suppliers participate in ITIL-based life-cycle processes, such as Service Asset and Configuration Management (SACM) and Change, Incident, or Problem Management via structured interactions with our SMS that integrate with their own Service Management processes. VITA-selected STS entities will utilize our provided SMS directly to maximize service integration and to minimize complexity and duplication of management systems that normally increase costs. If VITA selects and authorizes an STS that uses its own Service Management components, our SMS solution offers the flexibility of industry-standard interfaces for bi-directional communications between the STS and our SMS. In both cases, the central and common database and path to process participation is via the MSI SMS that are subject to the controls of operational oversight and compliance. This ensures consistency and integrity of the SMS as the system of record for reporting and analysis of all services to VITA and Customers. This approach also allows VITA to easily and rapidly change or expand the mix of Service Tower Suppliers from which it may draw upon to meet the requirements of each Customer.

◆ *Control, Transparency, and Expanded Service Access.* In our approach, VITA and its Customers participate in the operational oversight and direction to the ITISP via workflows that we also enable by SMS automation. This provides fast, responsive service delivery. VITA retains control over definition of each process implementation. Both VITA and Customers have access, based on VITA-defined authorization controls, to each component of the SMS to provide comprehensive and transparent operational visibility and to assess supplier compliance supported by ongoing MSI reporting and analysis. Our implemented Service Management practices will enable VITA to offer the broader range of vetted and qualified services to each Customer in a manner that improves customer service and satisfaction. MSI operational oversight and compliance activities provide individual Customers with actionable information on the specific services they consume, and MSI support for continual improvement of services provides VITA with the understanding to increase the efficiency, quality, and breadth of IT services and technologies available.

1.2 Main Processes

Our solution incorporates and fully integrates each of the primary processes identified within Exhibit 2.1 via a delivery organization composed of three overarching functional areas:

◆ *Enterprise Operations (EO).* Our Account Manager leads our EO functional area. EO consists of highly skilled professional teams that perform and manage the operational processes for Incident, Event, Problem, Request, and Configuration Management. It includes a comprehensive, Virginia-based

Service Desk for direct support of Customer Users, and a Joint IT Operations Center (JOC), in proximity to VITA's primary data center, to conduct process operations and coordinate response across suppliers to Major Incidents and Problems. Both operate 24/7/365. EO also provides for the continuous operations of the SMS.

◆ *Program Office.* Our Project Executive leads our Program Office. The Program Office includes our Program Management Office (PMO) that performs all aspects of Demand Management, Project and Project Portfolio Management, and fully coordinated Change and Release Management. Our Demand Management and change approaches include a professional Business Relationship Manager and IT Financial Management teams that directly interface with and assist VITA's Customer Account Managers (CAMs) so that the MSI fully understands any Demand Management adjustments and change impacts, and so that any resultant IT environment changes will be communicated to the appropriate Customers. The Project and Portfolio Management aspects of this organization shepherd results from the Service Strategy and Service Design stages of the ITIL model through Service Transition and into Service Operations.

◆ *Architecture, Strategy, and Design.* Our Chief Technology Architect leads our Architecture, Strategy and Design (ASD) functional area. This area evaluates new technologies and service approaches for efficiency, maturity, security, and, above all, effectiveness and value to the Commonwealth, resulting in an expanded Service Catalog available to all Customers. SAIC ASD teams support strategy generation and will perform IT technology planning, overarching Capacity Management, Service Continuity Management, and CSI. The CSI team will review both MSI and Service Tower Supplier services, processes, and procedures for optimization and cycle innovation into all ITIL life cycle phases.

The SAIC MSI organization is Customer-focused. We understand that to achieve a high level of customer satisfaction from our Customer, our mission is to continually delight Customers so that VITA is their premier provider of multisourcing integration services. We accomplish this through a responsive, innovative, communicative, and collaborative organization that continually seeks to understand and define Customer requirements and then, using our extensive automation capabilities, delivers the right services—quickly—while maintaining full operational visibility. Our project team is structured to guide the overall ITIL implementation effort, and improve solution design, solution communication, and solution acceptance.

Figure 1.2-1 illustrates our organization for VITA MSI.

The SAIC Team's organizational approach is built on five principles, recognizing that VITA MSI requires an integrated framework of processes and controls to maximize value, minimize disruption, and sustain IT services delivery at expected performance levels.

◆ Provide a light-weight, flexible, responsive organization to act as an extension of VITA's IT management team in that it participates in the ITISP Governance processes and collaborates with VITA to establish and improve governance processes, particularly at the operational layer, with specific responsibilities for Customer engagement of those consuming IT services aligned to the Operational Governance model
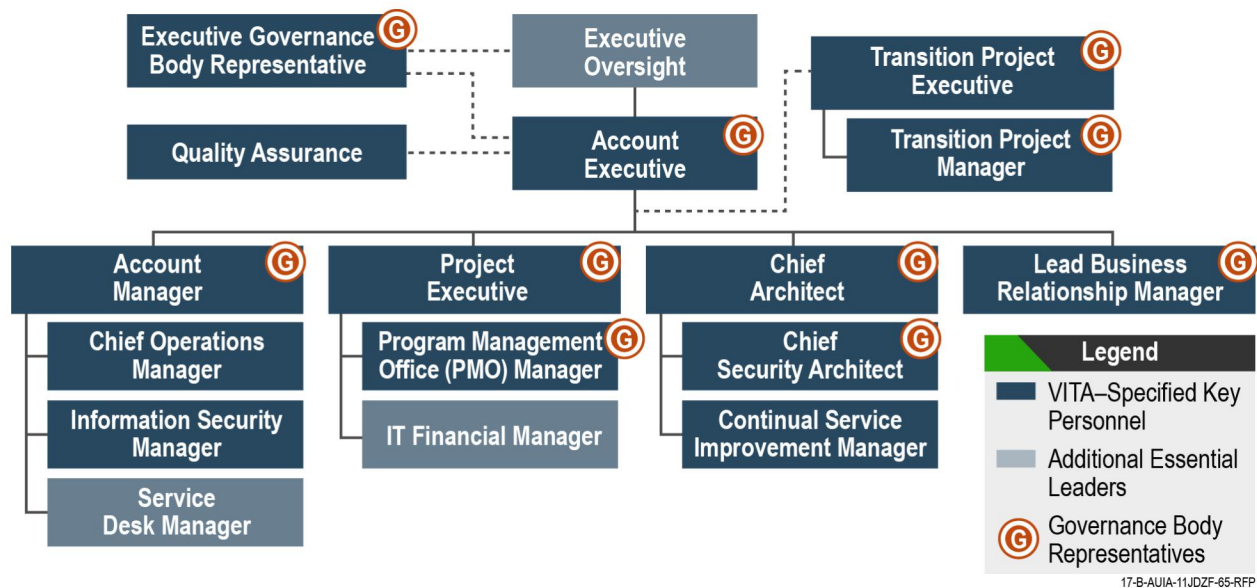
Figure 1.2-1. The SAIC Team Project Organization. *We provide a customer-focused organization to encourage communication and collaboration in an ITIL-based structure.*

◆ Provide MSI experts in system integration, Program Management, Strategic Planning, and Customer engagement and advocacy to deliver planning, management, and monitoring of the delivery of IT services to VITA Customers

◆ Deliver Customer focused services—staffed with experienced Business Relationship Managers with the experience to assist with translating these Customer needs into technology requirements

◆ Offer fast, visible, automated services, provisioned rapidly, under full operational visibility (transparency) that is only possible with the type of extensive, automated integration provided by the SAIC Team

◆ Locate and hire staff, keeping Virginia first and creating jobs for the Commonwealth

Our framework incorporates the processes across the five ITIL life-cycle stages of Strategy, Design, Transition, Operation, and Continual Service Improvement, and leverages people, processes, technology, tools, and physical facilities to efficiently and consistently maximize the value of VITA's investment in IT and the delivery of quality services.

Level of Access and Authority

SAIC defines level of access and authority in terms of the size, complexity, and cost of the request. The SAIC Team understands that immediate decisions are sometimes necessary to keep a project moving in a process-dependent environment. We facilitate decision-making at the lowest possible level, enabling operational managers to commit resources based on their level of access against time and cost thresholds established across the organization. For example, if the request is to have one person for eight hours, the front-line manager can commit that resource without escalation. If the resource request, however, is for three people for a week, this decision would need to move to the level of the SAIC Team Project organization that has the authority to decide within that scope. The highest-level positions are responsible for higher thresholds. In all cases, SAIC provides immediate action at the appropriate level, enabling rapid resolution of unexpected events while controlling risk. Our approach substantiates our commitment to customer satisfaction and successful performance against all service levels. **Figure 1.2-2** provides the access and span of control for each member of our key personnel team.

Role	Access/Span of Control
Account Executive	◆ Accountable for overall contract performance and oversight ◆ Faceoff with key VITA leadership including Executive Director, and Platform Relationship Office ◆ Authority to make decisions with respect to SAIC program actions ◆ Focused on day-to-day running of organization ◆ Senior SAIC executive leadership for VITA
Executive Governance Body Representative	◆ Participates in Executive Alignment Governance Meetings and Relationship Management Committee ◆ Direct access with SAIC executive leadership to: — Align corporate investment and R&D initiatives with VITA's future, long-term vision — Maintain immediate access to corporate reach-back resources
Account Manager	◆ Accountable for services delivery ◆ Customer satisfaction and service level attainment ◆ Authority to make decisions with respect to the ordinary course of day-to-day performance of services ◆ Participates in Operational Governance Forums ◆ Span of Control over the Service Desk, Joint Operations, and Information Security Operations
Chief Operations Manager	◆ Joint Operations Center response coordination ◆ Incident and Event Management ◆ Problem Management ◆ SLA compliance measurement and reporting ◆ Service Catalog and Request Management ◆ Change and Release Management ◆ Service Asset and Configuration management (SACM) ◆ MSI Platform Administration
Information Security Manager	◆ Security Event and Incident Management ◆ Identity and access management (IAM) administration
Project Executive	◆ Span of Control over the PMO, the Business Relationship team and IT Financial Management
Program Management Office (PMO) Manager	◆ Oversight and responsibility to manage MSI, STS, and third-party service providers ◆ Demand, Project and Portfolio Management ◆ Request for Solution Management ◆ Service Management Manual (SMM) administration ◆ Documentation and reporting management
Lead Business Relationship Manager	◆ Customer assistance and support ◆ Program Customer satisfaction ◆ STS relationship management
Chief Architect	◆ Span of Control over the IT Architecture, Continual Service Improvement, IT Engineering, Service Continuity Management, and Technology Currency Management
Chief Security Architect	◆ Information Security Management System (ISMS) program management ◆ Risk Management ◆ Information Security policy and procedure compliance ◆ Third-party audit coordination
Continual Service Improvement Manager	◆ Process compliance and quality assurance ◆ Process maturity assessment ◆ Process and operational improvement

Role	Access/Span of Control
Transition Project Executive	◆ Accountable for implementation performance ◆ SAIC Corporate executive interface ◆ Implementation Governance ◆ Vendor Implementation Relationships ◆ Supports VITA's Organizational Change Management (OCM)
Transition Project Manager	◆ ITISP program implementation ◆ Implementation of risk mitigation

Figure 1.2-2. Access and Span of Control for SAIC Project Team Members. *All project team leaders have full authority to perform assigned roles with direct access to applicable SAIC resources and management.*

SAIC will use the processes as documented in VITA's existing Policy and Procedures Manual as the starting point for the development of processes the ITISP will use to provide services. During Implementation, we will leverage SAIC's United Solutions PAL (**Figure 1.2-3**) and work with VITA to update the SMM. United Solutions is a robust set of standardized Project Management, engineering, and IT Service Management (ITSM) processes and tools. SAIC has populated this process framework based on our more than 40 years of experience with critical federal, state, and local government entities. We use this process set as the basis for our International Organization for Standardization (ISO) 9001:2008, ISO 20000-1:2011, and ISO 27001:2013 location certifications. We continually refine and improve our United Solutions processes, leveraging our experiences using ITIL, PMI best practices and PMBOK content, agile
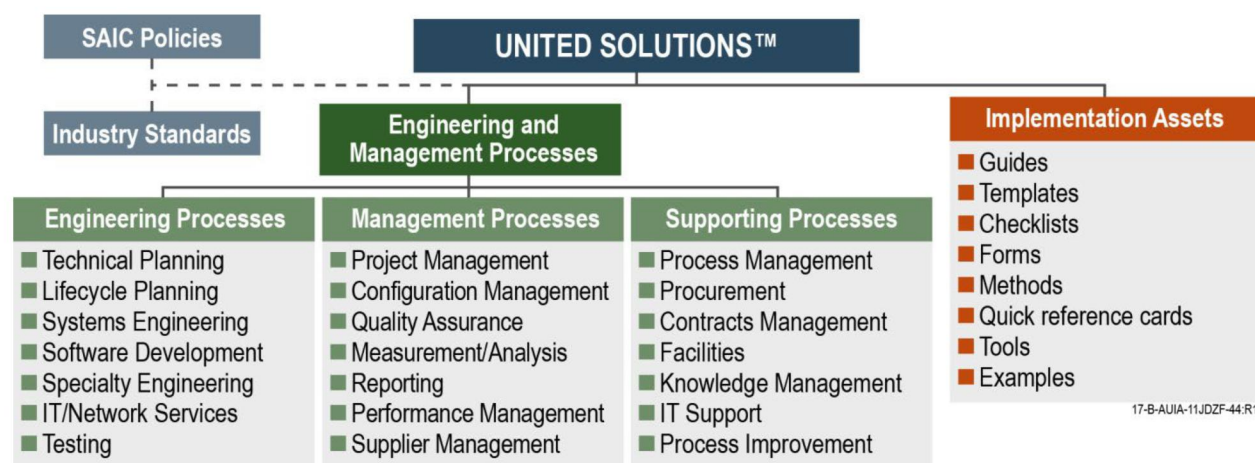
Figure 1.2-3. Processes Within United Solutions PAL
Will Speed The Development of The Service Management Manual (SMM)

and DevOps best practices, and Systems Engineering (SE) "V" Model artifacts producing a reliable, repeatable catalogue of proven processes. This toolset is under a disciplined CSI process to improve service quality and houses all baselined process-related documentation. We will select and customize the United Solutions framework and process assets to align with the SMM as approved by VITA or ITISP Governance, and implement them using automation in Keystone Edge. **Figure 1.2-3** shows the resources found within the United Solutions PAL.

1.3   Service Integration

Our solution provides inherent support for the integration of all primary processes through our common SMS — described below — that is accessible to, and used by VITA, Customers, all MSI personnel, and each STS. The SAIC solution includes three-party collaboration – VITA, MSI, and STS – to establish Operating Level Agreements (OLAs) for the MSI and each Service Tower Supplier that codifies the specific responsibilities each party bears to each other. We have implemented this ITSM approach for many clients, including the County of Orange, DOS (Vanguard), U.S. Army Reserve (Data Center), and U.S.

CENTCOM where we manage services across multiple providers or vendors with which the client holds the direct contractual relationship. In some cases for these referenced client relationships, we provide aspects of the MSI and supplier role, thereby providing us with intimate insight in how to collaborate effectively with the STSs. Through the OLA mechanism, each supplier always understands what it must provide, the manner in which it must be provided, and how that provision will be measured in order to work seamlessly for the benefit of the Commonwealth.

The SAIC Team views OLAs as living documents that evolve over time through a process of ITISP Governance in which all parties participate. As the MSI, we not only facilitate the governance process (as detailed in our response to Exhibit 2.3.2), but ensure that its artifacts are recorded, with version control and review/approval history within the document management components of our SMS, and are integrated within the overall SMM hosted within it. We continuously monitor the operation and status of the document system and the SMM content (See Section 1.4).

Our approach to Service Integration includes continuous monitoring of compliance to all relevant ITISP policies and processes. We view monitoring as a core MSI responsibility as compliance issues must be remediated immediately, and in some cases, will carry contractual or service level agreement (SLA)-related credits or other consequences. Of often-greater importance, however, is that close attention to compliance is essential to revealing areas in which processes and/or procedures should be improved. Our CSI program (See Section 7) recognizes the opportunity presented by compliance issues to advance the overall maturity of the integrated program—processes that are efficient, well documented, easily understood, and highly automated resulting in greater compliance. Higher levels of compliance benefit the Commonwealth with improved efficiency and effectiveness of service delivery.

Our CSI program includes process compliance monitoring with both on-demand and regularly scheduled reporting. Our solution requires biannual process compliance and Capability Maturity Model Integration (CMMI) assessments of the entire integrated supplier process and sub-process to drive higher maturity throughout the program, resulting in broader implementation of standardized, repeatable processes. Furthermore, SAIC proposes to assess existing VITA CMMI processes using our ITIL Maturity Assessment framework as part of our proposed implementation of services described in our response to Exhibit 2.4. This initial assessment of the current state allows SAIC to tailor our implementation and integration of services to minimize disruptions and identify processes that do not need immediate improvement during the implementation period.

1.4   Service Management Systems

SAIC's SMS (**Figure 1.4-1**) consist of five modules, the core of which is provided by SAIC's Keystone Edge, based on the ServiceNow product family. The other four components are Collaborative Enterprise Navigational Toolset Environment and Repository (CENTER™), the Security Suite, the Cloud and Financial Management Suite, and the Information Security Management System (ISMS). The Keystone Edge component is a highly integrated platform for ITSM providing the IT Portal, unified data store, and comprehensive process and workflow automation for all aspects of the Services. Within this platform, SAIC has implemented over 100 customizations to data structures, process relationships, automated workflows, and advanced reporting to provide Customers with efficient, effective, and innovative IT Service Management. SAIC has deployed and currently uses the Keystone Edge platform in support of over 35 commercial clients and agencies at all levels of government, bringing those clients a responsive marketplace of services and access to new technology.

Our SMS automate the management of all Incidents, Service Requests, Problems, Changes, and Releases as well as hosting the Configuration Management Database (CMDB) and the ongoing performance of SACM. It hosts our Knowledge Management system to provide all Customers with direct access to curated knowledge articles and training materials for IT services and for authorized STS entities and third parties

to contribute knowledge and receive computer-based training (CBT) in the use of the MSI SMS and VITA-approved policies and procedures.

The SMS supports reporting on-demand, on an ad hoc basis, at defined intervals (with electronic delivery) and, for specific data subsets, in real time. Extensive usage, analytic, trending, and custom reporting is available to the Commonwealth.

17-B-AUIA-11JDZF-35:R5
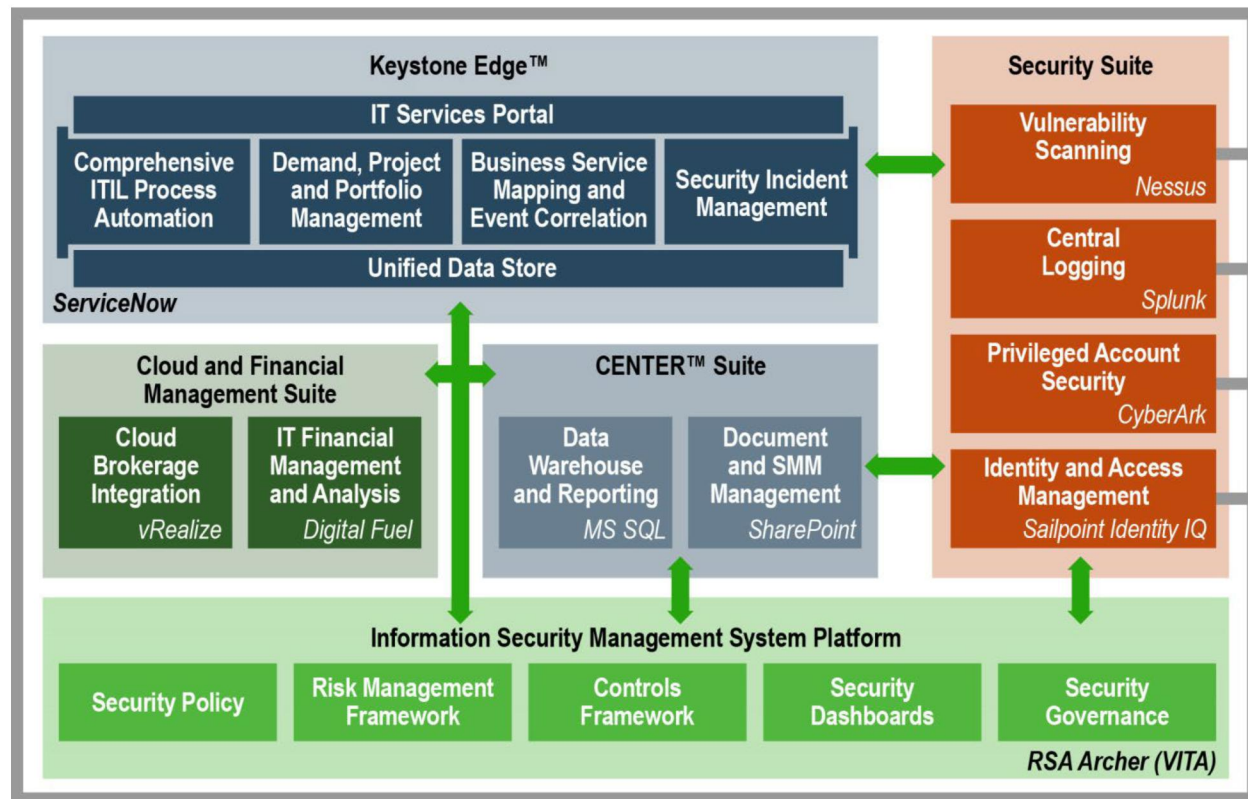
Figure 1.4-1. SAIC's SMS, Consisting of Keystone Edge and integrated SMS Components, Provides An Integrated Automated Capability Supporting Program Management and All ITIL Life Cycle Phases

Keystone Edge also provides centralized automation for our PMBOK-based management of Projects and Project Portfolios. It provides full life-cycle support for the qualification, sizing, evaluation, and approval of demand requests that may ultimately result in chartered Projects, requests for change, or Service Requests. We will utilize the Project Portfolio Management (PPM) capability of Keystone Edge because it provides a single source of truth to the Project Managers and full visibility into Project status for stakeholders using a simple web interface and via a single application. This PPM capability is accomplished through direct integration with real-time updates with all of the other information in Keystone Edge. Additionally, SAIC is providing a Microsoft Project Server instance for added flexibility in supporting Project scheduling and resource management. Our solution also supports Primavera. Keystone Edge captures the relationships in the Configuration Management Database (CMDB) between Configuration Items (CIs) to support visual mapping of business services and correlation of events from across STS entities and services to support identification of Project dependencies. Keystone Edge provides a single source of truth regarding Projects and services, automation for service ordering and reporting, and flexible User interfaces that allow for customized dashboards and data analytics.
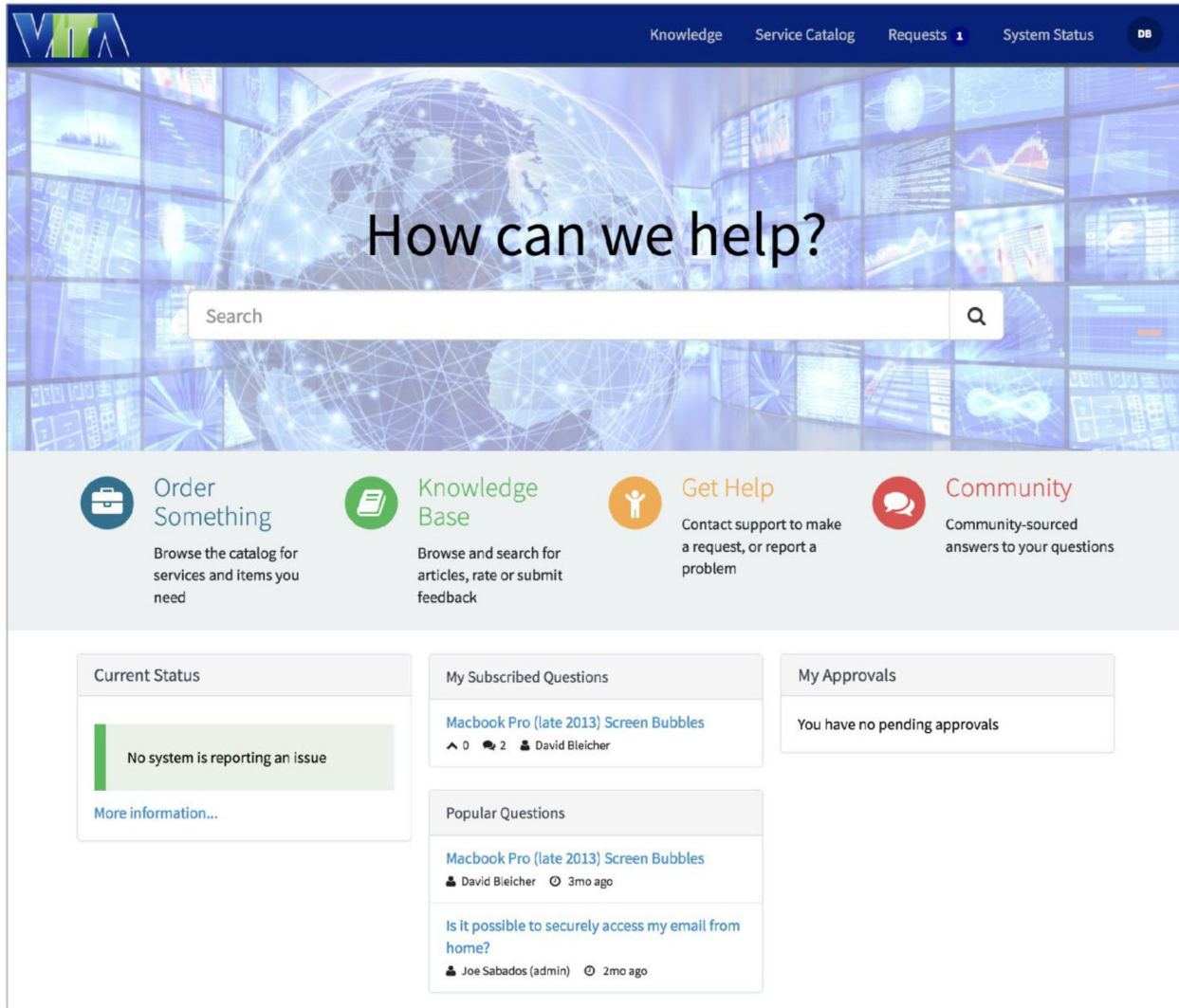
Figure 1.4-2. Example Keystone Edge Service Portal

IT Services Portal: The Keystone Edge Service Portal (**Figure 1.4-2**) provides access to all IT services and support from a single, customized, User-centric interface. Through this portal interface, authorized Commonwealth Users have the ability to:

◆ Quickly view the current status of services and system

◆ Directly enter reports of Incidents or requests for support

◆ Access SAIC's extensive knowledgebase of curated support and training articles for self-service resolution of questions and issues

◆ Access and order, as authorized, hardware, software, and services from the comprehensive Service Catalog (i.e., marketplace of services)

◆ Immediately see the status of any/all pending requests for services or support

◆ View any outstanding requests for approval a User is required to address

SAIC will customize the Service Portal for each Commonwealth Secretariat if requested. This would include the underlying service menus of the Service Portal page presenting tailored and relevant views of the services and information. However, for ease of personnel movement between Secretariats, SAIC encourages as much Service Portal uniformity as possible. Note that individual, group, Customer and Secretariat home pages have significant customization capabilities. SAIC will provide customization for the

main Service Portal as well as one per Commonwealth Secretariat. Customizations for group and personal home pages will be completed by Customers with assistance from SAIC if requested.

Our SMS solution also includes community messaging functions—similar to instant chatting/ messaging and subject to VITA approval—to allow Users to communicate helpful information with each other and to directly provide suggestions (with attribution or anonymously) for new services or service improvements back to the MSI, VITA, and STSs.

The SMS enables Customer issue self-resolution (i.e., self-help), which our experience has shown us improves the User experience. Keystone Edge permits Customers to identify opportunities to improve their internal business processes by leveraging its data and capabilities.

To complete SAIC's SMS solution, we integrate the Keystone Edge platform with four service-specific automation suites.

The CENTER Suite provides:

◆ *Document Management & Repository.* This CENTER component will act as the primary document repository for the SMM and for the publication and version control of all document artifacts related to MSI services. It utilizes Microsoft SharePoint technologies with Keystone Edge-specific integrations and controls.

◆ *Data Warehouse & Reporting.* This CENTER component provides User-defined queries and ad-hoc reporting capabilities of integrated ITSM data to authorized Commonwealth Users. It permits defined reports to be saved for later re-use and/or retention under version control. It utilizes a Microsoft SQL Server instance and associated reporting services.

The Cloud and Financial Management Suite provides:

◆ *Cloud Brokerage Integration.* Advanced provisioning, monitoring, and control of cloud-based services, including the tracking of performance and life-cycle of authorized Commonwealth SaaS, PaaS, and IaaS services are provided by VMware's vRealize Automation and tools. These tools are integrated fully into Keystone Edge through its Application Programming Interfaces (APIs) and with a broad range of cloud service provider systems to provide direct provisioning workflow and integration with virtualization and network infrastructure of STS entities as authorized by VITA. Additional details regarding these components are described in Section 7.7 of this document.

◆ *IT Financial Management.* Comprehensive tracking, allocation, analysis, and chargeback reporting of financial information related to consumption of IT services including Project resource, Service Request, and Service Catalog consumption are tracked by Digital Fuel and integrated into Keystone Edge with financial information exposed by VITA-retained financial systems through integration between Keystone Edge and VITA's designated financial system(s). This automation provides Customers with direct, interactive access to IT service billing, forecasts, and budgetary comparisons. Additional details of this solution are described in Section 3.3 of this document.

The **Information Security Management System** supports our overall, National Institute of Standards and Technology (NIST)-aligned approach described in Section 4. This system will integrate with VITA's existing RSA Archer system to provide information security Governance, Risk, and Compliance (GRC) support. The system includes management and automation for security policies, the Risk Management Framework (RMF), Controls Framework, security dashboards, and GRC via VITA's Archer. The SAIC RMF is hosted on our SAIC CENTER suite. CENTER also provides a centralized location for risk and controls life-cycle management activities, and will contain risk registers, logs, risk assessments, controls, assessments of controls effectiveness, action plans, Plans of Actions and Milestones (POAMs), and other artifacts required to provide an end-to-end, policy-based security program across the Managed Environment. SAIC will integrate our ISMS automation components and processes, in a bi-directional manner, with Archer to maximize the value of VITA's existing investment in this technology.

The **Security Suite** provides vulnerability scanning, central logging, privileged account security, and Identity and Access Management. Together, Sailpoint IdentityIQ and CyberArk Privileged Account Security Solution Identity and Access Management (IAM) provide comprehensive IAM automation for all MSI, Service Tower Supplier, and VITA-specified systems. They also provide integration and federation with external systems. This suite provides fine-grained control over User account management, rights and access in a seamless, consistent fashion. Splunk provides centralized logging service, an ability to correlate events with other forms of actionable threat intelligence, and security data analytics. Nessus provides for automated scanning against a wide variety of standards, threats, and vulnerabilities providing a rapid approach to assessment of gaps with applicable standards, including Payment Card Industry, Center for Internet Security, and the Defense Information Systems Agency (DISA) Security Technical Implementation Guides, amongst many others.

SAIC has developed integrations between Keystone Edge and each of the platform extensions to provide seamless operation of the full SMS. Platform and tool suites are fully integrated at the API level with bidirectional data exchange leveraging industry-standard web services protocols. The solution provides all 24 of the requested SMS components and satisfies the requirements specified in Exhibit 2.1 Section 1.4.

Our solution will host the vRealize Suite, Digital Fuel, CENTER Suite, ISMS Components, and IAM solutions within the VITA data center environments on ITISP-provided/managed hardware systems. We will deploy the Keystone Edge platform within the ServiceNow-managed cloud environment, with primary hosting in the ServiceNow Culpepper, VA, data center on high availability (HA) infrastructure. For redundancy, failover, and continuous operations during upgrades, secondary hosting is provided within ServiceNow's San Jose, CA, data center facilities. This deployment approach provides VITA and its Customers with the following key advantages:

◆ Primary platform hosting within the Commonwealth
◆ Secure access by authorized personnel from any location
◆ Reliable, continuous operations for use by VITA, Customer, MSI, Service Tower Supplier, and Third Party Vendor personnel within Virginia, including SAIC's primary Service Desk located in Southwest VA, with uninterrupted, simultaneous access from secondary Service Desk and support locations should a primary location experience outages

2.0 PROGRAM MANAGEMENT

To provide efficient, effective, and responsive service delivery within the MSI structure, SAIC will tailor the automation of Program Management Office (PMO) processes within our SMS to the specific VITA requirements. This will provide VITA with improved oversight, reporting, and reduced turn-around times for new technology implementation Projects that will provide new or modified services within the marketplace of service choices for Commonwealth agencies. Keystone Edge and CENTER facilitate the PMO's automated operation and incorporate tools such as Microsoft Project Server.

SAIC's PMO solution is designed to effectively manage the portfolio of IT Projects across the state to ensure VITA is responsive to Customer needs and to support the citizens of the Commonwealth through effective utilization of the state's IT budget. In our approach, the PMO is the core management organization supporting the key activities of Project assurance, Project support, Knowledge Management, standardization, training and development, and governance. For Project Management, we use the PMBOK life cycle and focus on the monitoring and controlling work in progress since support and compliance to standards is necessary to ensure all STS collaboratively work towards the Commonwealth's IT strategic service delivery goals and objectives. In our role as the MSI, we use our PMBOK-based approach to resolve issues at the lowest level possible by (i.) communicating the principle of lowest-level issue resolution among all ITISP participants, (ii.) clearly articulating decision-making authority based on ITISP role, and

(iii.) by open communication, dialog, and guidance between the SAIC Team and the STSs to ensure understanding of how the lowest level resolution applies to specific issues.

We will meet all of the requirements outlined in Exhibit 2.1, Section 2 for Program Management (PMgt) of the MSI and provide a PMO to oversee all Projects, standardize processes, and be VITA's advocate to its Customers. We will also adhere to the Commonwealth's Project Management Policy and Standard, as required by VITA and PMI best practices for Project and program management and operating a PMO.

2.1 Program Management Office (PMO)

To implement and manage the ITISP framework, SAIC will provide VITA a PMO that has oversight and responsibility to manage MSI, STS, and Third Party Vendors. The PMO will implement integrated managerial and IT Service Management discipline, processes, and procedures that focus on (i.) maintaining and improving service quality provided by the MSI, STSs, and Third Party Vendors; (ii.) managing a portfolio of Projects providing cost-effective and competitive desired services to the agencies; and (iii.) providing the visibility and accountability to VITA that ensures alignment between stakeholder needs and innovative, high-quality IT service delivery.

The PMO will take the lead role in coordinating implementation and transition activities between STSs, the Incumbent and VITA. This will include serving as the primary point of contact during disentanglement of the Incumbent and implementation of new STSs. The PMO will use best efforts to resolve issues and will escalate to VITA if necessary. If and to the extent VITA has engaged the services of the DART Team, the PMO will coordinate disentanglement and implementation activities with the DART Team.

The PMO's disentanglement and implementation acitivies will include the following:

- Overseeing STS implementation and disentanglement plans and activities

- Managing asset transfer from Incumbent to incoming STS or VITA, as appropriate

- Facilitating knowledge transfer from Incumbent to incoming STS or VITA, as appropriate

> **Case Study USDA – Agile PMO Services**
>
> USDA's Risk Management Agency (RMA) relies on SAIC's PMO to deliver their *RMAgile* Software Delivery initiative. The *RMAgile* delivery model has quantifiably reduced the time to production for legislatively mandated changes and increased the delivered quality (less outages, fewer failed changes, and less rework). Moreover, to effectively support project portfolio management and reporting, SAIC developed the customizable *RMAgile* methodology to direct all aspects of program and project management, planning, and control to efficiently manage all staff and ensure that deliverables are short-term and focused. This included current and ongoing projects and solutions requests as well as on-going programs. All PMs and Business Analysts were trained in *RMAgile* and used it daily. *RMAgile* provides innovative project management tools that yielded significant value to the government, including project status dashboards that enabled frequent project-status communication. SAIC's dashboard adds clarity to the weekly project status deck with an at-a-glance view of all active projects and their key success factors. The dashboard includes the project's status, percent complete compared to the target, percent change from the previous week, and items of note.

- Facilitating communications and activities between STSs and Incumbent regarding Incumbent personnel resources

SAIC bases our PMO solution on industry best practices that continually align with the current PMBOK, as documented in our United Solutions PAL and tailored to the Commonwealth's Program Management Policy and Standards, so that we can guide collaboration and alignment between VITA, customers, ITISP Governance, and the STS. SAIC will bring Agile methodologies as part of our toolset for operating the PMO for the VITA MSI. Agile-PMO is an adaptive methodology that allows for quick, tangible progression to the ultimate business goal. It is best deployed when end-to-end clarity of paths and/or risks are complex, while still providing an effective framework of measurement, control and accountability.

SAIC worked closely with the U.S. Department of Agriculture (as outlined in the adjacent customer past performance vignette) to develop an Agile PMO approach that was highly successful. Likewise, SAIC will utilize Agile innovations, other appropriate Project Management techniques and best practices that enhance our PMO's utility for VITA's stakeholders. This will enable ease of interaction, and provide an efficient, lightweight Project Management support infrastructure.

As noted by Chuck Cobb in his book "Making Sense of Agile Project Management," in considering an Agile PMO one must recognize that "the role of the PMO becomes more of an advisory role and a consultative role rather than a controlling role. The function of the PMO should be to put in place well-trained people coupled with the right process and tools to make the process most effective and efficient and to keep it well-aligned with the company's business."

We will collect, document, and publish our standard practices in the SMM. Within the ITIL life-cycle phases, we will document the PMO aspects of Demand Management, Project Portfolio Management, and fully coordinated Change Management and Release Management in the SMM.

To support an MSI environment, SAIC's PMO solution features the following innovative and responsive features:
◆ Provides an adaptive service framework to quickly respond to changing conditions and service delivery needs in the Commonwealth
◆ Leverages Keystone Edge SMS to plan for and be ready to fulfill fluctuations in demand
◆ Improves integration of processes and procedures to automate the management of the SMM, rapidly onboard new suppliers, and manage the provisioning of improved services
◆ Provides a means to incentivize agencies to come to VITA first for solution and service support
◆ Embodies continuous process and quality improvement in PMO practices
◆ Enhances communication and awareness across the enterprise via open and automated reporting

We designed our PMO to establish a management and communications framework to support VITA in the management of requests for IT services, solutions, and associated projects across the state. Our priorities for implementation upon award are to establish the PMO associated processes, procedures, and tools within the SMS, establish a concept of operations (CONOPS) and associated policies for resource management, and configure SAIC-provided PMO IT tools to provide VITA immediate (i.e., "Day One") benefits. Our resource management process will be backed by our SMS' single source of truth. We will begin with an accurate asset inventory and supplement this by ensuring we get accurate and timely data from the STS. This coupled with our own quality assurance processes and updates to the SMS will ensure we have an up-to-date accurate view of the resources available within the Commonwealth. By managing the Projects in the SMS we will bring both the resource demands and availability together into a single view and effectively manage any resource contention. Our preference would be for Customers to also include their resources in the SMS, but where this is not practical or possible we can work with the Business Relationship Managers (BRMs) to get an accurate picture of the Customer resource availability.

Using the PMO framework as defined in the CONOPS, SAIC will manage a pool of Project staff resources, including Project Managers (PMs) at various skill sets and experience, assigned based upon factors such as risk, complexity, funding value, and other criteria defined and agreed upon with VITA. SAIC will evaluate and report on estimated future demand of PM and other project resources (e.g., quality assurance, technical architect) and work with VITA, agencies, and STS to modify resource pools to meet demand. This project resource pool will include STS PMs. SAIC will coordinate with the STS's to determine availability of the PMs and utilize our Keystone Edge SMS to also track their workload. All PMs supporting the MSI will be Project Management Professional (PMP)-certified and will take the one-day Commonwealth PM orientation training session. SAIC will ensure PM's assigned to the PM resource pool have documented their certifications, education and experience and vet that documentation against their respective

contractual requirements. SAIC will assign projects, sub-projects, and tasks to the various PMs as appropriate. The SAIC PMO will provide a single consolidated report on project schedule and budget and variances will be handled in a uniform fashion via a consistent process that will be developed during implementation. When conflicts arise between various projects, the SAIC PMO will resolve the constraints through prioritization established with the ITISP. The SAIC PMO will ensure that project artifacts are delivered and stored in the Document Data Store and that projects are managed in accordance with the requirements documented within the Service Management Manual.

SAIC's experience in using a PMO to manage programs has shown that a fully integrated enterprise operation and management structure is the most beneficial. In our experience, scalable, open solutions like our Keystone Edge-based SMS are responsive to the ever-increasing pace of technical improvements and meet the key support requirements of a PMO.

Keystone Edge is our single system of record for the MSI PMO. We will use Keystone Edge Project Portfolio Management to centralize Demand Management and align resources to business strategy. Its built-in collaboration tools and workflow automation will enable provisioning of high‑quality services faster, improving productivity and response time. Through these automations, our SMS enables our staff to efficiently manage projects from ideation to project execution to completion. Stakeholders will get visibility all the way through service transition to production and other ongoing operations.

SAIC will coordinate and integrate STSs for each existing and planned Customer Project. Coordination in a direct, controlled interaction between STSs in Customer-sponsored Projects allows for the reduction in "lost in translation" problems. Integration and STS "buy-in" allows for faster problem escalation when needed and encourages resolution of issues and risk identification between STSs, resulting in fewer demands on VITA for project problem resolution. SAIC will, via STS OLAs, require participation in QA and CSI activities.

The SAIC MSI PMO will support all aspects of solution proposal development in a collaborative manner, engaging the Customer, VITA, STSs, and any required Third Party Vendors. The SAIC MSI PMO will coordinate all aspects of proposal creation, including requirements gathering, cost analysis, schedules, risk, and resource requirements. SAIC will integrate this process into the Demand Management process to standardize the process flow of proposal creation. Each proposal creation effort will be tracked and monitored in the SMS to allow for automation of progress reporting and on-demand inquiries into activities.

SAIC reviewed the Project data provided by VITA to determine the number of Project Managers required by the MSI.

Exhibit 2.6 from the RFP indicated four types of projects in the pre-ITISP environment:
◆ Commonwealth Projects
◆ Infrastructure Projects
◆ Ongoing Programs
◆ Solution Requests

The PMO will support Commonwealth Projects in terms of schedule coordination and impacts on other Projects or Customers. The MSI will coordinate closely with the VITA Project Management Division (PMD) and Customer-assigned PMs where applicable. A combination of the MSI's ASD organization and PMO will provide the primary support needed. Since infrastructure will be provided by the STS or Third Party Vendors, it is expected that PM services will be provided by the supplying provider. Where coordination between multiple STSs is required, an MSI project manager will be assigned to provide Project integration and oversight of STS Project Managers.

The PMO will fully support the scope and volume of the Infrastructure Projects provided.

The PMO will fully support the scope and volume of the Ongoing Programs provided.

AS VITA notes, "Solution Requests require requirements assessment, proposal development and implementation. They are requested by the Customer and solutioned and managed by the Supplier."

It was also important to delineate what constitutes a Project and where the Project Management responsibility lies (PMO, STS, VITA, or Customer). We are consistent with the Commonwealth's Project Management guidelines and policies and are in support of the requirements of Exhibit 2.1, Section 2.0.

The approach to determine if a Solution Request requires PMO Project Management support will be determined in accordance with the SMM, and may include the four factors listed and explained below.

1. Is the Solution Request a stand-alone project?
2. Is the Solution Request the normal responsibility of the STS requiring minimal cross-coordination?
3. Does the requesting Customer have qualified project management resources to support the Solution Request?
4. What are the estimated one-time costs for the Solution Request?

In determining if a Solution Request should be treated as a Project supported by the PMO it is important to understand if it can be completed without any significant resource needs or cross-tower coordination. All Service Catalog orders are not considered Projects. However, a significant number of the same Service Catalog item may be considered part of a small project requiring support if it:

a. Affects a large number of Users at a single Customer.
b. Requires new network circuits be installed to support its operation.
c. Requires coordination between multiple STSs.

It should be pointed out that the above list is not all inclusive and there may be other factors to consider.

In determining if a Solution Request should be treated as a Project supported by the PMO we also consider whether or not it is the normal responsibility of the STS to manage the work.

Customers subject to Commonwealth Project Management governance requirements select Project Managers for their IT projects based on guidelines supplied by the VITA PMD. The PMO will provide the necessary PM tools and framework to support the Customer PM, as applicable. The PMO will serve a single point of coordination for the Customer PM to ensure necessary support from the STS and reporting to VITA.

SAIC will categorize Projects and standardize their management controls and mechanisms using our SMS and in accordance with the SMM. The SMS ITIL integration with Demand Management allows for service solution or requests to be entered into the workflow from multiple means (e.g., Service Desk, online form, email), thereby funneling all requests for project support through the Demand Management module. This provides a method to automate categorization of Projects by risk, complexity, and funding in an unbiased fashion. Since information is centralized in the SMS, our PMO will assign proper resources, policies, processes, and procedures, and implement gate reviews and rules to ensure compliance with the VITA SMM.

The SAIC PMO will facilitate and manage cross-contractor and cross-Customer Projects. By "cross-contractor" we are primarily referring to Projects that involve multiple STSs. SAIC does recognize that Customers may have the occasional need for services from a Third Party Vendor to support a Project. The SAIC PMO would provide the necessary level of Project Management support in those cases where the PMO is supporting a Customer that requires a Third Party Vendor. Likewise, if the PMO has support responsibility for a Project that involves multiple Customers, we will provide the necessary Project Management support and work closely with the assigned BRMs. SAIC will hold regularly scheduled Operational Governance forums to facilitate information exchange with VITA, Customer, STS, and – as

applicable – Third Party Vendor staff to ensure coordination and participation. The PMO will participate in collaborative pilot projects across STS and conduct forums to discuss changes to the enterprise architecture, technology trends, business trends, and integration opportunities.

The PMO will ensure that PMs will track Project status daily, weekly, or biweekly and by "walking the halls." We will deal with deviations quickly and make adjustments as required. PMs will proactively interact with technical staff for status so the Project can quickly progress to the next stage of development. They will enter relevant project status information (e.g., technical, schedule, budget, risk status) into the SMS as required by the SMM. This gives VITA, Customers, and STS a rapid response mechanism to keep Projects on track before problems occur.

By implementing our standardized approach to program and Project Management—one that can be followed and adhered to by all stakeholders and integrated with our Keystone Edge SMS component to provide a single source of truth—we eliminate the possibility of a stove-piped, disparate, out-of-sync Project and increase the probability of successful implementation.

2.2   Project Portfolio Management and Reporting System

SAIC will provide VITA a mechanism to track and report the Portfolio of Projects and programs associated with the ITISP. The system will enable reporting of status, schedules, task assignments, issues, and risks. SAIC's solution is to simplify and automate the Project Portfolio Management and Reporting System. Project Portfolio Management within Keystone Edge will be the module used to centralize Demand Management and align resources to business strategy. Keystone Edge will facilitate the rationalization of resources by ensuring we are maximizing the effectiveness of their use or providing recommendations for their redeployment where applicable. By having our Architecture, Strategy and Design team continually involved at the necessary waypoints in rolling out a project we are assured that resource rationalization considerations are made each time. Up-to-date and complete inputs into Keystone Edge by the STS also ensures we have a complete picture of the Commonwealth's IT resource available. Finally, the MSI is responsible for managing resources and ensuring their most efficient use. For example as we are monitoring software license usage we will be providing recommendations to VITA or Customers. First we collect data on SW licenses, their allocation and use from STS tools integrated into our Service Asset and Configuration Management (SACM) system. Next, based on that data collected we are able to report on license utilization and trends. Those reports form the basis for recommendations including purchase of additional licenses if over-utilized or reduction in licenses if under-allocated or underutilized. This will help to either quickly identify a problem or achieve a potential cost savings for the Commonwealth.

We will use our SMS to provide complete, clear, and current information that will inform VITA stakeholders about achievement of their (or related) portfolio objectives.

The Keystone Edge SMS component has a powerful and easy to use Project Portfolio Management and Reporting System (**Figure 2.2-1**) that supports alignment of demand request objectives with project execution metrics. This enables project and portfolio decision-making to ensure we are "doing the right work." This PPM is part of the Keystone Edge system, bringing the benefit of a single system to track the entire end-to-end lifecycle of a project. This provides VITA a way to see the entire portfolio from inception-of-ideas through project-close-out.

The Keystone Edge PPM supports other leading Project Management software such as Microsoft Project and Primavera P6. This tool flexibility allows Customer and STS PMs to work with their system of comfort while still providing VITA project plans, progress to schedule, cost, and scope necessary for control. The SAIC Project portfolio process manages and reports on project performance across the entire life cycle of a project.

Collaboration tools within Keystone Edge will deliver high‑quality services faster, improving productivity. Keystone Edge will be SAIC's single system of engagement for the PMO, allowing staff to manage Projects from initial idea to Project execution. Stakeholders will get visibility all the way through service transition to production and other ongoing operations.

Any Project request enters through the Demand Management process. The SMS filters demands using all necessary information to be considered for a proposal. The SMS portfolio module provides insight into how the proposed Projects align with VITA objectives and provides recommendations for what Projects to include. The portfolio module also allows for "what-if" scenario planning through modifications to Project elements, which are then compared to other Projects in the portfolio displayed graphically in four quadrants using stoplight charting. This gives VITA an unbiased methodology for determining which ones pass the first gate and a simplified view of the Project size, feasibility, and Return on Investment (ROI). It provides a simple comparison to other potential projects. It also provides unified reporting and dashboards for VITA to quickly see the status on the IT infrastructure and health of IT systems.
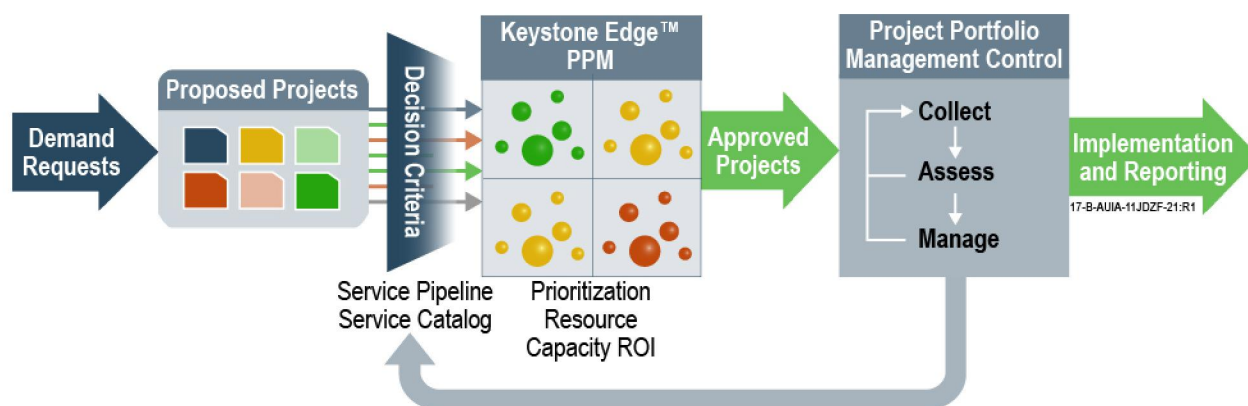
Figure 2.2-1. Project Portfolio Management Life Cycle

Other "what-if" scenario planning tools within our SMS include the CIO Roadmap view that allows our PMO and Architecture, Strategy and Design team to graphically view and move along a timeline of Projects for a mix of Customer- and Commonwealth-wide programs, to determine timing and impacts from Project schedule changes. These various tools within the SMS allow the authorized VITA Users to model various "what-if" scenarios to schedule, cost, risk, and scope and determine the impacts or support prioritization decisions.

2.3   Current and Ongoing Projects and Solution Requests

At any given time, VITA is managing approved "work-in-process" Projects that may be managed by different methodologies. Our solution assesses the status, risks, and remaining work on these Projects so that we can immediately begin managing VITA's planned and in-flight projects. The SAIC Team will learn and follow existing processes outlined in the SMM during program implementation.

Projects that are identified as Current Projects will be the first Projects to be entered into the SMS's Project and Portfolio Management and Reporting System during implementation. SAIC will determine the level of complexity, risk, and funding and will assign a qualified PM to pick up Project Management duties during and after transition/ implementation, as applicable. Upon Effective Date or otherwise in accordance with the Implementation Plan, SAIC will conduct interviews with all outgoing contractor PMs and, where necessary, shadow all outgoing PMs to rapidly gain understanding of the project. During this stage, SAIC will gather necessary information and status of these Projects to learn where the Project is in the Project life cycle and to evaluate the health of the project. We will evaluate the health of existing Projects during implementation. For Projects that are in need of remediation, escalation, and reporting of

the issues, we will initiate a Corrective Action in the SMS to track and report on the actions taken to bring the Project back to acceptable health.

SAIC will assign personnel to assess the existing Project Management environment as part of the Program Management Office Implementation Module including the SMM, management practices, tracking methods, data elements used for tracking, and Project reporting. SAIC will determine any gaps by identifying differences in the existing and proposed processes. This allows for SAIC to interact with Customers and VITA personnel, focusing only on the differences between the outgoing practices and SAIC's incoming practices. The goal is to minimize costs from process adjustments, making small changes if needed both in SAIC's new processes to integrate Keystone Edge and the Commonwealth's existing processes. SAIC will give the existing PMs for these Projects Keystone Edge Very Important Person (VIP) training. SAIC's approach is focused on maintaining project momentum for VITA and its stakeholders, while transitioning the project to a desired, standardized, and centralized method using Keystone Edge.

2.4 On-Going Programs

VITA maintains support for critical enterprise initiatives, called On-Going Programs, that must be initiated, executed, and accomplished within specific timeframes regardless of competing operational efforts. SAIC will engage early, and periodically afterward, with VITA to attain an inventory of the Projects needed to support On-Going Programs, along with their essential timeframes and objectives. SAIC will enter these Projects into the Project and Portfolio Management and Reporting System of the SMS for tracking and monitoring in the Portfolio Management process. When necessary, custom data fields, specific to VITA On-Going Programs, will be included in the SMS to indicate Project alignment with the On-Going Programs and to enable tracking their impacts.

SAIC will track activities, achievement of milestones, and any necessary reporting for On-Going Programs and distribute the reports to stakeholders on an agreed-upon schedule. We will tailor customizable dashboards for near–real-time management. Based on On-Going Program User collaboration, we will configure tracking and monitoring rules with VITA Project Management requirements, enabling automated escalation when thresholds such as risk or cost exceed VITA rules. Our Portfolio Management capability described above will allow VITA to know if investment levels are being properly managed, schedules are on track, and any associated issues have been resolved or risks mitigated. The SMS will send automated email, text, and screen pop-ups to notify designated personnel of issues or risk. The SMS is configurable to the rules as outlined in the SMM and has the flexibility to be modified with minimal effort when changes to the SMM occur.

SAIC will assess On-Going Programs Project compliance with ITISP Governance, applicable state laws, federal regulation and mandates and will facilitate forums and compliance groups on a quarterly basis to evaluate compliance. When non-conformance to ITISP Governance or VITA Rules is identified, we will initiate activities within the CSI or QA process for corrective action and remediation of the non-conforming elements.

3.0 SERVICE STRATEGY

3.1 Strategy Generation and Management

The strategy generation and management approach is a key starting point for enhancing Virginia's service to its citizens. SAIC has found that the ability to continually update and improve the Service Catalog, and bring new and innovative services to Customers and VITA requires a highly collaborative and transparent IT strategic planning and road-mapping approach that includes the key influential and candid stakeholders drawn from VITA's customers, Commonwealth agencies and sub-agencies, STSs, MSI, and Third Party Vendors.

SAIC's approach to strategy generation and management begins during program implementation with an early start-up of the Business Relationship Management process that engages with VITA CAMS to establish the trustful relationship with Customers and the Supplier Management process that does the same with the STSs and other suppliers. Establishing these relationships is a critical success factor for the implementation of the ITISP framework since good stakeholder relationships will enable the free flow of issues, ideas, innovative concepts, and candid communication that are fundamental for the generation of a successful and implementable strategy that balances the needs of each Customer with the consolidated needs of the Commonwealth.

Soon after these relationships have been initiated, we will launch strategy generation activities. We use a six-phase strategy generation approach (**Figure 3.1-1**) to establish or annually update the IT Service Strategy:

1. *Determining the mandate and scope.* This phase identifies key regulatory requirements, strategic Commonwealth and Customer business needs, and technological realities (i.e., a given technology is at end-of-life and must be replaced) that the IT Services Strategy must support and identifies the strategy's scope so that it does not attempt to accomplish too much or "boil the ocean."
2. *Assessing strategy drivers and constraints.* Identifies the budgets, legislative or technical hurdles that need to be accommodated or, via the strategy, overcome
3. *Evaluating the current IT state.* Determines the existing service delivery performance and any key issues that influence service delivery.
4. *Developing a target state vision.* Uses structured interviewing and facilitated meetings within ITISP Governance to gain consensus on the IT service end state and the associated goals and objectives needed to achieve the vision.
5. *Defining the initiatives.* Uses ITISP Governance again to identify the program or Projects that are needed to achieve the strategy's goals and objectives. We may use methodologies such as "Design Thinking" (a methodology to creatively solve complex problems) with small focused groups to solve particularly difficult problems.
6. *Building the initiative roadmap.* This establishes the IT Technology Plan (See Section 3.2) underpinning the IT Service Strategy.
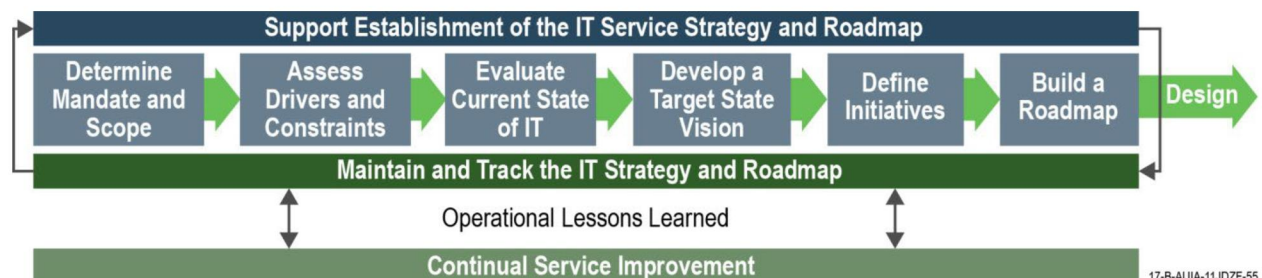

Figure 3.1-1. SAIC's Strategy Generation and Management Effectively Enables The Service Design Approach To Evolve VITA's Service Offerings In Alignment With The Commonwealth's Business Strategy

Our approach additionally takes advantage of our CSI process by integrating operational lessons learned to help drive future iterations of the service strategy. Additionally we support the ITIL Design phase activities by establishing the, framework and coordination with the other service tower suppliers to enable effective integration with the enterprise strategy. We track the strategy phase activities by maintaining status of the initiatives using our Project Portfolio Management and Reporting System (See Section 2.2). An inherent aspect of any strategy is that the defined strategy will change, even over an annual update cycle. To maintain the IT Service Strategy, we will proactively identify issues that will affect the strategy or its execution.

To provide proper oversight, SAIC uses a well-defined communication plan to maintain constant collaboration with the STS as they develop the strategy for the new initiative. This communication plan will safeguard that the intake process is followed and feedback to the STS is provided in a timely manner to expedite development. These issues may include identification of disruptive technologies, changes in budgets or funding, change in political strategy, or poor project execution. We will use the forums and decision-making framework as defined in the SMM to provide VITA and Customers the information necessary to understand the identified strategic issue and render an appropriate decision.

3.2 IT Technology Planning

SAIC's solution for IT technology planning is a logical extension of our IT strategy generation approach. It uses as inputs the prioritized Commonwealth and Customer initiatives from the IT Service Strategy above, Process and Technology Currency and Innovation plans from the CSI approach in Section 7, MSI or STS new service proposals, and technology vendor forecasts. We first begin by logically breaking down the IT Service Strategy initiatives into a set of candidate Projects. Second, we map the Currency and Innovations Plan activities or Projects, new service proposals, and vendor forecasts into the candidate Projects, modifying their scope as necessary to achieve alignment. Third, we perform dependency analyses on the candidate Projects to obtain their logical sequencing, and we estimate each Project's approximate size, length, and cost, adjusting the sequencing as necessary. Lastly, we estimate Project risks and adjust the Project sequencing to minimize risk to the Commonwealth.

We facilitate our IT technology planning approach by continually updating plans (i.e., roadmaps) that lay out technology-based Projects in a visual schedule format. These maps identify key dependencies, trends, and decision points that are used to proactively support and inform the ITISP Governance process. They depict interconnectivities within technology areas (e.g., products, standards, emerging technologies) and are essential for understanding how a change in one Project or technology area affects other areas. We will complete and deliver a full set of technology roadmaps and plans yearly, review them in an annual technology event, and provide VITA with semi-annual technology plan briefings.

3.3 Financial Management

In the pre-ITISP environment, VITA utilizes multiple cost accounting systems to provide four separate, function-specific invoices to each Customer, each month. These systems do not meet the needs of VITA and its Customers for a single IT financial management platform providing complete financial transparency through consolidated IT financial information and invoicing. Our financial management solution will make it easier to consume and substantiate (i.e., greater transparency supported by objective data) financial information, and structure it in a manner that allows correlation to Customer budgets, forecasts, and retrospective analysis to feed critical business decisions and activities. Our solution has clearly defined roles and responsibilities as outlined in **Figure 3.3-1**, along with the processes and tools to support the Commonwealth. During transition from the current IT financial management environment to SAIC's proposed solution, SAIC will follow the process for the existing IT financial management environment as a vendor until the new SAIC solution commences.

	Commonwealth			Managed Services Integrator							
	Finance	VITA	Agencies	Financial Management	Planning & Analysis	Vendor Management	IT PMO	IT Operations	IT Asset Management	Invoice Management	Tool Enabled
1. Financial budgeting (Capex and Opex) activities	A	I	C	A	R		C	C	C	C	✓
2. Financial reporting and variance analysis	A	I	I	A	R				C	C	✓
3. Forecast and track resource utilization		I		A	R		C	C			✓
4. Manage service cost allocation/charge-back process			I	A	R						✓
5. Manage charge-back dispute process	I	I	C	A/R					C		✓
6. Process invoices	I	I		A/R	C					R	✓
7. Review and audit all telecom invoices	I			A	C	I		I		R	✓
8. File and track invoice claims, disputes, fee reductions, and earn-backs	I			A	C	I				R	✓
9. IT consumption and demand reporting	I	C	I	A/R			C	C	C		✓

A - Accountable   R - Responsible   C - Consult   I - Inform

18-B-AUIA-11JDZF-EN-06

Figure 3.3-1. A Solution With Defined Roles and Responsibilities

SAIC is proposing an IT financial management solution that fully integrates cost data received from multiple suppliers and disparate measurement units, and presents a consolidated view of these charges in a highly interactive format allowing comparison of specific charges from month to month, to budgets and forecasts across IT service categories. The solution will also integrate Service Level Management reporting capabilities to assess any credits in the event of a Service Level Default and track Earnback for all ITISP suppliers.

In our proposed solution (**Figure 3.3-2**), individual Customer requests for services are tracked within the Keystone Edge SMS component along with the consumption of resource units. This information provides objective proof of the resources a Customer has requested, and directly correlates with the charges for the services that Customer receives. This platform provides automated, auditable workflow for request approval(s) and comprehensive integration with automated provisioning of vendor- and cloud-based resources in response to approved requests.

SAIC's solution, based on Digital Fuel, leverages VITA, Customer, and supplier input to maintain a cost allocation model that maps IT consumption information from SMS requests to supplier invoices to produce interactive IT financial analytics easily navigable by individual Customers and departments. The resulting drill down data will provide VITA with all of the supporting details necessary to facilitate payment to the ITISP suppliers.
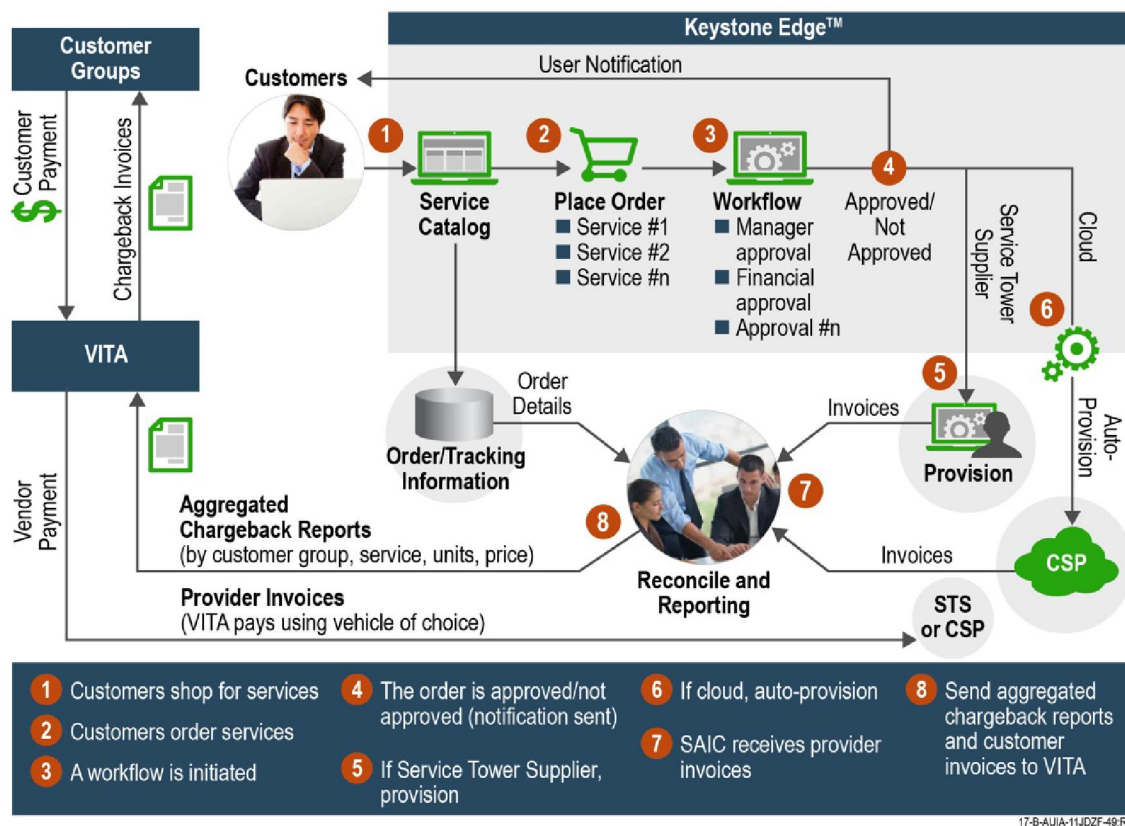
Figure 3.3-2. SAIC's Financial Management Process Provides Comprehensive Integration With Automated Provisioning of Vendor and Cloud-Based Resources

Aggregated Chargeback reports are provided to VITA, while individual Customer invoices are presented directly to each Customer via the Service Management System. Invoices are available directly on-line, and may also be delivered electronically or via hard copy if requested.

For every invoice created per Customer, per month, a unique identifier is assigned and payments are tracked against it. A receivables report is managed by the IT Financial Management (ITFM) team and is kept current as they track invoices, payments and fee disputes by the various agencies. This report is reconciled by the ITFM team with VITA to verify invoices outstanding and payments received. Reconciliation will be automated through integration between Keystone Edge and VITA's designated financial management system. This information is made available in reports and views to the various stakeholders in the ITFM tool.

We will migrate VITA from its current, multi-system chargeback approach to a single, fully integrated model during implementation via a three stage process:

1. *Current State Assessment.* SAIC will begin with a detailed assessment of the Commonwealth's current processes and supporting systems utilized for IT cost and chargeback accounting. This assessment will fully document the existing environment and identify the required changes necessary to achieve the future state desired by VITA and its Customers. The assessment will result in a documented gap analysis (current vs. future state) with prioritized recommendations for implementation in the next phase.

2. *Process/Catalog Design.* SAIC will design new or modify current processes to support the future state objectives, define any changes required to the Service Catalog/CMDB structure necessary to

accommodate financial attributes, and develop the financial cost models that will satisfy the allocation methods desired for each cost category. This design will accommodate the hierarchy of views and levels necessary for precision cost analysis, budgetary correlation, and forecast planning.

3. *Implementation.* The SAIC Team will review the output of Phase 2 with VITA, and with its approval, implement the new processes and models within the production environment. We recommend running the new system in parallel with existing processes/systems to validate its performance and accuracy.

The resulting processes and system will provide VITA and its Customers with consolidated chargeback invoicing encompassing all required information necessary to verify charges and highly-interactive, reporting and analysis views, including drilldown capabilities. Customer financial personnel are able to view and "drill-down" through charges and compare expenses to budget and forecasts through a highly interactive, web-based interface.

Our solution provides the following features:

◆ Automated import of electronic vendor billing data from invoices and/or from the existing VITA general ledger system. In the event an alternative to electronic billing is necessary, our system is capable to support from such means as paper invoicing, .pdf, and hand delivery where required. We will also assist in any migration necessary to achieve the benefits that are associated with electronic invoicing. For pricing purposes, all invoice data required to be included in the IT Financial Management System (ITFMS) will be provided to SAIC in an appropriate electronic format.

◆ Discrete correlation of Customer request data within the SMS to the suppliers' invoices to ensure that Customers are only billed for services and resources for which an auditable request has been approved

◆ Fully interactive views and analytics for authorized Users of the invoice and financial data via the web-based IT Finance portal that supports comparative analysis of budgets, previous trends, and forecasts on an item-by-item basis

◆ Drill-down capabilities to view costs for overall services, individual systems and components, and direct correlation to specific IT assets and configuration items

◆ Comprehensive documentation and justification for all IT charges, with the ability to perform "what-if" analysis relative to previous and future IT resource consumption

◆ Integration with SAIC Cloud Brokerage automation for the tracking of Customer-requested, cloud-based resources from Third Party Vendors

The dispute resolution process consists of three sub-processes: (1) identification, (2) resolution, and (3) closure. During the identification sub-process, potential disputes are identified with the focus during this phase being to proactively identify potential issues in order to prevent actual disputes. If a dispute is identified, it will be captured and coded (e.g., category, reason code, and other required data elements). The dispute will then be validated through additional research as needed. Cause and resolution will be determined with STS, VITA, and Customers. If a corrective action is required, it will be executed and managed. After approvals are obtained (defined through the governance process), a dispute is moved to closed status with either credits issued or Customer collection initiated as needed.

3.4   Service Portfolio Management

SAIC has designed our service portfolio management solution to accommodate change over time because of nontechnical factors such as changes in new legislation affecting a Customer, changes in Customer demographics (e.g., increased average population age that creates greater demands on specific applications in the future) and because of technical factors (e.g., new technologies, technology obsolescence, and opportunities for continual service improvement). Our Service Portfolio Management approach considers and reviews all phases of the service life-cycle utilizing the Service Pipeline (a database that encompasses the Commonwealth's strategic outlook for new and improved services), the Service

Catalog of existing services, and the Catalog of Retired Services. As shown in **Figure 3.4-1**, the key inputs to the Service Portfolio Management process are the service strategy, technology plan, and Service Catalog. By combining these inputs with the involvement of key personnel from the suppliers as well as the MSI Business Relationship Management, Technology Management, and Service Strategy processes, SAIC will produce the quarterly Service Portfolio Analysis report, which analyzes the service portfolio and identifies potential opportunities for improvement. The Service Portfolio Analysis report provides VITA with the information necessary to make a service approval decision (i.e., gate decision). Every new or modified service needs Commonwealth approval, along with its associated level of investment, prior to its development, transition, and operation, to ensure that it will be able to successfully deliver its expected level of service. The first approval gate in **Figure 3.4-1** charters the development of the service, and its ultimate inclusion in the Service Catalog.
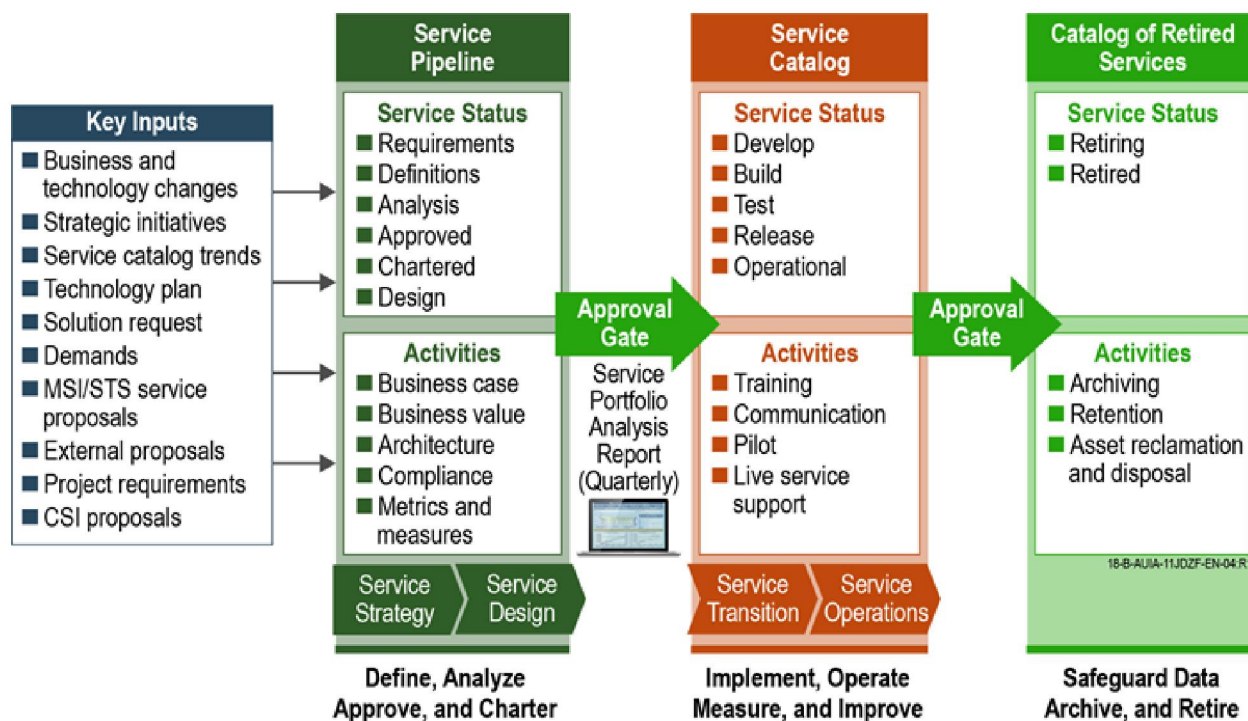
Figure 3.4-1. SAIC's Service Portfolio Management Process

Our quarterly Service Portfolio Analysis reports also support the approval to retire services. Services may be retired when they no longer meet the Commonwealth's business objectives and the level of investment required to maintain them outweighs their estimated return. The service retirement approval gate will require input from all Commonwealth Customers that are currently using the service to ensure that the service can be retired without impacting business needs. Once the retirement gate decision is made, SAIC will coordinate, with the associated suppliers, the archiving and retention of service capabilities and data, and the reclamation and disposal of any associated assets.

The Service Catalog and Project Portfolio Management modules of the Keystone Edge SMS component are the foundation for SAIC's Service Portfolio Management process. The Service Catalog module stores VITA-required key service attributes in a central repository and provides the required browser and mobile device accessibility for key VITA and Customer personnel to review or request services. As part of its approach of linking IT services with business outcomes, SAIC uses the Service Catalog module to document the business value and impact of each service. As described in Sections 2.2 and 2.3, SAIC coordinates and manages the work of the suppliers on Projects to implement new or changed services through the Project Portfolio Management module of Keystone Edge.

SAIC optimizes the business value of VITA's service portfolio by performing a gap analysis between the existing service catalog and the service strategy, Technology Plan, and service portfolio. Collaboration between our government business process and technology experts and VITA will identify service gaps and improve capabilities, identify changing business requirements, estimate the business impact and implementation priority of the new or modified services, and proactively propose portfolio change opportunities to VITA.

3.5   Demand Management

In SAIC's solution, demands for new or upgraded services or technologies to support the Commonwealth and its citizens are delivered in Keystone Edge. The challenge for VITA and the MSI is to review, consolidate, categorize, and analyze this information so that VITA can make informed, timely, and strategic investment decisions based on actual and estimated future demand for service. SAIC will analyze the demand for service using standard templates and approaches, assess the potential value to the Commonwealth and draft the business case. We will manage the prioritization and selection of specific demand requests, involving appropriate stakeholders in the decision-making process as defined in the SMM.

SAIC's Project Demand Management solution is grounded in the analysis of data that we receive from sources such as service portfolio usage, service strategy outputs, request for solutions by Agencies through the Service Desk, the VITA CAMs and our Business Relationship Managers. The results are then entered into the Keystone Edge system for tracking and transparency of the demand request. As the single system of record, our SMS enables easy management of service demands from VITA customers. We also balance available resources against those demands to ensure the most efficient utilization of available resources from the STS. Our technical staff will review trends, provide recommendations for increased capacity (or reduced capacity) where needed, and submit them for VITA's approval when necessary.

SAIC will follow a standard process for performing Demand Management as outlined in **Figure 3.5-1**. This flexible Demand Management process allows for exceptions or escalations when required to support critical needs. Our standard process starts when a User submits an idea to the online Demand Workbench in Keystone Edge. The Demand Workbench is a Keystone Edge form that guides the User through all necessary data fields and required documentation to submit a request for review. The form can also be completed by a requestor through the Service Desk, with an agent walking the requestor through the form for entry. We will review the request and determine what additional data are needed and how they will be obtained. Demand requests may also be generated based on analysis determining increased Service Requests, BRM's face-to-face interactions, and service strategy analysis. When a desired service is not available, an SAIC Demand Manager contacts the User to discuss the services or bundling of services required. Our process is designed to solicit and accept ideas for new and differentiated service offerings from Customers, STSs, Third Party Vendors, and the MSI technology planning and innovation functions will provide a steady stream of potential source demands.
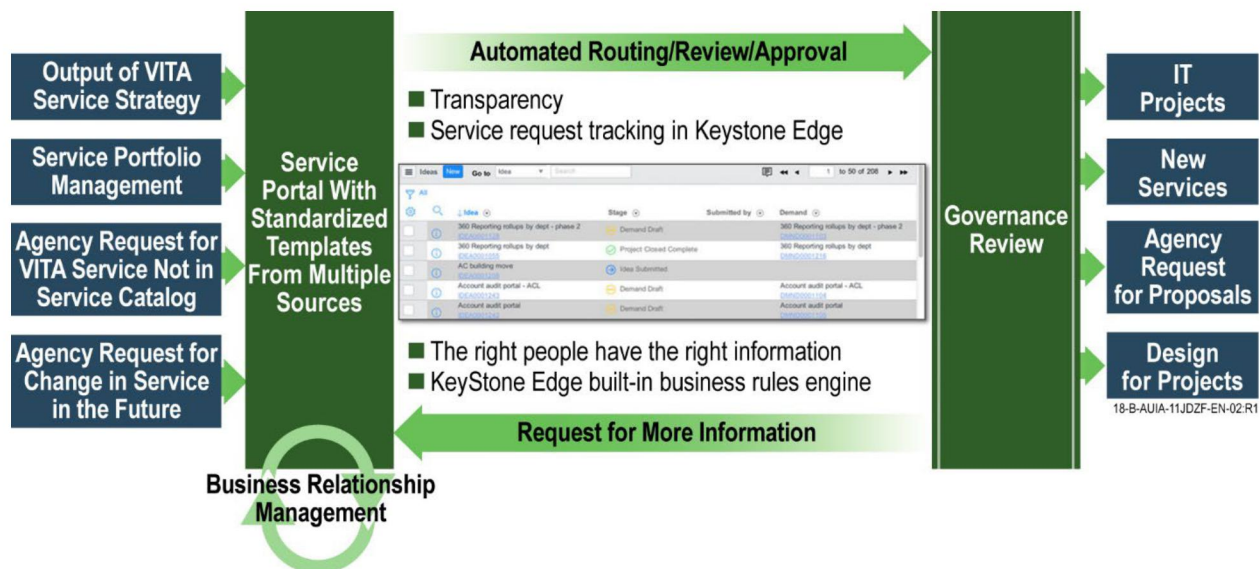
Figure 3.5-1. SAIC's Demand Management Process

Our Demand Manager will screen the demand requests against patterns of business activity. From experience performing Demand Management with other customers; if within one fiscal year, there are at a minimum three similar demand requests, a pattern of business activity is determined to exist, and the Demand Manager will submit the demand request for inclusion in standard service delivery. Beyond the analysis of current demand request SAIC will constantly be analyzing for future demand for service. All requests will be analyzed and in the case where a Customer demand request is determined to be an early User of a service, but this service will have growing demand in out years, a demand request will be recommended for the Service Portfolio. Demand requests are routed by the SMS to the appropriate ITISP Governance personnel.

Our Demand Manager will collaborate with the demand requestors and serve as their advocate to VITA. The SAIC approach to Demand Management is based on data analysis and SAIC's solution provides the visibility into demand analysis to provide a voice to actual demand needs by Customers to turn demand into Projects and services. The approval process will follow the ITISP Governance process as defined in the SMM. The demand requestor will be able to review the demand request at any time during the process. The qualification and analysis steps within Demand Management also ensure that valuable differentiated service offerings for Customers are promoted for evaluation and, when approved by VITA, included in the SMS Service Catalog.

The SAIC Demand Manager will manage the process flow of all demand requests, with performance measured as follows:

◆ Completeness of demand request at point of entry for VITA review
◆ Cycle time of demand request from Qualified status (point where a pattern of business activity is determined and demand request status is changed to Qualified) in the SMS to the date of governance review

By working with VITA and its stakeholders, SAIC will establish the key data elements and measures that will help frame the analysis necessary for managing customer demand across the tower provider resources. This approach will include formal short-term and long-term demand planning meetings with VITA and its stakeholders and with the Service Tower Suppliers. Our team will propose, and gain consensus in these meetings on, the appropriate measures for assessing the resources and their capacity, demand levels, and patterns of business activity to determine trends so that we accomplish proper demand

prioritization. For example, we might find a small number of Customers using an outdated application or resource that is costing VITA more to support than the cost of migrating the Users to a more modern application or resource that still has sufficient capacity, meets the base needs of the target Customers, and provides improvements to both the Customer and VITA.

Our Demand Management process is open to all VITA stakeholders to solicit and accept ideas for new and differentiated service offerings from Customers, STSs, and Third Party Vendors and to integrate them with our technology planning and innovation functions to provide a steady stream of potential source demands. The Demand Management process qualification and analysis steps promote differentiated service offerings of value to Commonwealth Customers for evaluation and, when approved by VITA, for inclusion in the service catalog.

SAIC's Keystone Edge SMS centralizes strategic business and IT requests. It allows the Demand Managers to streamline the investment decision process for new products, services, repairs, and enhancements. Customizable dashboards give VITA stakeholders visibility into Project health, cost, and portfolio performance, along with the capability to centralize, collect, and prioritize all demand. It also gives them the capability to assess, manage, and accurately forecast demand for products and services.

3.6 Business Relationship Management

Our approach to Business Relationship Management provides direct support to VITA's CAMs, with a focus on establishing and maintaining a collaborative relationship of trust among Commonwealth Customers, VITA, the MSI, and STSs. Establishing and maintaining trust in these relationships require open honest communication, reliability and consistency in our interactions, and continual demonstrations of the integrity of our team. Therefore, we have focused our approach on supporting VITA's CAMs as follows:

◆ Providing them with accurate and reliable information about the status of Customer IT services, systems, or requests from our "single-source-of-truth" SMS, thereby doing more than just supporting communication but enhancing communication activities of VITA and its Customers.

◆ Proactively providing direct insight into the status and next steps of all ITISP processes (i.e., keeping everyone on the same page) to enhance the reliability and consistency of interactions with all stakeholders

◆ Cultivating within our team the skills and behaviors that exhibit integrity to maintain excellent working relationships with the Customers so that efficient and effective services are offered by VITA's program

Our approach focuses on the following actions:

◆ Provide a business relationship team skilled in using and obtaining information from our SMS

◆ Require that all business relationship team members are trained in MSI processes, methods, and approaches, as described in the SMM

◆ Provide an SAIC Business Relationship Manager who continually reinforces the concepts of integrity, open honest communication, and reliability with the team

◆ Develop and distribute a biannual survey to Customer stakeholders to measure their satisfaction with the VITA relationship and services and to analyze and incorporate the results into the Business Relationship Management service area

Our Business Relationship Management team will assist and support CAMs by off-loading much of the operational requirements to allow for CAMs to work with the Customers on strategic direction, budget, business case reviews, and so on. BRMs will be assigned to Customers to support the development of relationships and consistency critical for the success of this role. Day to day operational requirements are greatly reduced due to the ease, speed, and completeness of the proposed Service Management system. To ease the adoption of this better way of doing business SAIC is overstaffing the BRM position to provide Customer training, evangelism and high levels of Customer support. We will provide assistance in navigating the processes and organizational groups of the full services delivery approach during this

migration to a more strategic organization. To support the migration to a more strategic support organization to the Customers, our Keystone Edge SMS provides direct visibility for Customer Users into operational items. This visibility and direct access means the CAMs and BRMs will have time to focus on fostering a strategic view and strategic direction for the Customers. We will track Customer requests to ensure that they are processed efficiently and that Customer ideas and suggestions for new services or improvements are expedited through the Demand Management process of qualification and review so that Customers directly benefit from enhancements to the offered services.

Complaint Management

Any Customer User may register concerns or complaints with a simple entry in the SMS Service Portal, through the Service Desk, or via communication to the SAIC Business Relationship Management representative. In all cases, complaints are recorded in Keystone Edge for review and action by SAIC's BRM team and VITA and are subject to automated escalation workflow based on nature and severity. Complaint response will also include a follow up call to the User from the BRM assigned to the User's Customer organization. The BRM will confirm the details of the complaint, ask for any clarifications or required additional information, and provide the User with information on the steps and actions to be taken as a result of the complaint. A complaint that requires a change in process, procedure, or policy for remediation will automatically trigger a demand record in the SAIC Demand Management system for further qualification and prioritization. For all complaints that are classified as major (or severe), an Incident will be generated and integrated into the QA process so that any corrective action or remediation is tracked to successful conclusion. We will process complaints related to individuals within the Service Tower Supplier in accordance with prevailing VITA and STS human resources policy and guidelines. A summary of complaints, follow up actions, and associated improvements will be presented monthly as part of the overall Service Management function as part of Operational Governance.

Day-to-Day Feedback

SAIC's proposed solution for Service Desk services provides for continual recording of feedback on MSI and supplier performance within Keystone Edge. Our platform and procedures provide automated after-call satisfaction surveys via email and portal link that routinely capture Customer satisfaction levels associated with the resolution of Incidents and Service Requests. Periodic Customer satisfaction reports will be provided to VITA. These surveys are sent to a percentage of random Customers that log Requests or Incidents with the Service Desk. That percentage will be agreed during Implementation with VITA and Customer participants. A typical sampling includes 15-20% of tickets logged. Additionally, individuals or Customers can opt-out of survey participation if they so desire and therefore not be included in the random sampling.

4.0 SERVICE DESIGN

4.1 Solution Design Management

SAIC will provide architecture and design support for the development and implementation of solutions by the STSs and will verify that proposed solution designs are consistent with VITA architectures and technology standards. SAIC's Solution Design Management process is the central technical oversight and integration function, as shown in **Figure 4.1-1**.

The solution design management function is led by the SAIC Chief Technology Architect. The SAIC technology team provides technical expertise across each technology discipline supported by the MSI and suppliers to review supplier technology recommendations. The SAIC technology team combines dedicated MSI technology staff members (who assess technologies being deployed in existing services) with reach-back to SAIC Team staff members (who are added for their expertise in new technologies).

Built through our decades of experience as a system integrator, SAIC's proven United Solutions Process Asset Library (PAL) equips us to drive the capture and validation of business and technical requirements as well as review the technical, schedule, cost, and risk aspects of proposed solutions. The processes included in our United Solutions PAL are deeply rooted in the ITIL lifecycle framework. Based on this framework, our proven processes provide the structure to safeguard that a proper Service Design Package is produced during the design phase, including the Five Aspects of Service Design. These five aspects ensure business requirements are properly captured in the Service Solution Design, the tools and Service Management systems needed to operate the service are captured, the technical design is complete, the measures and metrics for monitoring the service are defined, and the processes to manage the initiative are documented. This approach supports the proper integration of the "4 Ps," namely the assimilation of the People, Processes, Products, and Partners. Our SMS enables the necessary tight integration, via workflow automation, between the MSI and supplier technology teams for the routing and coordination of solution design activities and the facilitation of design approval by VITA and its customers. Our CENTER tool retains earlier designs and document version control for reference and potential reuse.
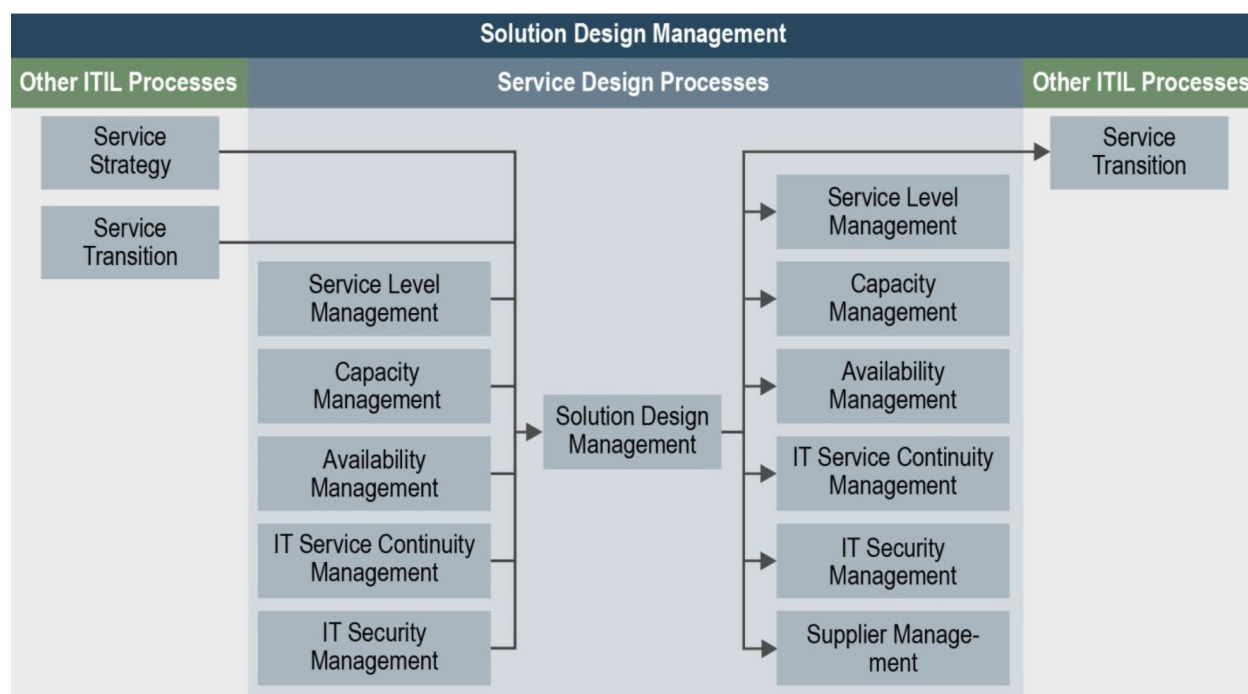
Figure 4.1-1. Solution Design Management Process

4.2   Service Catalog Management

The management of service catalog content is performed in SAIC's ASD organization, under the leadership of our Chief Technology Architect. For this process area, the ASD team is responsible for ensuring that each item in the Service Catalog is accurately defined and documented by the source organization (i.e., the Service Tower Supplier or Third Party Vendors offering the service), that its description is clear in the catalog, and that its entry remains current at all times until the item is removed.

Our ASD team uses an efficient and mature Service Catalog Management process to accept requests for new Service Catalog items. Our processes are designed to ensure the Service Catalogue is complete and properly describes the service, the processes used to enable the service, and the level of service the Customers can expect. The process starts with a Demand Management request from VITA or one of its Customers to provide such a service, followed by qualification and evaluation of the request and, with VITA approval, internal solicitation of Service Tower Supplier responses to the demand request.

Customers may also submit full or partial designs based on their own internal work as a foundation for a new Service Request. Our ASD team will develop the internal solicitations, using their knowledge of the IT strategy, proposed innovations, current and future architectures, and IT plans so that any service modification maintains alignment with VITA's technical direction. Tower provider responses to the solicitation for a new service item or for changes to an existing catalog item are electronically submitted in Keystone Edge, with required attributes defined for this process and documented in the SMM. These attributes include a description of the service, supported products, how the service is obtained, any terms or conditions for the service, and pricing of the service. **Figure 4.2-1** depicts key inputs, processes, and outputs of Service Design to manage and deliver effective Service Catalog services.
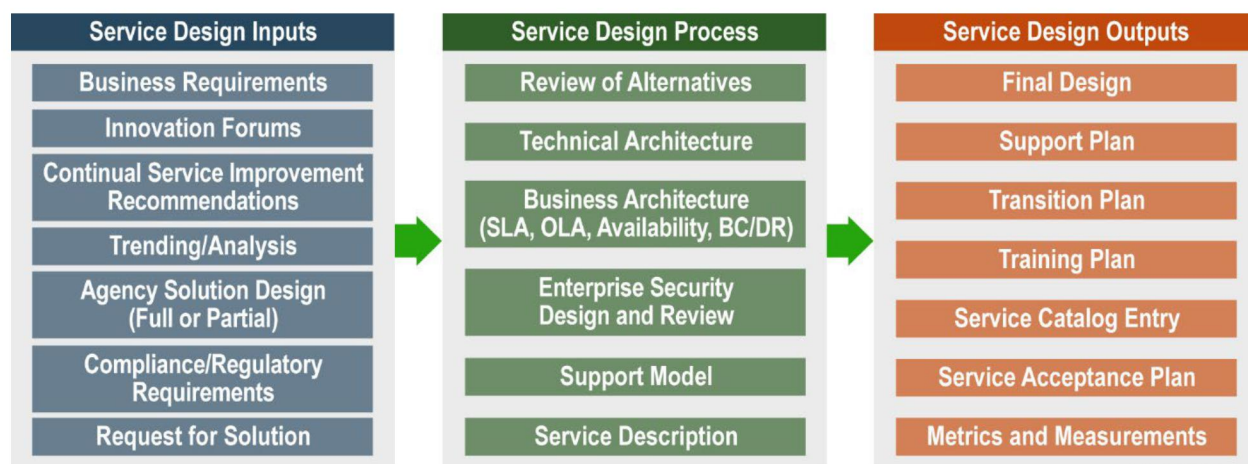
Figure 4.2-1. Service Design Provides Effective Management of Service Catalog Offerings

Our ASD team evaluates these submissions for completeness and compliance with the submission process and provides VITA with a recommendation for acceptance or rejection of the submission. VITA is thus provided with fully qualified information on which to base its decision to accept the new or changed service in the Service Catalog, reject it, or require further design and definitional work by the offering Service Tower Supplier. When requests are approved, SAIC's ASD team will initiate a request for change and will implement the change in accordance with the SMM.

SAIC's solution provides the Service Catalog as part of our Keystone Edge platform and as a core service that is fully integrated with its CMDB and IT Financial Management processing suite so that consumption (approved Service Requests) of each Service Catalog item is tracked across its life cycle. This approach provides auditable data on which requests are approved, by whom, and for how long. It also fully tracks and forecasts the overall capacity for the Service Catalog delivery item.

4.3 Service Level Management

Our Service Level management (SLM) approach establishes a meaningful view of the health of service delivery across all Service Tower Suppliers by collecting and integrating performance data from within the IT environment or from the STSs and making such data available for reports or dashboards. Our SLM process will be integrated in the full life cycle of all IT services for all Service Towers Suppliers. The Keystone Edge Service Management module is used to track all SLAs and service level requirements (SLRs) for all service towers in a centralized database. This module provides the mechanism to define the performance attributes of each SLA and SLR, track them for impending and actual compliance, and provide automatic and timely notification of potential SLA and SLR issues to prevent actual SLA failures for service towers and the MSI contractors. The module also integrates with other IT management processes (such as Event Management, Incident Management, and Problem Management) so that interaction with those processes can be automated.

In addition to the enterprise view of SLA performance available via report, dashboard, and on-demand access, the Portal also provides the availability of custom views of service performance by any logical grouping. For example, SLAs can be viewed for the enterprise, by individual Customer, by location; by Service Tower Supplier, by Application, or Business Service; or by any subset based on the fine-grained tracking data collected with Keystone Edge. This provides Customers, VITA, and SAIC the means to drill down into service performance on a granular basis, identity trends and opportunities for improvement, and to report meaningful metrics to User communities that are in alignment with their own personal experiences.

SAIC will post all monthly and historic Service Level reports in CENTER for easy and immediate access by authorized VITA staff members or Customers. This web portal will provide a repository for ongoing and historic records. SAIC will provide a live web portal dashboard through Keystone Edge to note all required Service Levels in near real time. The data for these postings are pulled and compiled from current Incident and change management records in Keystone Edge. Availability data will be pulled from Service Tower Suppliers and aggregated into a single view in a web portal to provide clear accountability. Keystone Edge offers the mechanism to interface with STS SMS, either directly or through easy-to-implement Simple Object Access Protocol (SOAP) web services. If the requisite data exist for calculating SLA performance in Keystone Edge, reports will be generated directly. If not, the web portal will provide direct access to those systems and to access real-time reports.

A sample Keystone report is shown in **Figure 4.3-1**, which depicts a visual view by business services for health, SLAs, Incidents, and changes in a customer environment. For the County of Orange, CA, using Keystone Edge, we manage and track 95 individual SLRs and present them in a real-time dashboard.
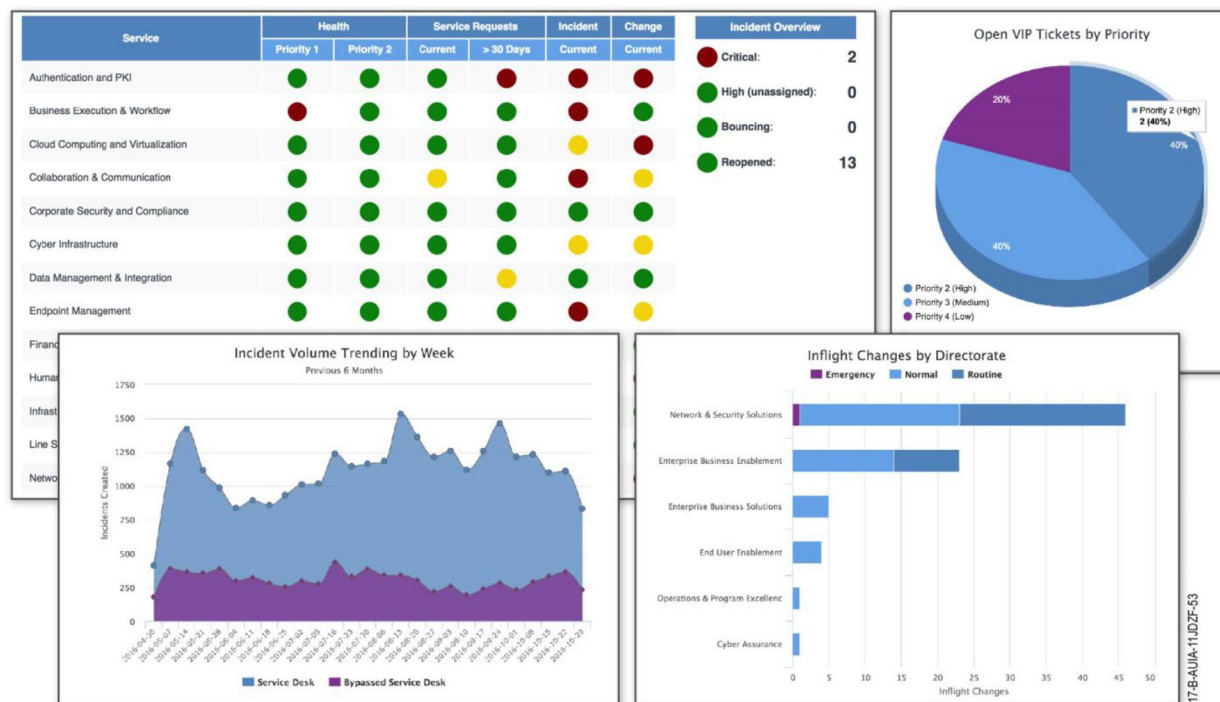

Figure 4.3-1. Sample Real-Time Dashboard SLA Report

4.4 Availability Management

Because Availability is a key measure of a service's business value, SAIC implements Availability Management approaches that have the following characteristics:

◆ Meet or exceed the current and future agreed-on needs of the business

◆ Meet or exceed agreed-on Service Levels
◆ Are cost-effective

SAIC's approach to Availability Management goes beyond just measuring the availability of individual technical components. Working with VITA and its Customers through the Business Relationship Management function, we will review and update the documentation, identifying the essential business functions and IT services. We then will document in the Keystone Edge Unified Data Store (i.e., CMDB) the relationship between the IT assets and the services for essential business functions. These data can then be made available for further analysis. This approach provides VITA with the following benefits:

◆ The business impacts of any supplier service outage can be immediately identified and communicated to VITA stakeholders
◆ The Incident response activities for service restoration can be prioritized if there are multiple simultaneous outages
◆ Proactive Availability Management can be performed to reduce future services outages

As described in Sections 6.2 and 6.4, SAIC's Incident Resolution and Problem Management processes are enabled by Keystone Edge to manage multi-supplier resolutions to Availability service issues.

In addition to working proactively with the suppliers to address known problems, SAIC's Availability Management process includes continual analysis of both the technical architecture for IT services and the supplier availability performance to identify improvement issues such as:

◆ Improvement requirements (based on not meeting service levels)
◆ Improvement opportunities

Through this analysis, we will identify potential high-impact Problems and then request and implement service changes to improve performance and better ensure that the Availability requirements are met before an operational problem occurs. We identify these improvement opportunities by conducting a trend analysis of the historical capacity and Availability data and linking those data with information on the criticality of the business processes supported by those components. The Keystone Edge Performance Analytics module provides the capability for historical trend analysis and is integrated with the CMDB module to allow prioritization of the recommendations for addressing potential Problems.

Once an important potential Problem is identified, SAIC will lead and coordinate the STSs in identifying and recommending improvement opportunities. As described in Section 4.1, the SAIC technology team will work with the STSs to validate whether the improvement should be made, using current or new technology. Using our collected information on the design of the services and the relationship of each component to the customer business processes, we also will present improvement opportunities that eliminate potential single points of failure in the delivery of important services.

4.4.1 Availability Management System

SAIC's Keystone Edge platform provides a responsive and effective Availability Management System through several mechanisms. Within Keystone Edge, physical CIs (i.e., devices) are subject to Availability Management, and Keystone Edge is configured to receive fault events via standard web services from the monitoring platforms of the responsible Service Tower Supplier. For example, monitoring tools established by the server and storage tower supplier for its servers will be required by OLA (and documented in the SMM) to post events to Keystone Edge when a server fails or ceases to become Available for any reason. These events are recorded in our platform as component outages and automatically generate Incident records for resolution by the responsible Service Tower Supplier.

For systems, services, and applications, our platform's CMDB is configured to relate the underlying physical components (CIs) via business service mapping so that fault events for an individual component register as an outage or service degradation of the larger compound system. The event correlation

components in Keystone Edge capture Availability events with both individual and compound CIs. Keystone Edge generates and relates Incident records for resolution, and it stores records for each period of unavailability (by component and system/service) for ongoing reporting.

In addition, Keystone Edge implements SLA monitoring for all individual or compound CIs for which an OLA or SLA defines a service level requirement. Availability events for these items trigger business rules in the platform for automatic tracking of SLA compliance. Keystone Edge includes automated notification and escalation workflow to highlight availability events that may lead to an SLA breach (or for which a breach is imminent), and if a breach occurs, Keystone Edge records this breach information. This function of the system informs Customers and Service Tower Suppliers about the potential for breach before it occurs and allows all integrated suppliers to proactively work toward resolution of underlying issues to avoid SLA breaches.

All Availability, Incident, and related Problem records (such as those requiring Root Cause Analysis) are retained in the system for both real-time dashboards and retrospective advanced reporting through the platform's performance analytics capability. The dashboard image in **Figure 4.3-1** provides one example of such real-time reporting. Our platform incorporates automation to meet all of the requirements specified in Exhibit 2.1 of RFP Section 4.1.

4.5   IT Service Continuity Management

SAIC's IT Service Continuity Management solution reduces the impact of disasters by effectively planning for the recovery of IT services. As shown in **Figure 4.5-1**, we support the business continuity plans of VITA's Customers; we document and test the Business Continuity (BC) and Disaster Recovery (DR) Plans (DRPs) for the services provided by SAIC; and we oversee the documentation and testing of supplier BC plans and DRPs.

SAIC's solution for IT service continuity management is built on our real-world experience that BC and DR planning must consider events whose occurrence cannot be forecast. We mitigate these risks by using a detailed and well-rehearsed disaster plan that we can begin executing at a moment's notice.

For example, when SAIC developed BC and DR plans as part of its contract for operating the communications backbone for the Department of Defense (DoD), we did not anticipate the events of 9/11. On that day, we were forced to execute the BC and DR plans for the classified network control center in the Pentagon. Our BC and DR plans were detailed and tested, and our staff was fully trained and aware of its roles and responsibilities for ensuring continuity of this critical DoD service. As a result of our proactive efforts, we executed our plans flawlessly and transferred operational control of the classified network to our alternate location as planned, without Incident, and in a manner completely transparent to globally dispersed DoD customers.
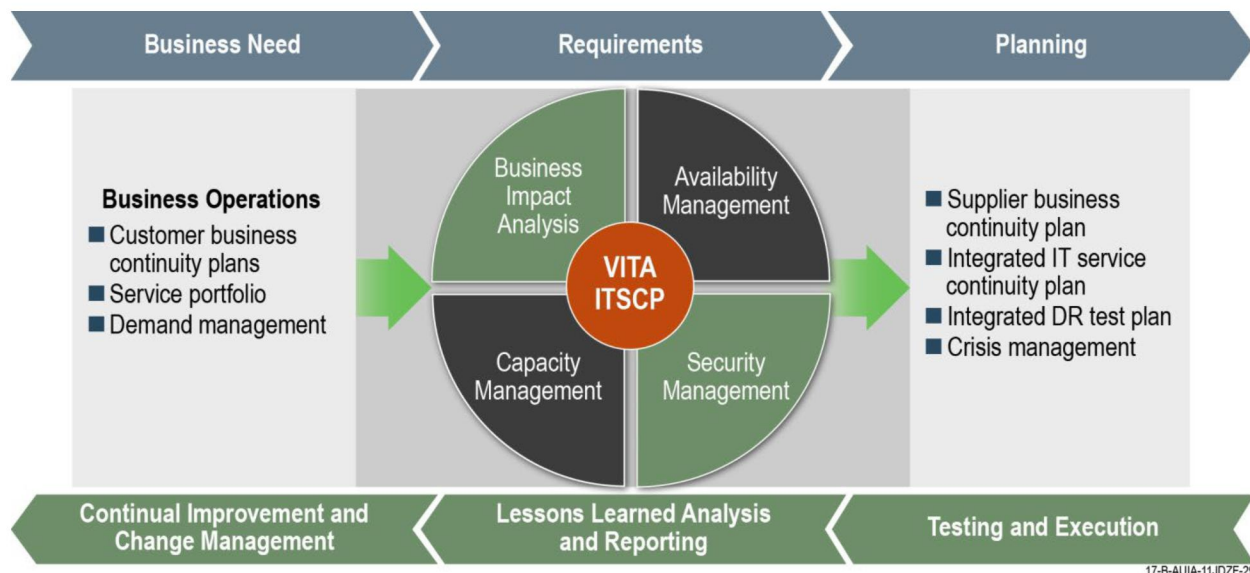
Figure 4.5-1. SAIC's IT Service Continuity Management Solution

The key aspects of our IT Service Continuity Management solution are as follows:

◆ *BC Plans for Customers.* SAIC's BC/DR Lead will serve as a single point of contact with the Customers and VITA on both BC and DR. SAIC will remain integrated with Customer BC planning through our Business Relationship Management function and VITA.

◆ *BC Plans for Supplier Services.* SAIC's BC/DR Lead will oversee all supplier efforts for BC planning and make sure that those plans integrate with the Customer BC plans.

◆ *Development of an Integrated IT Service Continuity Plan (ITSCP).* Led by SAIC's BC/DR Lead, SAIC will direct development of the integrated ITSCP, coordinating the service continuity planning of each supplier. SAIC will review and validate each supplier's documentation of the service continuity plan, processes, procedures, communications, and tools to confirm that it is complete, meets customer requirements, and conforms to industry best practices.

◆ *Validation of IT Service Continuity Solution.* As part of our solution design activities described in Section 4.1, SAIC's BC/DR Lead will work with the SAIC ASD team to oversee implementation of the supplier infrastructure necessary to execute the DR plan. As part of the event management activities described in Section 6.3, SAIC will work with the suppliers to implement effective daily monitoring of critical activities to support the DR solution (e.g., backups, data replication) so that any failures in the services to support DR are identified as Incidents and resolved in a timely manner.

◆ *IT Service Continuity Preparedness.* SAIC's BC/DR Lead will validate that all suppliers have trained their staffs in the relevant BC and DR plans, including crisis communication procedures. SAIC will develop and oversee execution of the multisupplier DR test plan. The SAIC BC/DR team will work with the customers to schedule the tests, then track supplier testing performance to the Recovery Time Objectives (RTOs). We will document the results, raise issues through the Problem Management processes for closure, and perform retesting as required by the SMM.

◆ *IT Service Continuity Actions and Crisis Management.* Because a disaster is truly a Severity 1 Incident, SAIC's BC/DR Lead will provide overall leadership for execution of the BC and DR plans. We will coordinate the actions of the suppliers, manage dependencies between the suppliers, and provide the increased support required by VITA to manage, contain, and resolve the disaster.

SAIC will support BC/DR planning for VITA using the Keystone Edge and CENTER components of our SMS to perform the following activities:

◆ Storing Customer and supplier BC and DR plans

◆ Managing BC and DR planning activities
◆ Documenting the linkage between Customer BC/DR plans and key business processes

4.6 Capacity Management

To support the evolving capacity requirements of VITA and its Customers, SAIC's capacity management solution provides efficiencies to VITA by integrating capacity management throughout the service and technology life cycle. We integrate Capacity Management into key MSI processes and operations and with service tower capacity management activities. The SAIC Capacity Manager coordinates with Customers through our Business Relationship Management staff with our Chief Technology Architect and the STSs to develop a capacity baseline and an integrated capacity forecast based on key business drivers, current Projects, and utilization trends. Our Capacity Manager will review customer requests from the service desk and VITA (including VITA CAMs), align requests to services, identify gaps, and collaborate with VITA as the requests are submitted. SAIC will coordinate with STSs to test the performance of new applications, services, and systems to meet planned performance and utilization expectations and requirements.

Integrated Capacity Plan
◆ Goals, objectives, scope, methods
◆ Current levels of resource utilization at the application, web, data, network, and infrastructure levels
◆ Current levels of Availability (average and peak)
◆ Current levels of Service Tower Supplier service performance
◆ Forecast future requirements
◆ Assumptions and recommendations

The Capacity Manager will also incorporate work schedules and dependencies between STSs into capacity management planning processes. The SAIC Capacity Manager will help specify and understand service and service component requirements, determine system measurement points and thresholds, assist in IT infrastructure design, understand usage patterns, and assist in the validation of capacity and performance requirements.

The SAIC Capacity Manager will create and maintain a Capacity Management plan and reconcile it with the Availability, Performance, and Demand Management Plans and with associated SLA, SLR, and service level targets. The Capacity Management plan will include and integrate with the Service Tower Supplier capacity plans.

Our Capacity Management approach uses iterative activities to analyze, tune, implement, and monitor business capacity, service capacity, and resource capacity. The Capacity Management Information System (CMIS) will provide the capability for Customers to add, modify, or delete their own capacity information (including future business-driven capacity needs) through workflows and User interfaces. We will conduct service and component capacity management for Human Resources, mainframe, server, message and directory services, backup and storage, voice and video, networking, facilities, service continuity, disaster recovery, security infrastructure, and other

SAIC CMIS Data and Information
◆ Customer business needs
◆ Service data, including thresholds, events, and alerts (e.g., transaction response times or batch job execution times)
◆ Utilization data, including thresholds, events, and alerts (e.g., network Availability data, CPU utilization, paging rates, bandwidth utilization)
◆ Technical data (e.g., maximum level of CPU utilization or physical capacity of a particular hard disk)
◆ Financial data (e.g., cost of new hardware or software components)
◆ Service performance information (e.g., completion rate on tickets and work orders)
◆ Workload and trend analysis information
◆ Identification of items and data by Customers and any associated STS or Third Party Vendor
◆ Identification of items and data by application, software, and/or service

evolving needs. The status of these activities will be documented in a set of periodic and on-demand reports that will guide Capacity Management decisions and actions. SAIC will provide a Capacity

Management dashboard that integrates data from capacity reports, monitoring systems, configurations, and service maps in the CMDB. This dashboard will include capacity information (technical capacity, thresholds, forecasts) of newly acquired items, changed items, and any other relevant information. SAIC will review customer capacity requirements, track actual versus planned utilization, and include such information in the monthly reports.

The SAIC CMIS is a Keystone Edge module and serves as a performance analytics module. This performance analytics module provides a repository for current and historical capacity utilization data; using its built-in analytical capability, we will be able to identify current capacity issues as well as potential capacity issues based on trend analysis. The Configuration Management System (CMS) will use Keystone Edge's Asset, Configuration, and Change Management modules to support right-sizing the IT infrastructure to meet defined services levels. The CMIS will serve as an aggregation point and single source of record for all supplier services, STS services, and designated Third Party Vendors' Capacity Management activities. We will update and maintain the CMIS within the designated timeframes in the SMM.

By continually monitoring service demand and capacity, SAIC will be able to maintain a proactive posture for overall capacity and avoid service degradation attributable to capacity issues. The CMS Performance Analytics module is part of our SMS, which provides a comprehensive system of record, tightly coupled with our other ITSM process (e.g., Incident, Problem, and change.) This approach enables coordination of the service changes required to address future capacity issues to be coordinated with the Technology Plan and thereby avoids the need for emergency investments in technology approaching obsolescence.

4.7 Security Management

The sophistication and types of attacks against IT systems and networks as well as the attack vectors are changing daily and present a real threat to the information entrusted to the Commonwealth resources. SAIC will expand on the work that VITA has done to employ a layered defense (defense in depth) to protect COVA information resources by delivering a comprehensive solution that advances protection through integration and automation of security controls. SAIC will work closely with the VITA CISO, Customer Information Security Officers (ISOs), and the Service Tower Supplier providing the Security Operations Center (SOC) functions to tailor our approach to the specific threats and compliance requirements required for the Commonwealth. All aspects of the solution will comply with VITA rules and with state, national, and international regulations, policies, standards, and guidelines, including VITA's Information security standards SEC 501, SEC 525, Internal Revenue Service (IRS) Publication 1075, National Institute of Standards and Technology (NIST) Special Publications (SPs), and ISO 27001.

Our solution is based on SAIC's CyberSecurity Edge™ (CSE) security services and security systems engineering practices. CSE is based on a Discovery-Mitigation-Management approach (**Figure 4.7-1**) that performs an initial security assessment and refines security-specific requirements (i.e., Discovery), tailors the security design to VITA-specific requirements and implements and tests the security solution (i.e., Mitigation), and then continually monitors and validates the effectiveness of the Security Program Plan (SPP) (i.e., Management). We will perform the initial assessment during program implementation to establish the security baseline. SAIC will also use CSE to perform quarterly assessments to verify the effectiveness of the baseline controls and detect changes to the baseline. In the three-month transition period prior to Commencement, SAIC will identify the current policy and baseline; compare against policy, requirements, and best practices; and then develop and recommend plans of actions to achieve recommended future state. The projected timeline is partially dependent on Customer personnel availability.
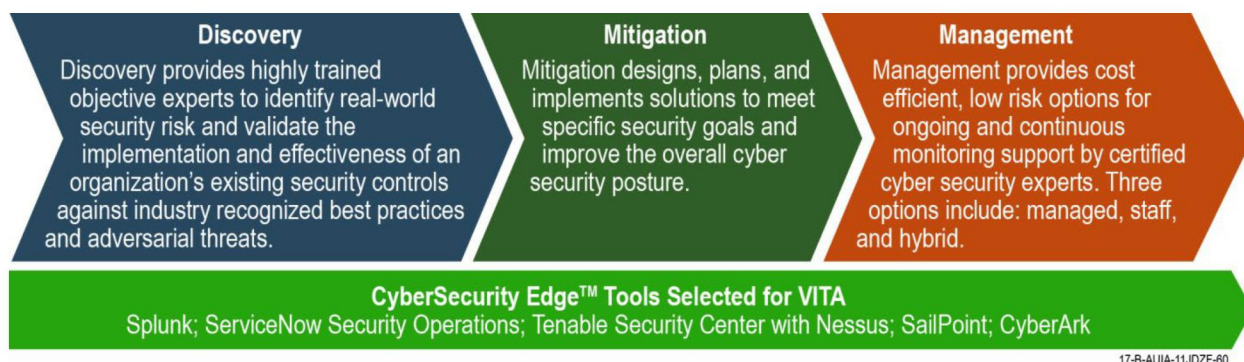
Figure 4.7-1. SAIC's CyberSecurity Edge Solution to Ensure the Confidentiality, Integrity, and Availability of Commonwealth Data and Services

As a part of the initial assessment performed during implementation, our Chief Security Architect and cybersecurity team will conduct discovery interviews with key VITA and STS personnel, review relevant documents, and gather and analyze data, using SAIC security assessment tools. The data gathered and analysis results will enable the SAIC Team to document the Managed Environment's security baseline and to publish a security assessment report, which will include recommendations and an action plan for VITA's approval. This approach will provide VITA and SAIC with a solid understanding of the current security baseline, specify detail requirements to be included in SAIC's final security technology solution, and inform development of the SPP.

SAIC will enable effective security management of the managed environment by using the following five key security-focused tools in the SMS:

◆ Splunk for log consolidation and security data analytics
◆ Keystone Edge Security Operations module to provide visibility into the environment's security posture
◆ Tenable Nessus for vulnerability scanning and management
◆ SailPoint for identity access management
◆ CyberArk to rigorously manage privileged access to the managed environment IT infrastructure and applications

Because the cybersecurity threat is continually evolving and adapting, the security environment of the Commonwealth and its Customers will change over time. These changes may introduce new security requirements. Identification of new and emerging threats, as well as new requirements for compliance based on federal and Commonwealth standards, laws, and regulations will come through a variety of sources. Within SAIC, our Cyber, Cloud and Data Sciences (CCDS) Service Line maintains forums for sharing of information, including best practices, lessons learned, solutions, and emerging news relevant to our customers. This provides our teams supporting the Commonwealth access to a host of resources and information to remain current and to bring the benefit of our organizational experience to VITA and the Customers. We also will collaborate with the VITA CISO office as well as Customers' Information Security Officers (ISOs) to understand their requirements and incorporate them into our enterprise approach. Our Chief Security Architect will participate in the technical and business governance and planning sessions of VITA and its customers to identify security requirements and will offer enabling security solutions to satisfy the emerging business needs. The Chief Security Architect will lead a forum consisting of STS security leads to regularly review ITISP security performance, explore technology options, discuss specific Project status and progress, and share technical information about cyber threats and market studies. Our Chief Security Architect will use information gained through this forum to inform the development of solutions to satisfy security requirements to support VITA and customer evolving IT supported business needs. We will accomplish this by using new security technologies, industry best practices, and features and capacities of the current environment.

On the U.S. DOS Vanguard 2.2.1 contract, SAIC supports the Information Assurance (IA) Directorate and Diplomatic Security to define and facilitate their OpenNet reauthorization process to ensure compliance with DOS security standards. We provide traditional certification and accreditation (C&A) and are implementing continuous monitoring across information resource management (IRM) systems. SAIC developed an enterprise-level dashboard that provides the health status and hourly performance trends of four key IRM services (email, Internet access, network connectivity, and SharePoint) at DOS locations.

Integration with Managed Security Services STS. A high degree of integration between the SAIC Team and the selected STS for Managed Security Services (MSS) will be important to achieve overall effective, efficient and comprehensive security services across the ITISP. Our solution provides a range of strategic and operational security services including Risk Management, Security Incident Management, and comprehensive Identity Access Management functions. We will also provide oversight for vulnerability remediation and provide a single source of vulnerability identification leveraging the asset information supplied by Service Tower Suppliers into our SACM database. These functions are further described in Sections 4.7, 4.8 and 6.6.

SAIC's Security Operations Team will provide overall coordination of the MSS and STS response to security Incidents. This will provide ownership of the overall security Incident, engagement of resources, communications, escalation, and tracking Incidents through completion.

To support a high degree of interoperability between the SAIC Security Teams and the MSS, SAIC will provide the ability for electronic integration from the MSS Security Operations Center (SOC) to SAIC's SMS to allow for immediate escalation of triaged events to security Incidents where required, and to maintain a single source of authority for security Incident information within Keystone Edge. SAIC will also provide a Security Services Catalog to the MSS along with designated Customer and VITA security staff. This Security Services Catalog provides the ability to directly request security specific services and have those requests routed automatically for the most efficient service. Where supported, Security Service Catalog requests may also directly initiate services such as vulnerability scans providing the MSS provider supports that integration. As with all Service Catalog items, workflow for routing and approvals will be utilized for efficient handling of requests.

Security Program. Using information gathered during the initial security assessment, the SAIC Chief Security Architect and Security Analysts will compare the relevant Security Program information against SPPs that SAIC has developed and used on similar security programs (e.g., DoS Vanguard), VITA requirements, and NIST SPs and ISO 27000 standards and guidelines. Our Chief Security Architect and Security Analysts will then develop a draft SPP that will define formal, up-to-date, and documented requirements, standards, objectives, processes, and procedures.

SAIC security engineers will document standard operating procedures (SOPs) that clarify who, what, where, when, and how information security activities are to be implemented across the ITISP. Our implementation activities will clearly define IT security responsibilities and expected behaviors for IT management, asset owners and Users, personnel, and IT security administrators. SAIC will provide the SPP draft to the STS security contacts and the SAIC Chief Information Security Officer before submission to VITA for review, comment, and approval before implementation.

The SAIC Team will employ a comprehensive training solution to identify, train, and track security awareness training. Our training approach is discussed in Section 5.5.1. Our solution combines the capability of SAIC's Enterprise Learning Management (eLM) system to identify and track completion of required training, WOMBAT Security web-based security awareness training for User training, and the SAIC Cyber Institute. This Cyber Institute provides a collaborative training, education, research, and solution development environment to educate and train SAIC employees and partners in general and specialized knowledge and skills in both cybersecurity and cyber operations.

Security Assessments. SAIC's solution to security assessment is based on our knowledge, experience, and successful delivery of cybersecurity and information assurance (IA) services to DoD and the federal government. SAIC will use CSE discovery phase methodology (**Figure 4.7-2**) as the foundation to meet the VITA and Customer requirements for assessing the risk to mission and business from using IT assets. SAIC will implement COVA-centric information security requirements that are similar to and follow the NIST Guide for Conducting Risk Assessments (NIST SP 800.30), which we have used in performing security assessments for our DoS Vanguard work.

Our solution incorporates capability for the RMF overview support, preliminary security control assessment, and security control assessment, using a tailored CSE Discover phase that will assess security control compliance and find vulnerabilities, threats, and risks for each system's network and applications.
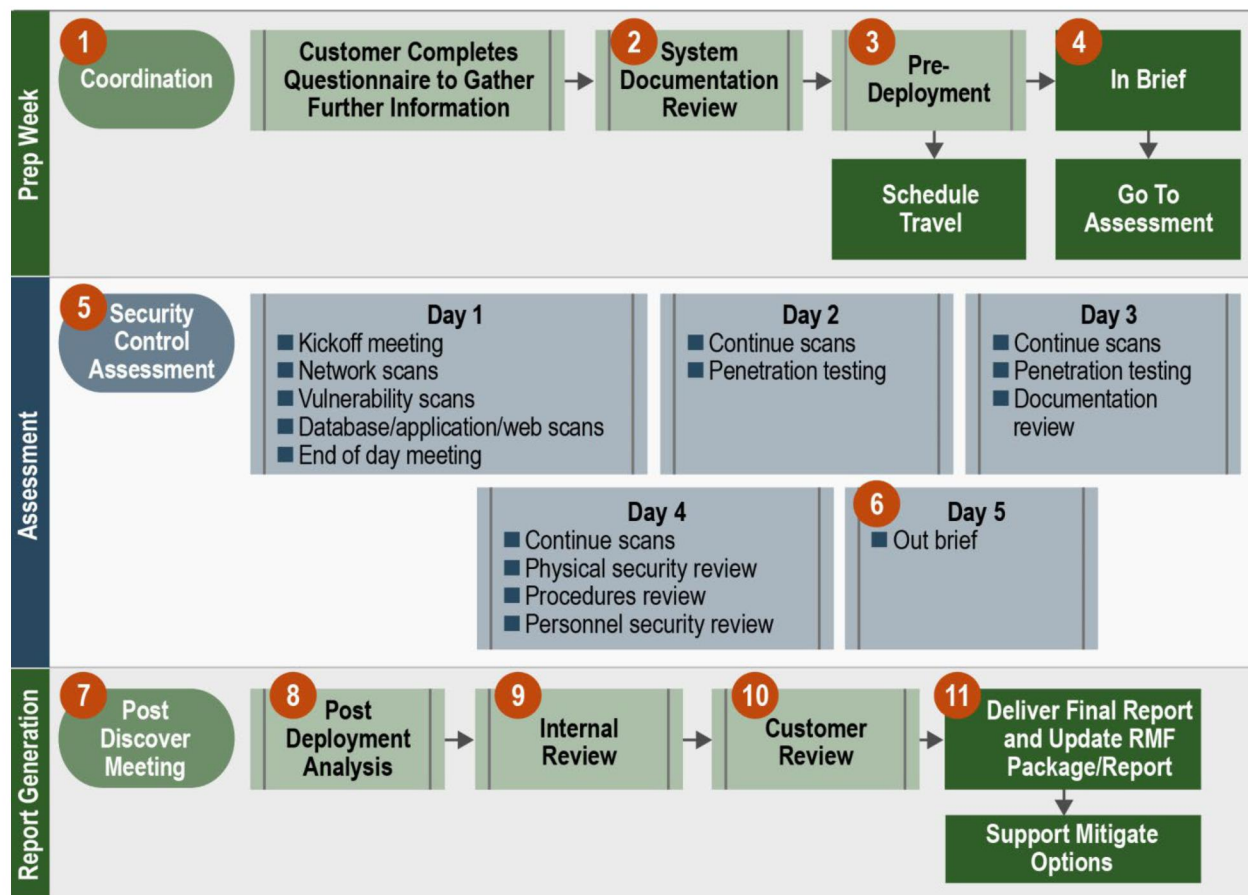
Figure 4.7-2. CSE 11-Step Discovery Phase Methodology to Provide a Structured and Robust Solution for Conducting Security Assessments

Security Assessment by Third Parties. The SAIC Team supports independent verification and validation as part of information system security assurance that complies with the VITA risk mitigation strategy and addresses the information security life cycle. SAIC routinely submits to and encourages third-party independent assessments as a means to further optimize the continual monitoring of security controls. In particular, we require assessor independence that provides a degree of impartiality to the monitoring process. To achieve such impartiality, SAIC will work with the assessor to avoid mutual or conflicting interests with the organizations where the assessments are conducted. SAIC will develop and propose to VITA the criteria to be met by any selected third-party assessor. These criteria will be used in selecting assessors throughout the term of the program. SAIC will work directly with the assessor to identify,

confirm, and report to VITA about systems that have failed to meet SLAs over the period defined for the assessment. Our Chief Information Security Officer will oversee the assessment to ensure the independence and integrity of the assessment findings.

Security Incident Management. SAIC's approach to providing security Incident Management combines the expertise of credentialed professionals, VITA rules, industry best practices (e.g., ITIL, NIST SP 800-61), cooperation of and with STSs, and market-leading tools (e.g., CyberArk, Splunk, Keystone Edge based on ServiceNow) to create a response solution that mitigates security Incidents affecting the COVA IT environment. SAIC will address threats to VITA and Customer information systems and data, using a full life-cycle approach that integrates Plan-Do-Check-Act management with the NIST-recommended Incident life cycle, as depicted in **Figure 4.7-3**. SAIC's Security Incident Management activities—including Incident response coordination, forensic investigation, and escalations to VITA and Customer security contacts—will be provided on a 24 hours per day, 7 days per week (24x7) basis. Staffing will include dedicated security operations staff throughout the Business Day with on-call support for off-hours, holidays, and weekends consistent with practices in place today and commensurate with security Incident workload and patterns.
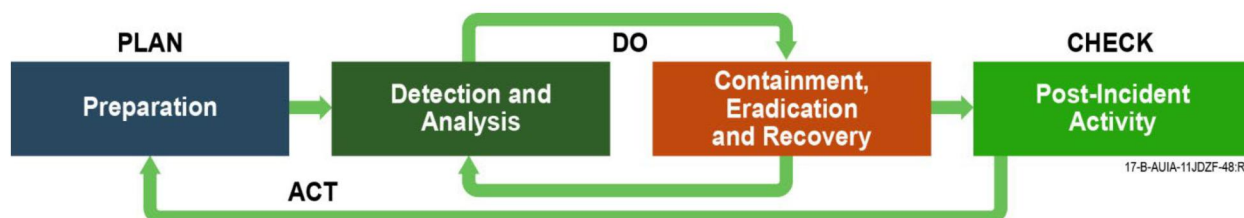
Figure 4.7-3. SAIC's CSI-Based Incident Management Life Cycle

Effective performance of the Incident Management lifecycle requires harmonized technology, people, and process of SAIC as the MSI coordinating MSS with the other STSs. SAIC focus on overseeing and managing the end-to-end lifecycle by leading the development and refinement of the Incident Management plan with participation from VITA and the STSs. The MSS, using the MSS-SIEM, Intrusion Detection and Prevention Services (IDPS), firewalls and other Incident detection and analysis processes and tools, focus intensively on identifying, detecting, analyzing, recording, and qualifying cyber Incidents. When SAIC is notified by the MSS, and we will coordinate and ensure effective and appropriate communication with all required parties. SAIC will direct the performance of the Incident Management plan to achieve rapid containment, eradication, and recovery. These tasks (containment, eradication, and recovery) require coordinated and execution of technical tasks to return systems and services to operations. In the final stage of the lifecycle, SAIC leads the Root Cause Analysis and post-Incident recovery with participation from all the suppliers to learn from each Incident as well as document and plan changes to further improve VITA's cyber security posture and cyber security operations through better prevention via additional or changed tools, controls, processes, and procedures.

SAIC's initial assessment performed during implementation provides detailed insight into the IT environment security Incident Management capability, threats, existing Incident Management plans, security Incident history, and tools and techniques in use. Following this assessment, SAIC will document the existing Incident Management baseline and finalize the design and implementation for the SAIC Incident Management solution. The SAIC Lead Security Analyst responsible for Incident Management will lead the establishment of a documented baseline of existing processes, SOPs, technology platforms, and key stakeholder priorities. As needed, VITA's Incident Management plan will be updated to reflect the current baseline.

SAIC will coordinate with STSs to develop an updated Incident Management plan that reflects the introduction of the SAIC Incident Management solution structure, processes, procedures, and integrated

SMS technologies (Keystone Edge for Incident Management, Splunk for data analytics, and CENTER for document storage). Our solution will enable efficient and effective Incident handling capabilities, using automation and enhanced analytics in collaboration with the STSs. The integration of Splunk Enterprise Security and the Keystone Edge Security Incident Response module will link IT and security Incident Management, aid rapid detection and analysis of Incidents, and communicate response status and security posture situational awareness, thereby improving overall security Incident Management. This solution will equip SAIC and STSs to accomplish the following:

◆ Identify advanced persistent threats through analysis
◆ Initiate and track security Incident records
◆ Inform VITA and customers of User situational awareness by interfacing with SAIC CENTER
◆ Leverage policies that govern the response to security Incidents across the Managed Environment for supplier, STS, and Third Party Vendors
◆ Use the SAIC CENTER solution to store security standards, policy, and procedure documents because CENTER is capable of providing two levels of security to protect sensitive documents

In addition, SAIC will collaborate with the STSs to access our mutual subject matter expertise for the establishment of an SAIC-led Computer Security Incident Response Team (CSIRT). The CSIRT will consist of standing members as well as on-call members, as identified in response scenarios and escalations. Team experts will include System Security Engineers and Security Analysts with specialized knowledge and experience in several technical areas, including intrusion detection, forensics, vulnerabilities, and exploits.

Threat intelligence is an essential element in effective Incident Management. The combined capability of the MSS and SAIC's threat intelligence are leveraged to enable protection before impact as well as rapid and targeted response to threats in the IT environment. SAIC will integrate the MSS SOC functions and threat intelligence through defined, documented processes and procedures that will be collaboratively developed and published as a part of the shared service manuals and enabled through the ISMS and technology such as the SAIC-provided Incident Management function of Keystone Edge. Essential elements include the Incident response plan, Incident Management, and Change Management processes. Additionally, SAIC's Senior Cyber Security Threat Analyst will work with the MSS team to define and document methods and guidelines for the SOC to collect, analyze, share, and process threat intelligence using the SAIC ISMS, MSS-SIEM, SAIC Splunk-Data Analytics Platform, and Keystone Edge Incident Response technology.

After implementation, SAIC's Incident Handlers will overlay the continual improvement principle of Plan-Do-Check-Act on the Incident Management life cycle. SAIC Incident Handlers will provide information, direction, and assistance to address security Incidents related to OLA and SLA objectives to minimize or mitigate any impact to VITA and customer information systems and data. We will capture data, analyze data, and disseminate actionable threat and vulnerability intelligence to STSs for action. After successfully responding to any security Incident by executing the established Incident Management Plan, SAIC will perform a post-Incident review to inform updates of the plan and to identify and implement additional controls to prevent future occurrences of the same Incident. Periodically, SAIC will provide threat and vulnerability briefings to a wide variety of stakeholders across the VITA and Customer community.

The SAIC Cyber Institute will provide collaborative specialized cybersecurity training, education, research, and solution development support to assist in maintaining the operational knowledge and skills of SAIC VITA information security professionals and team members. This will maintain the readiness of our information security professionals to respond effectively to information security threats to, and Incidents affecting, VITA and its Customers. This training may also be made available to VITA and designated Customer personnel.

Security Clearance Management and Security Clearance People. To enable robust security clearance management, SAIC will establish a comprehensive security clearance database capable of tracking and reporting on all STS personnel. We will develop the policies, processes, and procedures for managing, updating, and editing the database. Keystone Edge will provide workflow for provisioning new employee equipment. It offers a portal-based solution that allows supervisors to request the proper training and access for Users based on their job roles. Keystone Edge's role-based security capabilities will be used with the system to manage User access of applications to validate and/or initiate the appropriate background check, validate and/or initiate required training, and apply appropriate roles, groups, and permissions upon approval. In addition, a request to disable a User Identification (ID) or to revoke User access to applications will trigger an automated workflow to remove or update roles, groups, and/or permissions.

We will use Keystone Edge to document, track, and assist in managing access approvals to VITA or Customer facilities, systems, services, and information. We will establish records for each individual with the required individual attributes, as shown in **Figure 4.7-4**, for all personnel requiring unescorted access to facilities, systems, and/or services.

SAIC Security Clearance System	
Employee Database Required Entry Fields	
Full Name	Company
Position/Title	Manager Name
Physical Location Assigned	Date of Clearance
Additional Customer Clearances	Customers Supported
Security Program Training (Completed)	Background Checks
Privileged Access Facilities	Security Badges Issued—Inventoried Item
Access Rights—User, Advanced User, Administrative	Free Form for Additional Remarks Not Otherwise Included

Figure 4.7-4. SAIC Security Clearance System

We will provide access to the SAIC Security Clearance System (via a portal) to STSs, Customers, and authorized Third Party Vendors. New personnel or new access requests will be initiated by opening a Service Request through the SAIC self-service capability in Keystone Edge or by directly contacting the SAIC Service Desk. Approved new User accounts will be updated within 24 hours. SAIC will document policies and procedures to be approved by VITA for removing personnel systems, service, and facility access and for deleting all User accounts, privileges, and access rights to VITA and Customer systems, services, information, and facilities. All SAIC employees, contractors, subcontractors, and any other identified parties proposed to be assigned to perform services will have successfully completed a background check before assignment.

4.8 Risk Management

Using our CSE solution, described in Section 4.7, we will discover the IT security risk baseline for VITA and its Customers. For ongoing management of IT risk, we align with the NIST RMF. Our CSE solution Discovery, Mitigation, and Management methods use our ISMS to identify threats and vulnerabilities; determine probability and potential impact; and assess, prioritize, and recommend mitigations to minimize IT security risks to VITA and its Customers. Our approach to managing IT security risk follows the six RMF steps depicted in **Figure 4.8-1**:

1. *Categorize Information Systems.* SAIC will collaborate with VITA and its customers and the STSs to categorize systems and data that are key to its business processes.

2. *Select Security Controls.* We will select an initial set of baseline security controls for the information systems based on the security categorization, tailoring the controls as needed by VITA and its customers.
3. *Implement Security Controls.* Our experienced staff will translate the required controls into requirements and design details to ensure that the controls mitigate the risk and vulnerabilities.
4. *Assess Security Controls.* We will use the CSE assessment of security controls compliance, deficiency level and remediation activities to identify risks to the Commonwealth.
5. *Authorize Systems.* Operations of an information system will be based on a systematic determination of the risk to VITA and it Customers.
6. *Monitor Security Controls.* We will implement continuous monitoring and an ongoing assessment and authorization process, as defined by NIST SP 800.137, to determine that the set of deployed security controls remain effective in light of planned and unplanned changes to the systems and environment over time. In this step, we combine the assessment discover and continual monitoring features of CSE.
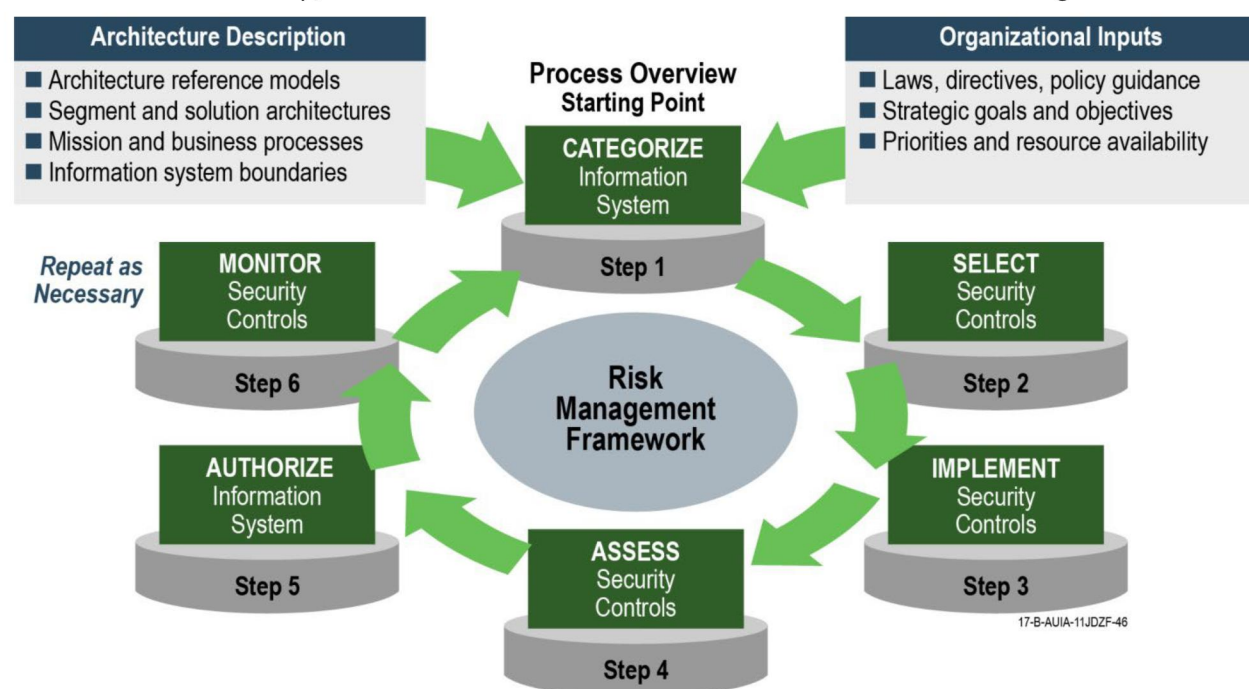
Figure 4.8-1. SAIC Application of NIST RMF to Risk Management

Risk Monitoring, Identification, and Reporting. SAIC will document risk management policies, methods, processes, and procedures in the SMM. This methodology addresses the full system (hardware or software) life cycle, starting at conception and including architecting and designing security into the system; implementing, testing, and evaluating the security of the system; and creating a security baseline before placing the system into operation. Early in the development life cycle or planned change, a monitoring plan is developed for new or changed systems.

Once in operation, systems will be monitored to detect anomalies and tested to verify that the systems maintain compliance with the designed and tested security baseline. We will monitor, test, and evaluate system to verify compliance, determine the ongoing effectiveness of risk response measures, and identify risk-impacting changes to VITA and customer information systems and information. Our Security Analysts and Chief IT Engineer will routinely analyze monitoring results to maintain awareness of the IT security risk. We will use implemented security tools to automatically monitor configuration settings, scan systems and applications for vulnerabilities, and assess security controls. Our monitoring activities will include

threat assessments, using methods from our CSE solution to identify exploitable weaknesses in deployed technologies that may affect VITA or customer mission success.

SAIC will provide access to monitoring data and analysis results to VITA's staff, auditors, and regulators in conducting assurance activities on the design and effectiveness of key controls across the end-to-end services. All analysis results and derived reports will be maintained in the SMM, including an operational risk register. Analysis data and reports stored in CENTER and Keystone Edge will be made available to existing VITA tools via an automated interface.

Risk Prevention and Mitigation. SAIC's solution for IT security risk prevention and mitigation is based on our knowledge, experience, and successful delivery of RMF services to DoD, NASA, and federal, state, and local government agencies. SAIC will work directly with STSs to consistently achieve end-to-end IT risk management for business services, and we will use our tools, integration, and collaboration processes to maintain efficiency, visibility, and transparency across the environment.

SAIC provides experienced, well-trained, and industry-certified—Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Security+, Global Information Assurance Certification, and Global Information Assurance Certification - Certified Intrusion Analyst— cybersecurity professionals. Our integrated team will provide a seamless end-to-end ITIL security support model that begins with existing VITA security and ITIL processes that will be created, updated, and maintained in CENTER as part of the SMM. Our approach and mature processes are tightly integrated with our Incident, event, and Problem Management activities to provide correlation and early detection of risks.

SAIC will maintain a continual service improvement register for cybersecurity and risk management and will use it as the basis for providing recommendations for improvements that, if approved, are implemented via the Change Management and Project Proposal processes. We work with the STSs to document and implement continual monitoring. This process determines whether the set of deployed security controls remains effective in light of planned and unplanned changes that occur in the system and its environment over time. As part of day-to-day operations defined in the SMM processes, SAIC will perform periodic vulnerability scans and will scan all new systems for threat mitigation before production implementation. If the scans detect weaknesses, we will collaborate with the appropriate STS to implement time-sensitive security patches to mitigate the vulnerabilities and will monitor their progress. If any of the weaknesses are identified as a zero-day vulnerability, also known as a zero-day attack, we manage the mitigation of these weaknesses with the objective of identifying the exploit as close to real time as possible and quarantining the specific attack to eliminate or minimize the damage that could be caused by the attack. Our scanning tool, Tenable Nessus, provides for automated scanning against a wide variety of standards, threats, and vulnerabilities, offering a rapid approach to assessing gaps with applicable standards, including Payment Card Industry (PCI), CIS, and the DISA implementation guides.

SAIC will perform periodic risk assessments for the managed environment in collaboration with VITA, Customers, and STS personnel. The results of those assessments will be stored in our SAIC CENTER-based risk management system, with integration to the Governance Risk and Compliance (GRC) system. In addition, SAIC will also act as the central point of coordination for VITA and Customers for the coordination of external Third Party Vendor audits. Our tools and integrations will provide designated Users with access to all dashboards, risk registers, artifacts, plans, policies, procedures, reports, and supporting documentation produced as part of overall risk management activities. Our ISMS, security Incident management, Vulnerability Scanning System, CMDB, and centralized logging solution will provide direct integrations to the GRC platform to support overall risk, governance, and compliance activities at the enterprise level and in an automated and transparent fashion. CMDB integration also supports our mapping of supporting assets to critical business processes, allowing for appropriate prioritization and

response to Incidents based on the criticality of services. Our dashboards, reports, policies, and procedures will be maintained on our access-controlled secure CENTER document data store, accessible for authorized Users via the single SAIC Portal.

The electronic integration of the Keystone Edge ITSM platform, including the asset database as well as the security operations module, will enable VITA to get additional value from the existing investment in the RSA Archer eGRC platform. In addition to the ability to prioritize responses as noted above, this integration also provides VITA with complete visibility and transparency into the assets that exist in the ITISP. This data access supports a variety of security management activities, including more holistic business impact assessments, by providing the ability to tie risks and threats directly to the business applications and their supporting infrastructure. Similarly, individuals with appropriate access rights will also be able to view, in real time, all current and historical security Incidents and to relate those Incidents to activities with RSA Archer, thereby providing a more complete view of enterprise security in a central dashboard and location. As a result, security activities are more responsive, complete, and easier to manage to support the compliance and security requirements of the Commonwealth. SAIC will complete the technical integration between VITA's RSA Archer and our Keystone Edge system, and will provide all ongoing maintenance required for that integration. SAIC does not require any additional support for our use of the existing RSA Archer implementation for risk management services.

SAIC Cybersecurity Analysts maintain awareness of emerging security threats, advisories, bulletins, new security technologies, and changing security regulations, directives, and guidelines, such as the Federal Information Security Modernization Act of 2002 (FISMA), NIST, and Federal Information Processing Standards (FIPS). The team will communicate that information to the STS teams to maintain the appropriate security posture across the managed environment infrastructure. We will lead the coordination and collaboration required for security Incident investigations and will escalate trends, major Incidents, and new risks to VITA for awareness and action, as required, including the development of proposals to raise the security state of critical assets and business services.

As an active element, risk management includes maintaining cyber situational awareness. SAIC actively participates in communities such as the Defense Industrial Base, NIST, and Department of Homeland Security (DHS) forums to stay apprised of changes in industry and the regulatory environment. Our Cyber Lead and Analyst supporting VITA are subscribed to publications, and they attend conferences and briefings to stay current on legislation that impacts cyber operation. This includes providing responses and input to government solicitations for input, drafting whitepapers, and developing briefings for VITA.

4.9 Supplier Management

The Supplier Management role is focused on enabling the efficient and effective operation of the Managed Environment by providing a management point of contact and oversight for SAIC with each Service Tower Supplier (STS). Our approach includes a dedicated Supplier Manager with responsibility and oversight for this function across the program, supported by other managers within SAIC's team who will be assigned to corresponding STS management contacts. These assignments will also encourage and support daily interaction as part of normal Service Management operations. **Figure 4.9-1** provides an overview of key interfaces and responsibilities for the Supplier Management function.

The SAIC Team's Supplier Management module in Keystone Edge is focused on monitoring STS performance across all provided services to evaluate whether the STS continues to provide business value to the Commonwealth. Because SAIC shares the STS oversight responsibility with VITA via the governance approach, SAIC's supplier management solution will attempt to correct STS service performance issues first and will only recommend a change of STS providing the services if our analysis

Interface to VITA and Customers	Interface to Suppliers
◆ Working in conjunction with VITA Customer Account Managers and SAIC Business Relationship Managers, identifies Demand Requests and coordinates resource requirements with STSs ◆ Acts as a management escalation point for service delivery and performance issues with assigned suppliers	◆ Ensures that STS services are available as requested by VITA and Customers at agreed to service levels and are performed in accordance with established OLAs ◆ Is responsible for consolidating requirements for strategy and design of new external services, scanning the market for potential providers, negotiating with the selected supplier, and assisting in the on-boarding of external suppliers and service roll-out to customers ◆ Is responsible for working in tandem with the BRMs in ensuring that value of services obtained from all STSs meets or exceeds Customers' expectations

Figure 4.9-1. Supplier Management Effectively Integrates Delivery Across the MSI and STSs

Interface to VITA and Customers	Interface to Suppliers
◆ Coordinates supplier technology and new service offering proposals	◆ Works with any new proposed Service Provider in development of contractual SOW for consideration by VITA ◆ Negotiates and documents OLAs ◆ Provides performance management and oversight of service delivery, including escalation when OLA and/or SLAs are in danger of breach ◆ Acts as an escalation point for Major Incidents ◆ Facilitates the effective electronic and process integration with MSI ◆ Oversees progress on relevant Continual Service Improvement initiatives ◆ Coordinates audit activities and oversees remediation action plans

Figure 4.9-1. Supplier Management Effectively Integrates Delivery Across the MSI and STSs (continued)

determines that it is not cost-effective for the STS to continue in that role. In addition, for new or modified STS services, SAIC will evaluate the feasibility and cost-effectiveness of STS proposed new services and will report results to VITA through the governance mechanisms. When necessary, we will incorporate supplier strategy within IT strategy and technology planning activities to guide change in the VITA supplier landscape.

Each STS is assigned a Supplier Manager (SM) to provide the necessary single point of MSI management oversight for each supplier's performance. Because of the criticality of this role, each SM is a senior IT staff member with experience in delivering and/or overseeing the scope of services provided by the STS. The SMs work directly with the supplier and participate in the STS meetings described in Section 3.4.2 to drive solutions to service issues and the development of new services. Our SMs are integrated with our Business Relationship Management team and approach. We will establish the supplier relationships around the fundamental principles of open communication, mutual trust, collective responsibility for service delivery, and shared risk.

Our SMs will lead the establishment of STS OLAs describing the specific service performance attributes, standards, measures, data ownership rights, and key process elements necessary for effective supplier management service delivery. As described in Section 1.3, SAIC will facilitate an iterative process with VITA and each STS to carefully and completely document OLAs that support VITA's SLAs and governance expectations. The SAIC Team will work to develop OLAs that are as follows:

◆ Only inclusive of obligations that require some form of formal agreement between two service towers and when possible they will be measured electronically to facilitate objective performance reporting
◆ Comprehensive and unambiguous, allowing the agreed-to operating level to be fully understandable from this one document
◆ Consistent with all other OLAs to support achievement of VITA's SLA performance goals

Keystone Edge and CENTER will be used to support the supplier management function. Keystone Edge provides key information on Incident, problem resolution, and Service Request performance. The SACM repository will be used to validate STS compliance with their patching, maintenance, and currency requirements. For any deficiencies identified, the SAIC Team will work with that Service Tower Supplier to ensure a remediation plan is in place and will monitor that plan through completion. Keystone Edge and CENTER together provide the central repository for supplier Project status and plans. CENTER is also the shared repository for OLAs and other documents.

In addition, the effective integration and operation of STS services into the overall ITISP will require each STS provider to:

◆ Provide a corresponding point of management contact
◆ Electronically integrate with the SAIC SMS and ITSM systems, including Incident Management, Request Management, Event Management, and Service Asset and Configuration Management
◆ Negotiate and agree to OLAs that underpin SLAs, as required
◆ Adhere to common processes and procedures, and develop tower-specific procedures, as part of the overall SMM.

5.0 SERVICE TRANSITION

The SAIC Team's service transition approach is to provide ITIL–based control mechanisms, such as change, release, and deployment, service asset and configuration, and knowledge management processes in the service delivery environment that is structured and automated and easy for the STS to use and will successfully introduce modified and new IT services into the VITA ecosystem. By implementing structured automated service transition methods, both the Commonwealth and VITA will benefit from the ability to field services more rapidly and with higher quality (e.g., improved, aligned with the Commonwealth's objectives, and with fewer defects).

We will provide integration, management, and coordination of all changed services between all providers using our SMS to track and correlate change and configuration information across functions, sites, regions, STSs, and Third Party Vendors. We will automate these process mechanisms so that the marketplace of choices available to Customers can rapidly evolve, and to provide newer technologies within those service offerings. Such automation will permit those Customers to focus on their individual missions to provide services to Commonwealth citizens, while VITA and the ITISP provide for their IT needs.

We based this approach on our successful delivery of implementing ITIL–based processes into an ITSM life-cycle framework across many government agencies, such as the DOS, USDA, NASA, Marine Corps, U.S. Army Central Command, and U.S. Army Reserve Command. Along with government agencies, SAIC uses our experience with commercial clients and in our own Integrated Service Management Center (ISMC) in Oak Ridge, TN, a living model of how to integrate ITSM into a mission-critical environment. We developed our United Solutions process asset library (PAL), which provides the SAIC Team with our documented, tested, and proven processes, from this experience and provides our team with a valuable asset to enhance VITA's ability to deliver IT services.

5.1 Change Management

The Change Management process provides the necessary controls to deliver IT services in a stable environment by facilitating beneficial modifications to VITA's IT operations and promoting efficiencies while mitigating risks. SAIC's approach to Change Management will be governed by VITA's SMM and the ITISP. SAIC's Change Management process will use the Keystone Edge SMS that automates strong integration between Change Management, Release Management, and Configuration Management, as demonstrated in **Figure 5.1-1**.

Keystone Edge provides the automated and workflow-enabled control mechanism used by all Service Towers for all changes to the operational environment, including normal changes, Standard Changes, and emergency changes. The Change Management process coordinates and tracks all changes until they are approved, tested, and implemented to maximize success and minimize risk. When the need for a change is identified, it will be registered and tracked in the Request for Change (RFC) module in Keystone Edge, which will contain all of the information required for the proposed change. The Change Management team will validate the readiness for review and identify impacted CIs based on the Keystone Edge CMDB module. Release Management will validate testing plans and results and will assign a proposed implementation time in the Forward Schedule of Change. Based on Change Control Board (CCB) approval, the Release Management process will oversee implementation of the new change into the environment and the Post Implementation Review (PIR) will evaluate the effectiveness of the change.

End-to-End Change Management

Service Provider			New Service Implemented
Change Management	Tower enters Request for Change (RFC) in ServiceNow → Validates RFC Based on the Services Management Manual	RFC Approved by Change Advisory Board	Oversees Closing of RFC and Post Implementation Review
Release Management	Oversees Testing and Implementation Plan	Coordinates RFC Implementation	Coordinates Early Life Support for New Service
Configuration Management	Determines Impact of RFC Based on CMDB	Updates CMDB to Reflect RFC	

17-B-AUIA-11JDZF-37:R2

Figure 5.1-1. SAIC's Keystone Edge Automates Integration Between ITIL Service Transition Process To Enable Rapid and High-Quality New Service Implementation

Change requests will vary in time to implement, and will require various degrees of planning, validation, build activities, test, and approval for implementation. To facilitate this and provide ongoing visibility into the process, SAIC uses the concept of Change Models integrated into Keystone Edge through workflows. Change Models allow changes of a specific type to have defined, expedited processes for approval. Commonly requested low risk changes, which have a defined trigger and well-documented tasks, will be further expedited as a pre-approved Standard Change.

5.2 Change Evaluation

Change evaluation assesses the potential change's impact before those changes are allowed to proceed. Major changes will constitute an engineering Project and be executed following the processes developed in our PAL.

Based on these proven procedures and tools, SAIC will provide an end-to-end Change Management process that minimizes risk, cost, and business disruption while protecting the computing environment and delivery of related IT services. The SAIC Change Management team will provide validation and management of the change process. Authorized stakeholders provide input in the evaluation of the change with VITA and jointly provide approval for changes outside of the pre-defined operational parameters and change windows. SAIC's practice is to ensure that Customers that may be impacted by a change are aware of the change and its potential implications prior to implementation for an informed agreement of the change and timing. It is SAIC's stated goal to minimize or avoid Customer disruption within the change process.

NASA EAST

SAIC supports:
◆ 10,000 software and system requirements for over 35 large projects
◆ 240 IT systems with 600 application integrations
◆ 60,000 users
◆ 500 release package deliveries, including 12 major releases

5.3 Release and Deployment Management

SAIC, as MSI, will provide full oversight and coordination responsibility for release and deployment into the production environment. Through process integration and automation using Keystone Edge, we assure changes to services will be tested, approved, coordinated, implemented, and verified, ensuring success while minimizing risk. Release and deployment works closely with Change Management to ensure that proposed changes are properly documented and tested. Once a change is approved, Release Management oversees the coordination, verification, and post-change activities necessary to successfully implement the change into the environment, according to the three following approaches.

> **U.S. Army Human Resources**
>
> SAIC supports:
> ◆ Full software development life cycle for new and existing web-based Army-wide applications
> ◆ 64 mission essential applications
> ◆ 50 releases every year of mission applications

All new or major changes to services will be approved through the ITISP Governance process as defined in the SMM, following approval by Commonwealth enterprise architecture and enterprise security teams for alignment with documented compliance requirements and standards. ITISP Governance may choose to approve a service pilot and as part of the approval would define the scope, duration, participants, and success criteria of the service pilot. Implementation of a pilot service would follow standard Project and Change Management practices including scheduled change control for the implementation of the service along with supporting communication to stakeholders and the end user community. Access to pilot services will be restricted via the Service Catalog so that only Users within the authorized pilot group will have access to request these services. Pilot services will be expected to meet all requirements of standard services, including but not limited to: Service Catalog ordering; service desk support procedures; end user communication and training (if required); creation or update of supporting CIs within the CMDB; and documentation of architecture, support model, and processes.

5.3.1 Service Validation and Testing (SV&T)

SV&T ensures that a service will provide the functionality and availability expected following the introduction of a change to the environment. This function will be coordinated from within the Joint Operations Center as part of the Change, Release and Deployment Management Team. The SAIC Team will coordinate SV&T activities across the Service Tower Suppliers and with Customer application staff to provide the validation and verification required to support confidence in proposed changes and releases applied to the environment. SV&T records will be maintained within Keystone Edge and will include the fields and attachments required to capture and store related plans, documentation, and approvals. All records will have direct association with related processes and process records including Service Asset and Configuration Management (SACM) and Business Service Mapping to provide for consistency in record maintenance and visibility into assessment of impacts of changes.

During Implementation, the SAIC Team will create a SV&T process as part of the SMM that will describe the process, key roles and responsibilities, and workflow associated with SV&T. The SAIC Team will also work with the designated Customer personnel accountable for business-critical applications and develop a standard checklist and set of controls associated with their applications. Once approved by the Customer application owner, the SAIC Team will ensure that these checklists and controls are utilized by the STSs as part of the Change Management process, including the attachment of this documentation to the associated change and release records and documentation of customer acceptance. Service Tower Suppliers will also have the ability to attach further documentation of their internal testing and validation plans and results.

SV&T of IT assets and services will often span across technologies managed by multiple suppliers and customers. SAIC's Release Management team will provide testing integration across STS testing plans and

customer test plans. Integration of SV&T plans will include; coordination, scheduling, and management of the overall process, ensuring supporting documentation is attached to the related change records within Keystone Edge; obtaining customer approval and sign-off for the integrated plans and results; and managing conflicts and gaps between plans to provide comprehensive and effective test results.

Test environments and test data will be maintained by the respective Service Tower Supplier and/or Customer. SAIC will provide support for the evaluation and selection of tools to manage test environments, as well as toolsets that support automated SV&T activities.

Our release management team will oversee testing prior to change approval. Using SAIC's ISO 20000–certified United Solutions' process automated in Keystone Edge, the SAIC Release Manager will ensure the release's test is documented (or has an approved exception) prior to its deployment into the VITA environment. Test plans from all STSs will be stored in the SMS release record, along with test results, and back-out plans. For all failed tests, release management will work with the technical teams to identify possible contingencies. If a contingency is not available or is unsuccessful, we will execute a back-out plan and initiate a Root Cause Analysis in conjunction with problem management. The outcomes of the SV&T activities will be reported back to the designated Customer contact(s) for each service affected.

5.3.2   Pre-Production Testing

The SAIC Release Manager will validate that the change has been properly tested across all appropriate suppliers. Validation of impacted CIs will be performed using the SMS, and test plans will ensure Customer completion of functional testing; systems integration testing; data conversion procedure; Local Area Network (LAN) and Wide Area Network (WAN) connectivity testing; system load, reliability, and performance testing; regression testing; compatibility testing; User acceptance testing; and Customer approval to release into production.

5.3.3   Post-Deployment End User Support

After production deployment, verification testing is performed in the production environment to confirm the release was successful. The Test Manager coordinating verification and User acceptance testing will report the results to VITA and the appropriate suppliers will conduct stakeholder acceptance. Acceptance documentation (e.g., email, screenshots, and test results) will be attached to the RFC. Once the release has been successfully deployed to the production environment and all release elements are completed, we shall set the RFC status to "Implemented."

If there is a significant post-production problem with the release, it may be determined that the release must be backed out and a contingency plan put into place. The Release Manager will work with affected suppliers and the Change Manager to document, communicate, and execute any contingency plan necessary. The steps required to reverse an unsuccessful release are described in the back-out plan.

For the USDA risk management contract, SAIC performs capacity, service-level, and release management for dozens of RMA applications. By applying the same approaches discussed in this document, we have increased their up-time by 20%.

5.4   Service Asset and Configuration Management (SACM)

A function of the Keystone Edge SMS is a consolidated CMS containing details of all configuration items and their attributes. This data collection will be automated as shown in **Figure 5.4-1** using open interfaces; SAIC will exchange data bi-directionally with STS systems to create a single system of record for all configuration information.

Customers and Third Parties may choose to use the CMDB to track assets that are outside of the ITISP but related to their overall business services and operations. Multiple forms of importing and maintaining that data are available including electronic integration with Customer systems or import of delimited data in CSV or similar format. As with all records within the CMDB, these assets will have various attributes

based on asset type and include notation of the asset owner, technical contact(s), and sufficient information to categorize them within the CMDB. These assets will also be used in creating Business Service Maps of end-to-end services to aid in the assessment of impact and criticality of Incidents relating to application services.

This consolidated CMDB, as part of Keystone Edge, will provide a single, transparent, authoritative source of information about the business systems and their component parts. Through the integrated SMS, impacts and dependencies for proposed changes will be more readily identified. The benefits of an authoritative federated SACM system include the following:

◆ Increased efficiency and stability by providing a single authoritative source of all configuration data for IT infrastructure and services
◆ Minimized IT risks with better understanding of dependencies of proposed changes
◆ Enhanced capability to develop accurate release plans to minimize the likelihood of improperly executed changes
◆ Asset and configuration insight necessary to more rapidly troubleshoot Incidents to minimize negative impact on the VITA mission
◆ Rapid assessment of the impact of degradations and outages
◆ Capability to perform root cause analysis to detect deficiencies in the IT environment
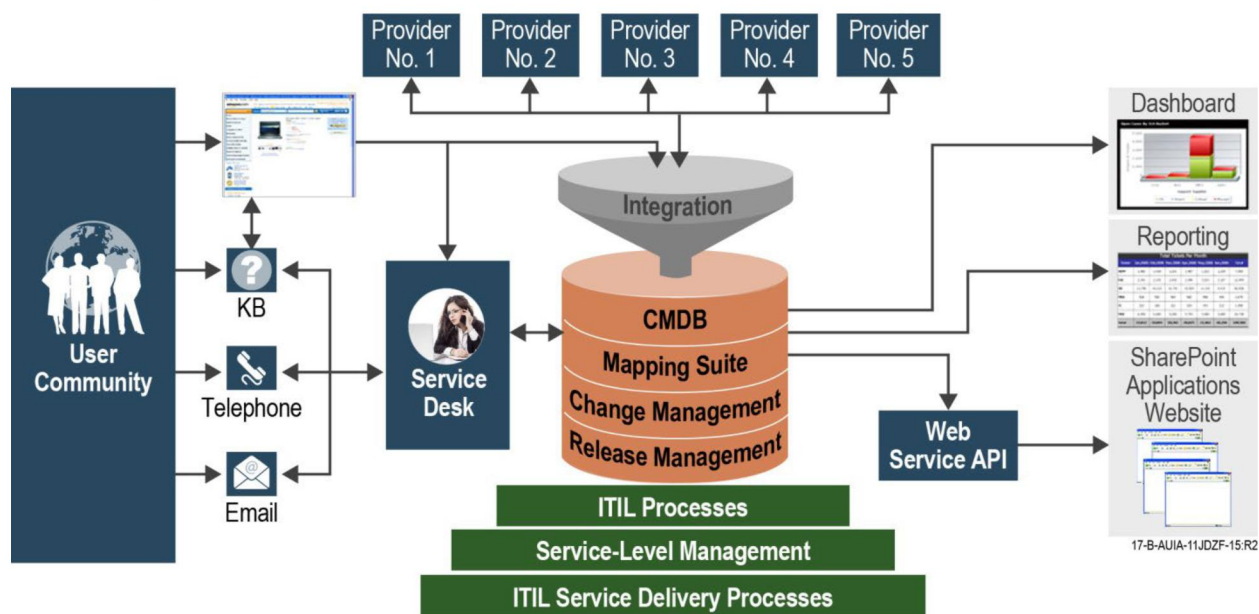
Figure 5.4-1. Federated Service Asset and Configuration Management System

License management and compliance are integral to Keystone Edge's CMDB component, enabling accurate tracking and monitoring of licenses. Inputs are collected electronically via integrations with each management tool utilized by Service Tower Suppliers. In the case of data discrepancies or changes, a review is triggered to ensure the accuracy of data in the CMDB. Each software license is also related to the underlying hardware, enabling traceability of usage. This up-to-date license information will then be used for a variety of purposes, including license allocation, utilization, and lifecycle assessments.

US Central Command

SAIC proactively reviewed software licenses and presented recommendations that saved $1 million annually

In support of the Defense Information Technology Contracting Organization, SAIC maintained $500 million in Defense Information System global network hardware and software assets deployed worldwide,

maintained and validated inventory information on 50,000 items, and tracked field change orders while managing $70 million in vendor maintenance agreements.

SAIC will also draw on our experience in bringing 61,000 CIs under Configuration Management control for the Marine Corps Enterprise IT Services (MCEITS), where we were able to maintain over 98.5% inventory completeness of all devices and provisioned software in the consolidated system.

5.5   Knowledge Management

SAIC's approach manages the collective knowledge of the ITISP using a knowledge-centered support construct to improve the speed, efficiency, and effectiveness of all operations. This methodology considers knowledge a key ITISP asset, where the content is captured and stored as part of standard operating procedures. We will work with VITA to develop a knowledge management taxonomy that structures knowledge artifacts in Keystone Edge and ensures their ease of use.

Knowledge Base (KB) articles (KBAs) from Keystone Edge will be used by all support levels, from self-service to Tier III, to answer How To's, request services, and perform troubleshooting. Initially, KBAs will be created from VITA's existing KB, and SAIC will use Keystone Edge's knowledge management taxonomy to structure them in the most efficient format for ease of access and use of information. Keystone Edge will also be the central repository for knowledge articles for other Service Tower Suppliers to ensure a common, Knowledge Base for service and support. Knowledge articles from other Service Tower Suppliers will be incorporated through direct integration as well as data import. This taxonomy structures the KBAs according to the knowledge base involved (e.g., STS and service provided), category of knowledge, published and valid-to dates, workflow state (e.g., draft or published), and linkages to attachments (other documents or images). Ongoing KBA creation and management will be a collaborative process between SAIC and suppliers, with the goal of continually providing information to enable the quickest response method possible. KBAs will be subject to a periodic review process to ensure they are still valid, valuable, and easy to understand. Our review process prioritizes review of articles by their use and removing those no longer pertinent to the current IT environment.

5.5.1   Training and Education

SAIC will provide a total training management and delivery solution to fully satisfy all of VITA's requirements. We have a long history of providing quality support to our customers based on direct experience with instructional support services. As a result, we offer a low-risk, high-quality solution to VITA's training requirements. We will meet this goal through highly experienced leadership supported by proven processes and best practices, unmatched client insight, and relevant, current IT training.

We will deliver training on MSI– or STS–provided services, our ITIL–based process implementations, and security procedures (see Section 4.7) through Keystone Edge to any User who needs training. Our training approach (see **Figure 5.5.1-1**) is based on a five-step process: requirements definition, syllabus and outline development, training-material development, training-material validation, and training delivery. We will adjust our process based on the completeness and maturity of the existing training curriculum and courses, and accommodate changes in services offered or Service Tower Suppliers.

Training for Customers to transition to the new support model will be conducted via live sessions that are also web-accessible to enable participation from a broad audience. Sessions will also be recorded and made available from the Portal. It is anticipated that most training sessions will take place in the 4 weeks preceding Go-Live. In addition to the live, web and recorded training additional documentation and How-To's will be provided via the portal for quick reference. Our approach and portal design emphasizes an interface that is intuitive and easy-to-use; as a result, past experience with similar transitions has shown rapid adoption and increase in customer satisfaction.
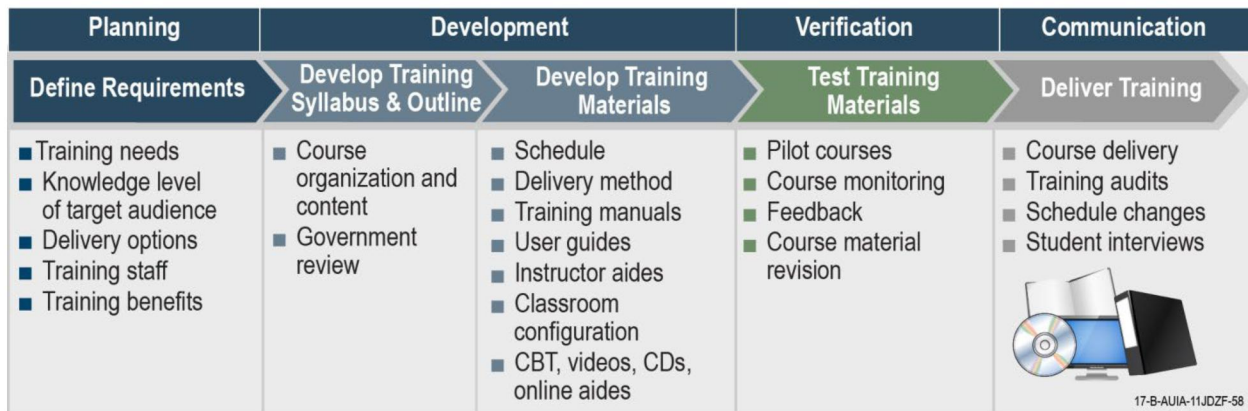
Planning	Development		Verification	Communication
Define Requirements	**Develop Training Syllabus & Outline**	**Develop Training Materials**	**Test Training Materials**	**Deliver Training**
■ Training needs ■ Knowledge level of target audience ■ Delivery options ■ Training staff ■ Training benefits	■ Course organization and content ■ Government review	■ Schedule ■ Delivery method ■ Training manuals ■ User guides ■ Instructor aides ■ Classroom configuration ■ CBT, videos, CDs, online aides	■ Pilot courses ■ Course monitoring ■ Feedback ■ Course material revision	■ Course delivery ■ Training audits ■ Schedule changes ■ Student interviews

17-B-AUIA-11JDZF-58

Figure 5.5.1-1. We Use a Solid Five-Step Training Approach That We Can Tailor Easily To Specific Training Needs

Step 1—Define Training Requirements and Plan the Approach. To develop a clear understanding of the training required, SAIC's training personnel interview Customer representatives about what the training should accomplish (e.g., IT security, specialized training required for our Federal Aviation Administration (FAA) client–deployed hardware and software). We then assess the knowledge level of the target audience, the desired knowledge level that the training is to provide, and the disparity between the two. If needed, we may convene a focus group of target audience members to help with this evaluation. Identified training requirements will define the development of training packages. We identify our team companies' trainers who are knowledgeable about the specified system or equipment and experienced in the subject to effectively explain training materials and bring background and specific applications knowledge to the classroom. We compare available resources and training objectives to determine the optimum length and intensity of training.

Step 2—Develop Training Syllabus and Outline. Based on the training requirements defined in Step 1, our trainer develops an outline and syllabus for the planned training program. Initially, we outline course material to identify course organization and content. We present the outline to the customer to ensure compliance with intended objectives, working iteratively with the customer to refine the outline for review and approval. This process minimizes the risk of omitting important topic areas.

Step 3—Develop Training Materials. The training requirements and scope determine the most effective training method. Many possible training methods and materials are available (including classroom training, CBT, videotapes, hard copy tutorials, and reference information). We may use focus groups to help determine the most effective method of delivery for each course. Our experience has shown that input from focus groups is valuable for mitigating the risk of using ineffective methods and materials. To minimize scheduling risks, we will develop a detailed training schedule, including reserving facilities and equipment, and will share with VITA to ensure uninterrupted essential work. Upon approval, the shared schedule—with its outline of topics, training methods, and testing requirements—will enable students to prepare individual schedules and provide insight into training goals and expectations.

Step 4—Test Training Materials. After the training materials are developed, the trainer conducts a pilot to evaluate the course. We solicit feedback from participants to identify concerns and deficiencies. We review and evaluate this feedback to improve the training course as appropriate.

Step 5—Deliver Training. We provide different types of training and take into consideration the location of the students and optimal training methods. We will provide instructor-led training, train-the-trainer, and online self-paced training. Upon training completion, students will undergo a skills assessment to ensure proficiency. Students will then be asked to fill out course evaluations and we will collect feedback on the course materials, the trainer, and future training needs. When appropriate we may offer a sandbox

environment post training in which trainees can complete optional assignments in a safe environment. This approach allows Users to enhance their proficiencies without risk to the production environment.

Compliance with Section 508 Americans with Disabilities Act (ADA)

SAIC uses industrywide best practices to provide Section 508–compliant learning materials. We incorporate Section 508 compliance throughout the course design and development process, offering deliverables that comply with the letter of the law and uphold the spirit of the law.

During the Requirements Phase, we will develop an Accessibility Plan that outlines accessibility features and testing processes. Using the Accessibility Plan as a guide, our trainers create courses with accessibility in mind. We strive to provide the Section 508 User with as close as possible to the experience of a standard User.

SAIC's training materials are designed to work with the Assistive Technologies in use by the Commonwealth and as identified during the requirements phase. Our primary training methods include Instructor-Led Training and Distance Learning. To accommodate different types of courses, we will consider accessibility from multiple angles. For example:

Instructor-Led Training (ILT). ILTs generally use Word and PowerPoint. Common Section 508 concerns include document and table formatting, graphics that are accessible to low-vision/colorblind users and have alternate text, and closed captioning for video/audio.

Distance Learning (DL). Distance Learning materials will be hosted on the Service Portal. Word, PowerPoint, PDFs and recorded videos are the main formats for this type of course. In addition to other Section 508 concerns, being accessible to a screen-reader is paramount.

Examples of approaches utilized for both Instructor-Led Training and Distance Learning materials include but are not limited to the following example steps:

◆ Verify that current on-screen focus is discernable by assistive technology
◆ Ensure color coding is not the only means to enhance identification of important features
◆ Ensure electronic forms allow assistive technology access
◆ Ensure a text equivalent is provided for every non-text element
◆ Verify all information conveyed with color is also available without color
◆ Identify row and column headers for data tables (screen-reader accessible tables)
◆ Ensure electronic forms designed to be completed on-line allow people using assistive technology to access all the information, field elements, and functionality required for form completion and submission
◆ Ensure all supporting training and informational video and multimedia containing visual information necessary to comprehend the content is audio described
◆ Document utilizes recommended fonts (i.e., Times New Roman, Verdana, Arial, Tahoma, Helvetica, or Calibri)
◆ Document refrains from using flashing/flickering text and/or animated text
◆ Document file name is concise, generally limited to 20-30 characters, and it makes the contents of the file clear

Maintenance Considerations. Creating courses that can be maintained and updated throughout the asset life cycle is important. By creating courses that are consistent with Commonwealth requirements, and maintained consistent with a robust maintenance plan, we will be able to provide courses that allow for efficient upkeep, including future modification of Section 508–compliant attributes to comply with improving technologies and changing regulations.

5.5.2   Document Data Store

To facilitate VITA's document data storage needs, SAIC will use our CENTER tool that is integrated with Keystone Edge. This SharePoint-based system provides a secure, role-based data repository and supports real-time and asynchronous team collaboration, document sharing, and communication. SAIC will establish and consistently use document creation, naming, and version control procedures. As a web-based tool leveraging Windows authentication, CENTER will be easy to use for all suppliers based on their role across all service towers. **Figure 5.5.2-1** provides an overview of the capabilities CENTER offers for document management. Section 2.6.1 of Exhibit 2.3.2 provides further details of our proposed Document Data Store.
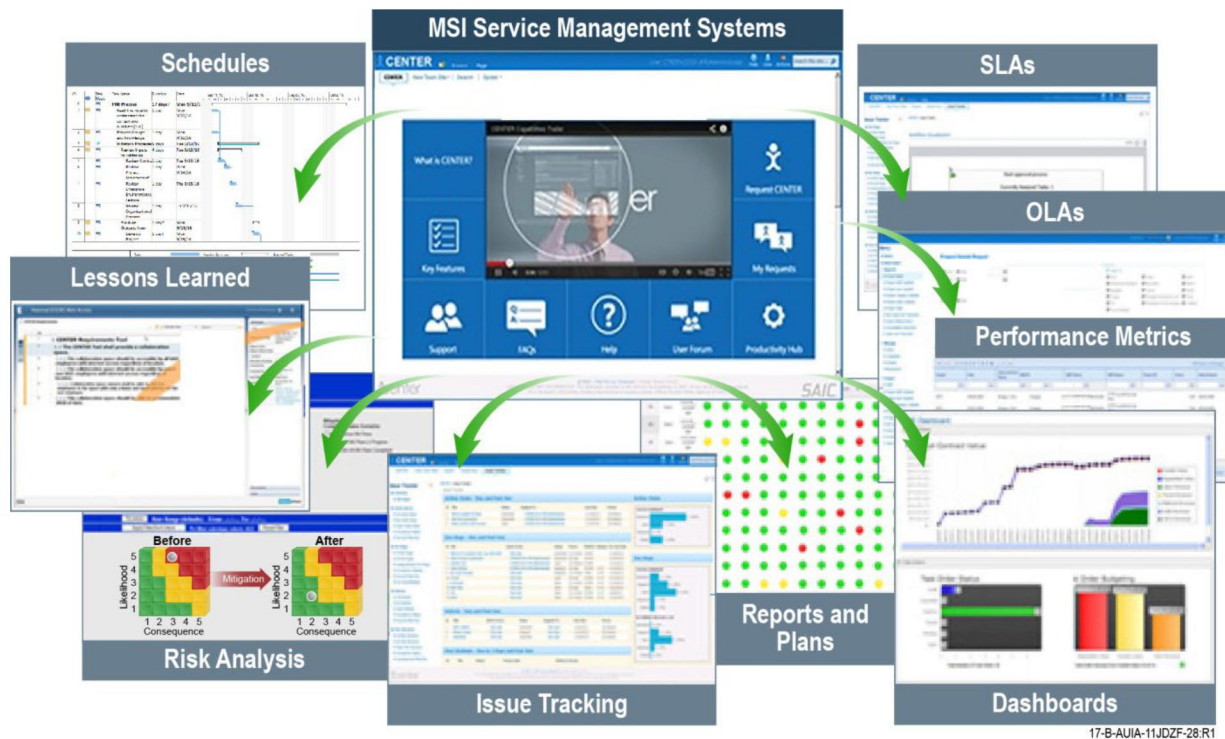
Figure 5.5.2-1. SAIC's CENTER tool

5.5.3   Contract Management

In addition to providing document management, the SAIC CENTER tool facilitates management of large-scale programs and their contracts. CENTER will enable VITA and the ITISP to collaboratively monitor, manage, control, and execute essential contract activities. Keystone Edge will monitor and track contract performance through its Service Management module to track all SLAs and SLRs for all service towers in a centralized database. CENTER also provides secure access to needed Project information and tools to enhance productivity and decision-making. CENTER and Keystone Edge comprise a centralized location to manage contract documents and enable connection to performance measurement dashboards.

5.5.4   Site Information Management and Customer Information Management

SAIC will track Site and Customer information as a program activity through CENTER. We will use metadata information maintained in CENTER will be used to populate needed information in Keystone Edge, providing consistent presentation and navigation.

6.0 SERVICE OPERATION

SAIC has extensive experience in providing service operations activities to many government agencies including NASA, MCEIT, U.S. CENTCOM, and U.S. Army Reserve Command. The "customer-facing" cross-

functional processes we apply from our United Solutions PAL are tightly integrated in Keystone Edge, which SAIC will use when operating the 24/7/365 Service Desk located in Southwest VA, and the Joint IT Operations Center located in Metro Richmond area. These will provide the flexibility to accommodate each Customer's unique requirements, and visibility into service delivery across all suppliers. In doing so, VITA and the Customers will receive the benefits of improved mission performance and clear service delivery accountability. **Figure 6.0-1** depicts how the solution delivers end-to-end operations, integrating with STSs and Third Party Vendors.
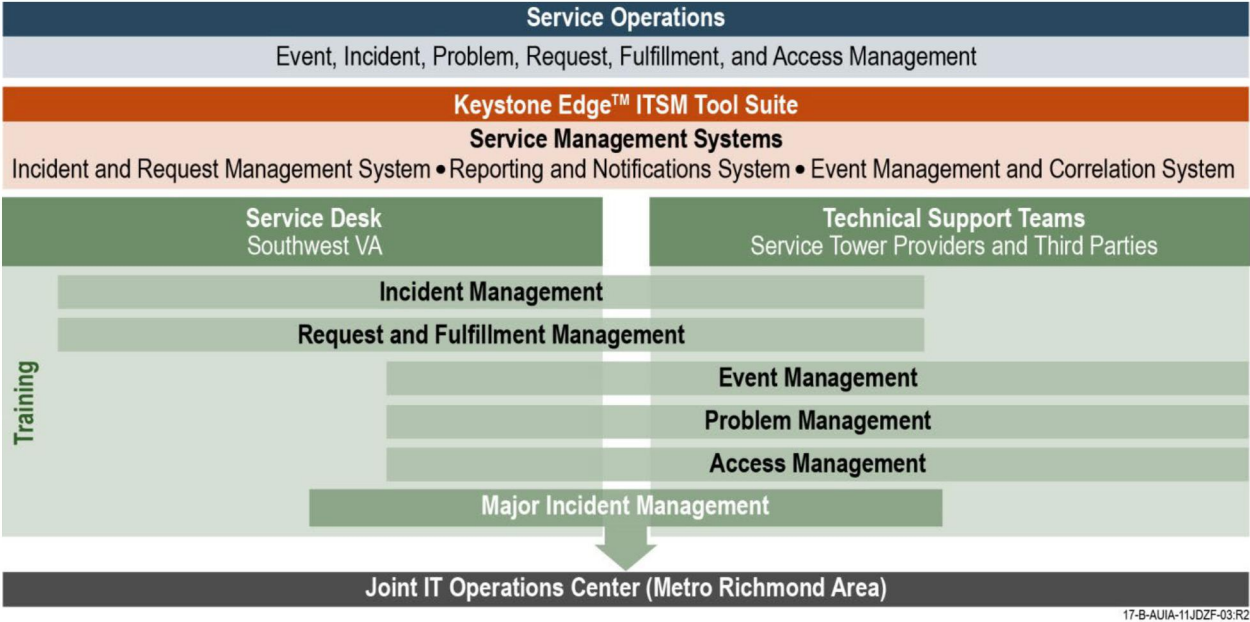

Figure 6.0-1. SAIC's Approach to Delivering End-to-End Service Operations

SAIC will apply our experience in providing support to commercial and government clients from our ISMC, which provides global Tier I, Tier II, and other managed IT services for government and commercial customers, including our own SAIC corporate users. Based on this experience and other engagements, SAIC will incorporate a suite of ITIL service operations-based repeatable, customer-centric processes that foster the environment needed for stable yet agile operations of the VITA IT infrastructure while reducing costs through continuous process improvement described in Section 7.0.

During the implementation phase, SAIC will perform an ITIL maturity assessment of VITA service operations to develop (a) what's working well, (b) what's not working well, and (c) what risks we foresee occurring by changing the technology and culture. We will pair this assessment with a road map for service modernization that will inform our efforts for improving both process and organizational maturity. Historically, the IT industry has tended to focus on process engineering and tool configuration without adequate governance consideration, which yields quick wins in transition but were unsuccessful in meeting their longer-term objective of connecting their improved process and tools with the people and governance processes. SAIC's approach focuses on the organization and Customers before changing each individual process area. We will collaborate with and work alongside suppliers with an emphasis on empowering them and identifying stakeholders to focus on organizational maturity.

Once the maturity assessment is completed, we will develop a deployment road map based on the current and desired state and gap analysis. The road map will include deployment of new tools including Keystone Edge and CENTER. Greater detail is provided in the process implementation response in Exhibit 2.4, Section 2.3, Process Implementation. As part of that deployment, SAIC will work with the STSs to

integrate their Service Management systems and event monitors with Keystone Edge, discussed in more detail in Sections 6.2 Incident Management and 6.3 Event Management. SAIC's solution will provide a consolidated view of IT operations for all service towers. This centralized view facilitates the ability to categorize and prioritize events, Incidents, and requests based on ITISP Governance.

6.1 Service Desk

SAIC is a market leader in providing Service Desk (SD) services. Our ISMC facilities in the United States (Broomfield, CO; Oak Ridge, TN; and Huntsville, AL) are certified by the International Organization for Standardization (ISO) 9001:2008 and are ISO 20000-1:2005–compliant. Our government and commercial customers include the DISA, NASA, Department of Energy, National Institutes of Health, City of Memphis, AOL, Marathon Petroleum, and the DoD.

SAIC Service Desk Highlights
◆ At our ISMC we receive over 1.3 million calls a year
◆ Log over 1.6 million incidents
◆ Support over 3 million global users
◆ Support over 20 government and commercial clients

SAIC has implemented a large number of successful SD transitions in government and commercial environments. We excel in rapidly establishing an IT SD to complement a full suite of program services. Services include deploying dedicated staffing, effective agent training, Incident Management system, customized automated call distribution, web-based Knowledge Base, and customized reporting. To ensure successful transfer of SD responsibilities, we will concentrate heavily on qualified incumbent capture, knowledge transfer, and introducing our PAL. To aid knowledge transfer on other SAIC contracts, SAIC has achieved incumbent retention rates greater than 97% when those incumbent personnel exhibit the necessary skills and experience to support our SD approach. Our detailed Implementation Plan in Exhibit 2.4, Section 2.1 depicts how we plan to conduct the SD implementation with no disruption of service to or negative impact on the User community.

We will apply the Single Point of Contact (SPOC) SD concept, where all Customers know where to go for information and help, providing an easy-to-use "one-stop shop" to resolve all requests and issues—from self-service help to creating or checking the status of a request or Incident. As illustrated in **Figure 6.1-1**, our approach greatly enhances the service response rate for Customers, our ability to detect trends, measure utilization, and expand the Knowledge Base for application to future efforts. In addition, calls to the Service Desk will be routed through our Automated Call Director (ACD) solution based on Genesys Pure Connect. This ACD system provides several benefits, including collection of metrics associated with time to answer and time on hold, call trees, informational messages, and the ability to route calls based on menu selections to ensure an appropriate agent is contacted.

The SD will be available for reporting issues, information queries, and requesting services 24/7/365 through a toll-free 800 number, web, chat, and email. We will train our agents in our ITIL–based and ISO–certified processes and procedures that include customer service skills and appropriate technical training.

Our "shift left" methodology will reduce VITA's support costs by creating a robust self-service portal to allow Users to report issues, request services, and access a User-facing KB, including a section for frequently asked questions (FAQs). This empowers Users to resolve their own issues and requests, reduces calls to the SD, and frees up Service Desk Agents to provide improved Customer service. Our experience has shown us that implementing this "shift left" methodology greatly improves User satisfaction. Additionally, SD personnel will be responsible for analyzing historical tickets to recommend FAQs for VITA approval that are pertinent to the current User environment and represent the most common issues and requests. SD Agents will routinely review the knowledge base to identify necessary updates and additions.

To provide VITA management visibility into SD effectiveness and help with understanding trends, SD personnel will provide standard scheduled reports required by VITA and ad hoc reports on request. We will also provide customizable dashboards with ticket metrics to ensure transparency.
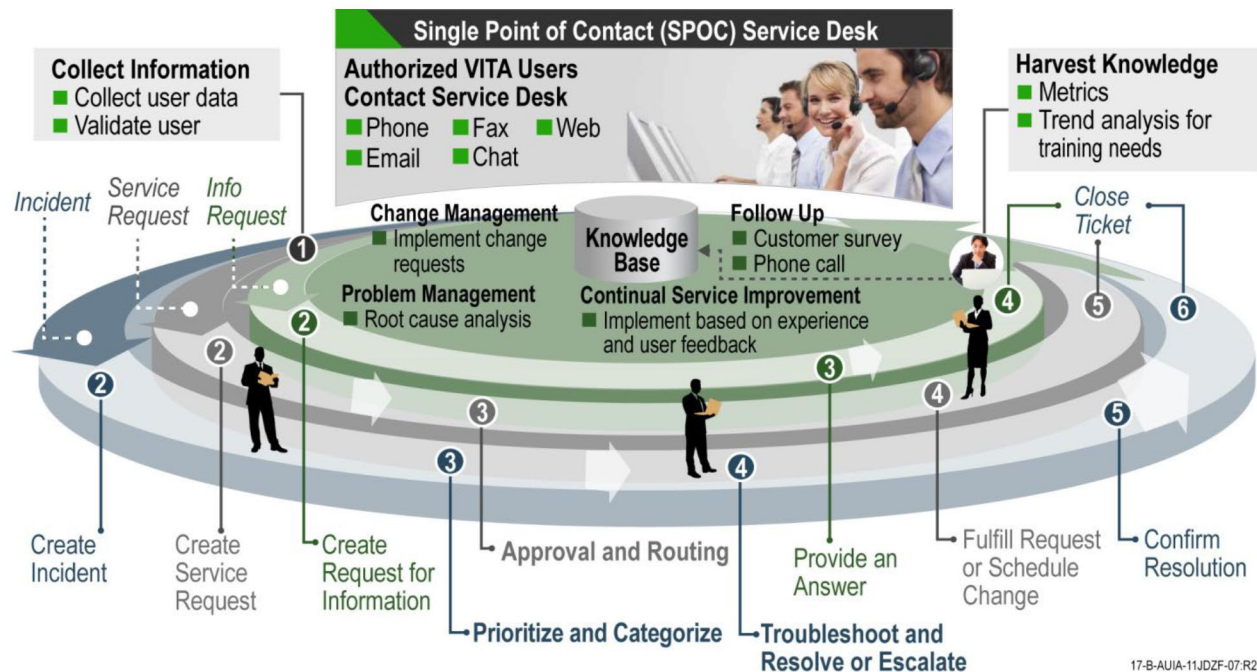
Figure 6.1-1. Single Point of Contact (SPOC) Service Desk Design

As depicted in **Figure 6.1-2**, our primary SD for the Commonwealth will be located in Southwest VA, to maximize capture of existing support resources and ensure support for the economy and employment opportunities of this area of the state. Clintwood, VA, has been selected as the primary location where SAIC has identified suitable facilities. This location has proximity to local universities that represent excellent training and staffing opportunities to contribute to the growth of the region. It is approximately 1 hour from the existing Service Desk in Lebanon, providing the opportunity to assess incumbent staff for transition. SAIC is also willing to explore the possibility of retaining Lebanon as the primary Service Desk location based on the availability of suitable facilities. Oak Ridge, TN, is our redundant Service Desk location. Both Clintwood and Oak Ridge are active at all times as a single virtual center with the majority of work performed from the Virginia location. The secondary location also provides surge and temporary augmentation capability and uses common processes, procedures, and workflow as the primary for seamless service regardless of location. The SD leverages Keystone Edge for automation of all services, providing continuity of service across multiple locations by virtualized ACD and Interactive Voice Response (IVR) and cloud-based platform hosting.

Disaster Recovery and overflow support will be provided from our ISMC in Oak Ridge, TN. This facility currently supports more than 30 customers and 3,000,000 end users. Disaster recovery between centers is tested annually, and cross-training programs are in place to ensure that support is seamless regardless of operation at the primary or redundant facility.
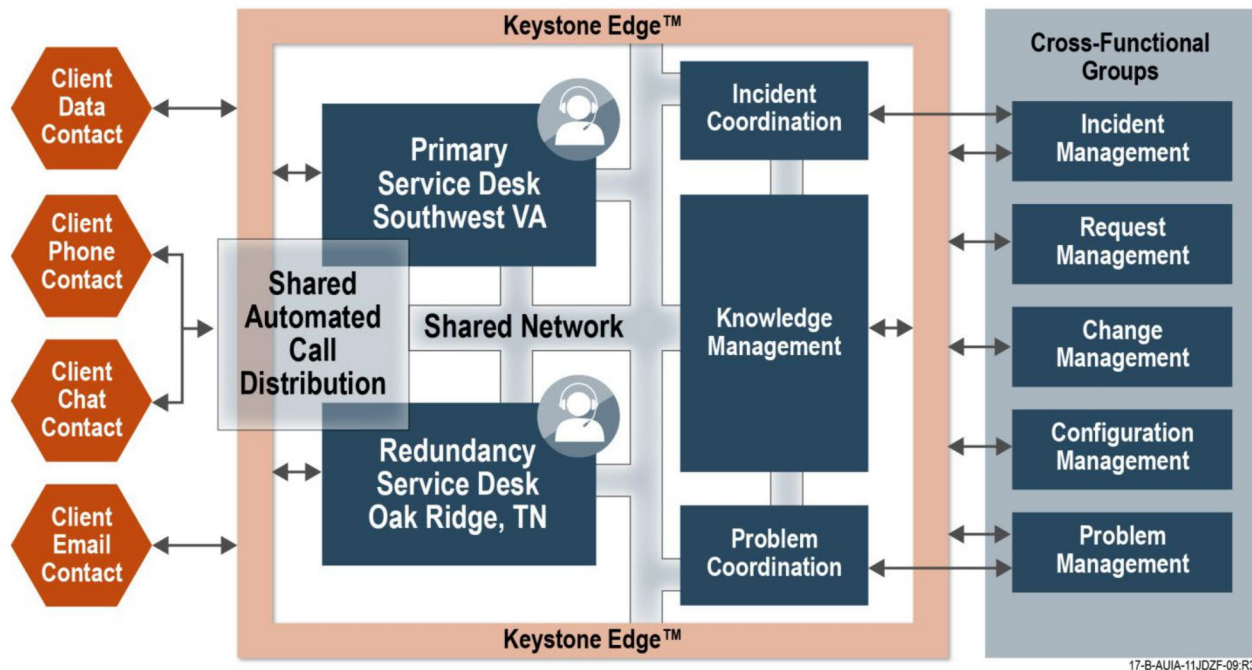
Figure 6.1-2. Service Desk Architecture

Our Service Desk solution utilizes Genesys Pure Connect for Automated Call Director (ACD) functions. This system is SAIC-hosted and virtualized for high-availability and continuous access across all ISMC locations, including the ISMC SAIC will implement for the Commonwealth in Southwest, VA. Additionally, the solution includes SAIC-hosted Bomgar Remote Support to provide for remote assistance for Commonwealth User computers by Service Desk personnel when requested and authorized by the User.

6.2   Incident Management

As documented in the PAL, SAIC's Incident Management (IM) process ensures a standard, ITIL–based method for handling Incidents. Our IM tools and processes, combined with our SD, will provide full life-cycle management and resolution of all Incidents across all STSs. Our solutions draw from over 20 years of providing IM from our ISMC and allow us to deliver the combination of ITIL best practices and real-world experience. Personnel may work and resolve Incidents at the SD, or escalate to appropriate parties (including STS or third parties) at any point. In the event that the Incident impacts a critical business system, the Major Incident Management process will be invoked. The SD is the common point to initiate this process and triggers a specialized form of IM that provides the swiftest possible services restoration. Major Incidents are defined by their severity and the business impact of the outage. SAIC will use a team of "Incident Commanders" to coordinate all actions across providers from the Joint IT Operations Center.

Timely, accurate and broad communications are key outputs from the Incident Management process. Users can self-subscribe to receive alerts and updates relating to business services directly through the portal and will automatically receive notifications when there is a status change for those services. Communication lists for management contacts will also be maintained within Keystone Edge, which will include all requested Customer and VITA representatives or email distribution lists for services. These distribution lists can include any number of Customer and VITA managers, Users, or sub-distribution lists. Incident notifications will also be posted to the web portal for visibility by all Customers. Communications include a description of the Incident, the known impact, and the major actions underway for resolution. These email notifications also include the contact information for the Incident Commander coordinating the response and the timeline for expected updates and resolution.

63

Incident Management is a component of SAIC's Keystone Edge that will be installed and configured during implementation on cloud-based systems hosted by ServiceNow in its primary data center located in Culpepper, VA. Backup services will be in its San Jose, CA, data center. SAIC has estimated sufficient licenses to provide access for required STSs, VITA, customers and third parties, and has included these costs in our proposal.

We will use Keystone Edge to notify Customers when an Incident is created, suspended, or resolved. These notification needs are often driven by the differing requirements between various Customers and the Incident's priority. For example, the resolution of a password reset for emergency responder tools would have a different impact and an associated higher priority than a password reset for a public library requiring quicker

U.S. Department of State

◆ Support more than 105,000 users
◆ Handle approximately 1,700 trouble tickets per month at embassies, consulates, posts, and annexes around the globe
◆ Implemented an incident management and problem management process that improved troubleshooting
◆ Reduced the number of categories for incident tickets,
◆ Enabling the Tier 1 team to process tickets more efficiently and enabling Tier 2 and Tier 3 engineering staff to focus on the most critical tickets
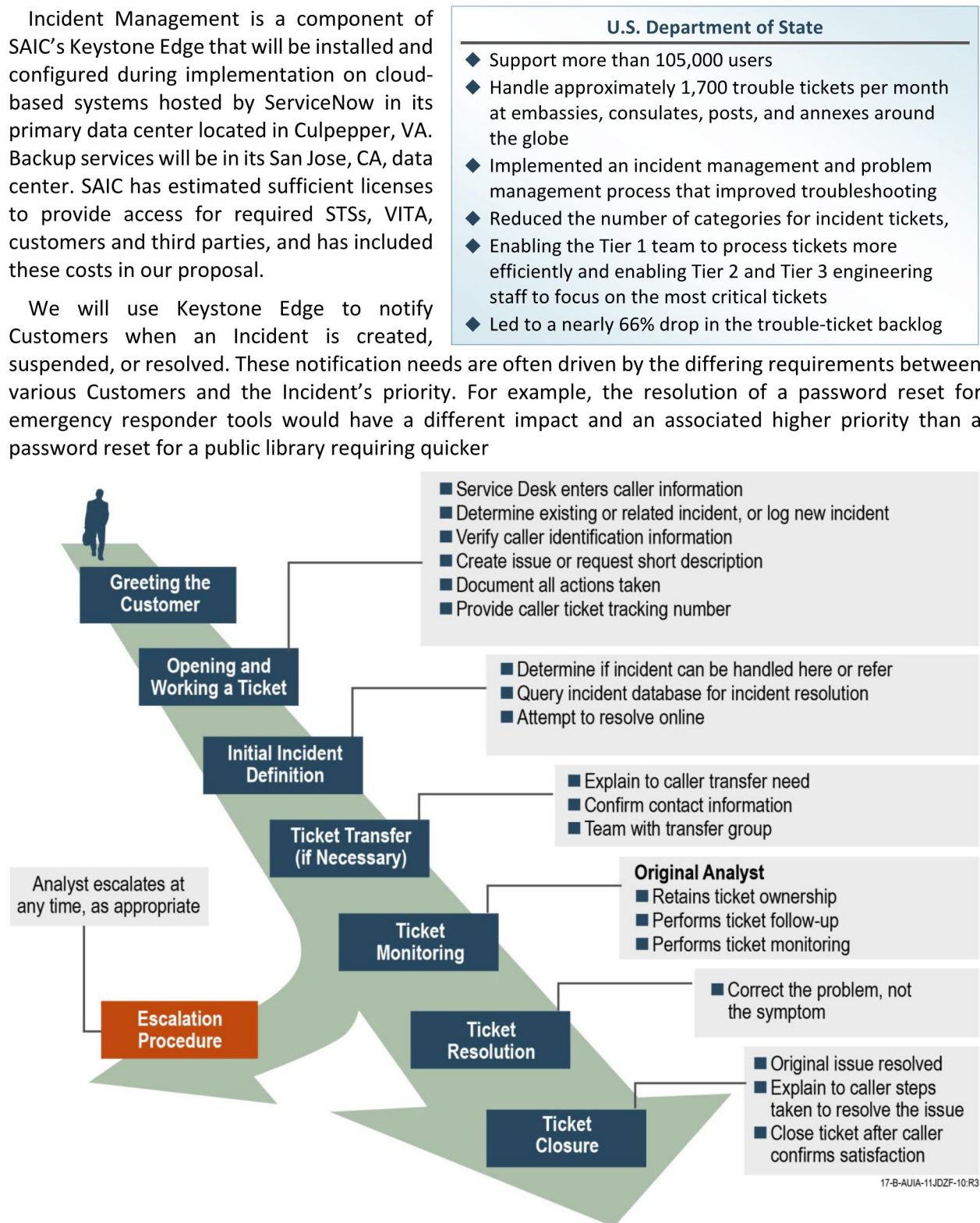◆ Led to a nearly 66% drop in the trouble-ticket backlog

Figure 6.2-1. Incident Handling Procedures

response to the request and associated notification. We have delivered these types of requirements for the City of Memphis and other clients. Additional requirements may be driven by understanding Customer-specific applications and compliance driven by local, state, and federal requirements.

Additionally, our business relations management team will identify COVA and Customer VIPs and provide any special requirements for SD activities. All notifications are part of the Keystone Edge automated workflow. The frequency of updates and notifications will be based on the severity of the Incident as listed in VITA guidelines. The system will generate email notifications for system outages on critical systems with updates on prescribed schedules. SAIC will provide optional methods of distributing notifications, such as page-outs and callouts.

SAIC will provide monthly compliance reports to VITA and Customers in the approved VITA format. These reports will be automated through Keystone Edge, including (but not limited to) the following:
◆ Number of Incidents by group, severity, service
◆ List of Incidents with details, description, reference number
◆ Links to problems and known errors
◆ Trend analysis

6.3 Event Management

Keystone Edge provides the mechanism to record, manage, correlate, and act on events gathered by supplier monitoring tools and integrated directly or through a web-services interface. SAIC will implement Keystone Edge's Event Management Module and deploy event management processes during the implementation phase. The module processes events, generates alerts, and manages alert and Incident resolution.

As described above, SAIC will use its Joint IT Operations Center to host coordination meetings and bridge-calls for event response coordination. Our solution includes a team of Incident Commanders to coordinate all actions across suppliers. Working with VITA to establish proper triggers, thresholds, and responses, Keystone Edge workflows will initiate an Incident, provide notification to critical individuals and stakeholders, and manage resources necessary to maintain IT service, thus minimizing the likelihood of a missed SLA.

6.4 Problem Management

Problem Management is a critical ITIL process designed to continually reduce the frequency and impact of Incidents in the environment leading to improved availability and utility of application services. SAIC will implement problem management through our PAL and Keystone Edge during the implementation phase and manage the end-to-end Problem Management Lifecycle across all Service Tower Suppliers. **Figure 6.4-1** provides a full description of the problem investigation life cycle.

Because Keystone Edge will be the common tool across all Service Towers, Problem Management will access the data necessary to analyze the problem and more effectively determine the root cause of an issue. SAIC's problem management process is closely coupled with our Incident and Change Management processes. The SD (and occasionally the problem management team) will initiate problem investigations based on recurrence of issues, or new issues with unknown resolutions. Our approach also systematically correlates all Incidents to identify potential defects in the environment. Once such defects are identified, problem management personnel will work with change and release management staff to correct the deficiencies in an effort to minimize the number and impact of Incidents. This information will also be provided to and used by the continual service improvement process. This combination of efforts will enable the SAIC Team to help VITA realize a more stable IT environment across all service towers. Problem Management activities will be reported as part of Service Management oversight activities in Relational Governance Forums. These reports will include details on activities related to all Problems worked during the time period and will include sharing of lessons learned. SAIC will manage the day-to-day follow up of Root Cause Analysis and execution of resultant remediation actions through direct contact with Service Tower Suppliers and through the Operational Governance Forums.

Problem Management also feeds our Continuous Process Improvement, as described in Section 7. It helps identify areas of repeat issues, unknown resolutions, and the root cause of the issue.
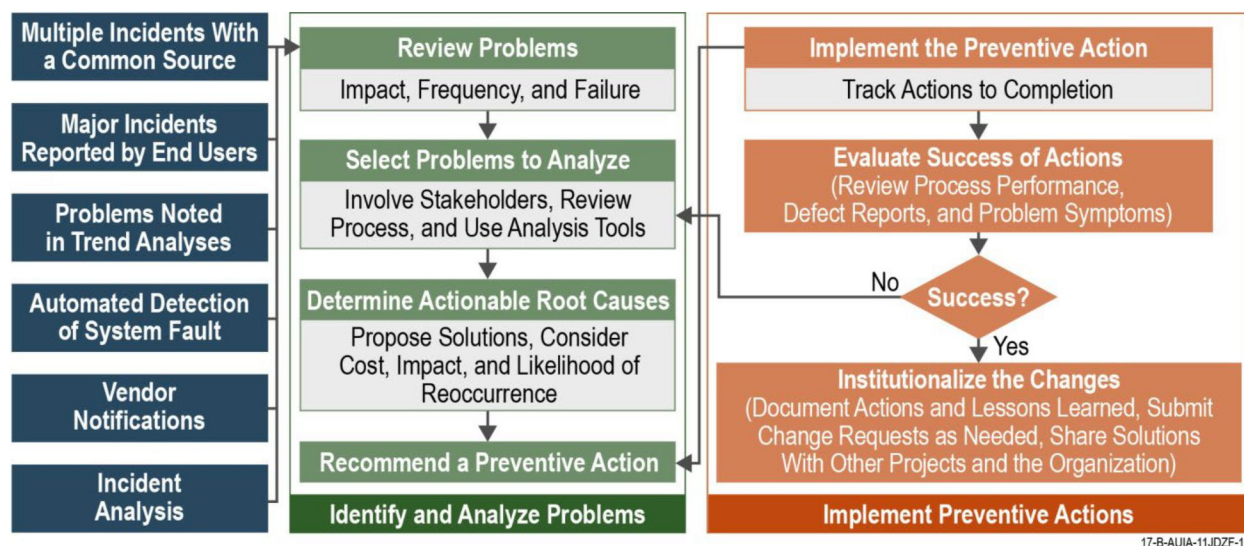

Figure 6.4-1. SAIC's Problem Management Process Implemented in Keystone Edge

6.5 Request Management and Fulfillment

Request Management includes two key categories: Service Requests and Solution Requests. Service Requests are for products and services that are defined and available via the Service Catalog. Examples include account maintenance and requests for new or replacement mobile devices. Solution Requests are requests to develop a service or product to meet a new or changed business requirement, where a design and

Alyeska Pipeline Service Company
◆ Implemented SAIC's online request system
◆ About 25% of all requests are now entered by users online through self-help portal
◆ Included complex employee on-boarding process that the client claimed *"could never be automated."*

standard service do not exist today in the Service Catalog. Both are typically initiated via the Service Desk through the web portal, chat, email, or a telephone call. Solution Requests may also be submitted via the Service Desk, through the Architecture and Design Governance Boards, and through Business Relationship Managers.

Upon initiation of a Service or Solution Request, the requestor will be provided with a tracking number for the full lifecycle of the request. Workflows allow for expedited standard changes to satisfy low-risk requests and include automated routing to the proper authority for those that

Defense Enterprise Computing Center
◆ SAIC provides 24/7/365 Service Desk
◆ 1¼ million users worldwide
◆ About 8,000 IMAC Service Requests a year

require further authorization (as defined by VITA standards). The system is also able to customize the presentation based on User affiliation, and the marketplace will offer only choices that each User is authorized to request. Service Requests that require additional input will be routed through workflow to the solution-design process.

As part of the self-service Portal, VITA and all Customers will have full visibility into the request system that provides visibility into the status of current requests and any changes to requests.

Service Requests that can be fulfilled by the Service Desk, such as account maintenance activities, are typically completed within 24 hours and in many cases will be completed at First Call with the requestor still on the phone. Service Requests that require other Service Tower Suppliers or procurement are routed to those groups, and fulfillment times are governed by the individual service SLAs. In all cases, SAIC's

Service Desk will track Service Requests, escalate those that exceed their expected thresholds for completion, and provide a single point of communication for status.

SAIC will coordinate review and action for Solution Requests with the required technical architects from each Service Tower Supplier. Reviews and design work will include validation of the requirements, review of security and compliance requirements, assessment of alternatives, and proposal of a design for review. Turn-around times vary based on the nature and scope of the Solution requested. Reviews of Solution Requests will be conducted weekly and the status will be communicated to the requestor in addition to being posted on the Portal. Customers may also provide partial or full designs from their internal IT support staff.

6.6   Access Management

SAIC has extensive experience in providing identity and access management (IAM) services to many government agencies, such as NASA, Marine Corps Enterprise Network, and Human and Health Services. We will implement a cost-effective, comprehensive, and flexible best-in-class identity management and access control service as depicted in **Figure 6.6-1**. SailPoint IdentityIQ will provide the identity and access governance capabilities coupled with CyberArk's Privileged Account Security Solution to secure, audit, and manage privileged accounts and credential vaulting (both passwords and SSH keys) using FIPS 140-2 encryption. The solution will be deployed in VITA's ITISP data centers. All User provisioning (including ability to modify, suspend, reactivate, disable, remove, monitor, review, report, and audit) will be performed in SailPoint and privileged User, account, and access data will be provided to CyberArk. These account management tasks can be performed on an individual User basis or simultaneously to a mass set of Users.
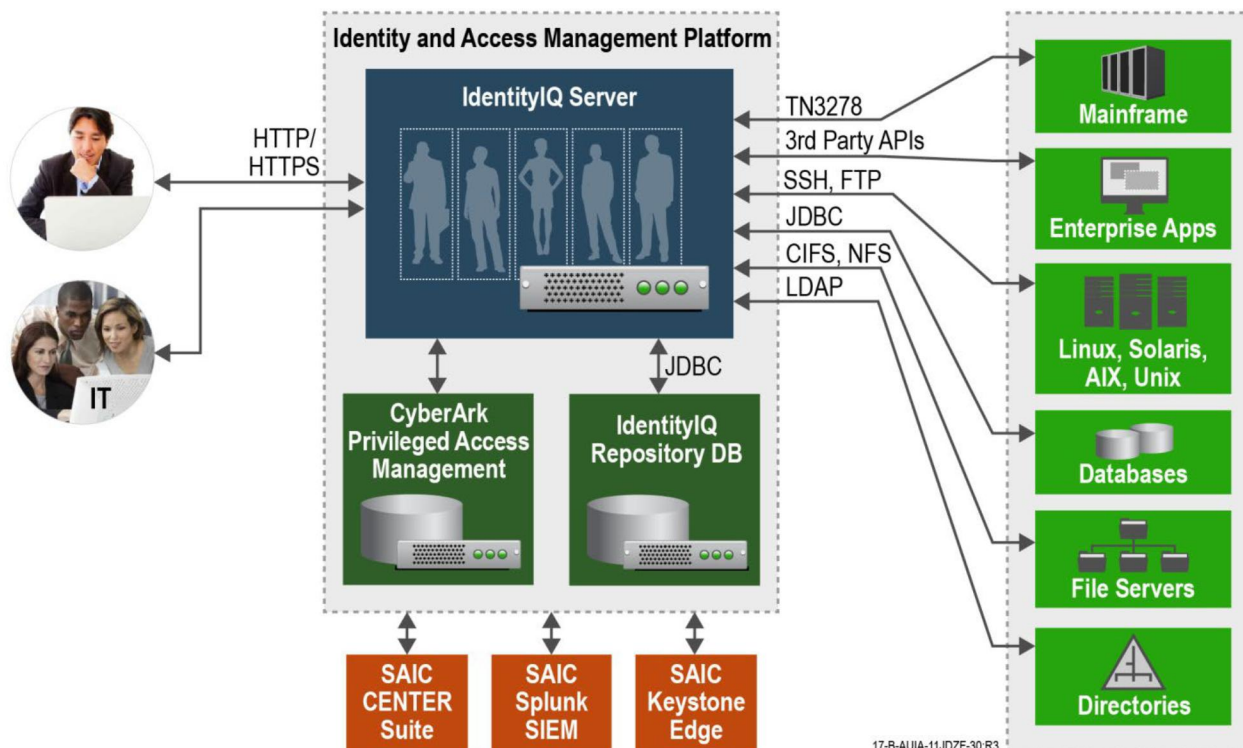

Figure 6.6-1. Identity Access Management Infrastructure Overview

SAIC will integrate SailPoint with Keystone Edge to coordinate fulfillment of User-access changes, provide visibility into the status of requests, and Service Desk Incidents. Self-service password management workflows will enable automatic handling of Tier I tasks such as change, recover, or reset

passwords through correctly answering configurable challenge-and-response questions or SMS text message code. Such password changes are automatically synchronized with target systems, eliminating the need to manually perform such changes. With these tools, the SD will handle such Tier I tasks as access change requests, adding people to groups, and locking or unlocking accounts.

The IAM team will manage privileged User accounts and escalations from Tier I. All requests for access, access rights granted, and access approval authorities will be retained as directed by VITA and its Customers. This tightly integrated solution enables SAIC to centrally view, manage with delegation, and enforce all identities (individuals and applications) and access rights; perform single- and multifactor authentication; quickly detect and mitigate suspicious, inappropriate, or unauthorized account access activity, while ensuring a User-friendly experience that addresses access policy and regulatory compliance.

Additionally, SAIC use the embedded capabilities of Sailpoint, CyberArk, and Keystone Edge to provide enhanced audit capability for all provisioned and requested accounts. Log data and change records from these systems are correlated to detect changes and inform SAIC IAM staff of anomalous changes (based on pre-established rules) via Splunk and Keystone Edge. Both our IAM staff and VITA authorized staff use the account audit function of Sailpoint and CyberArk to review account status, request, and changes, which includes a complete audit trail to include account change request, approvals, and execution via Keystone Edge reporting. Account audit intervals are established based on account type. Privilege accounts are audited monthly.

SAIC will also deploy compliance controls as part of the Sailpoint IAM solution. Compliance controls will be based on requirements as specified by VITA and Customer IT Security as well as application and data owners. Compliance controls will be used to enforce policies relating to a variety of requirements, including separation of duties for application roles and providing assurance that Users possess and maintain the appropriate security background checks and clearances required to access specified systems. Policy enforcement will include denial of access to systems and applications where a User does not possess the prerequisite access requirements or where those clearances have expired. All policy requirements and compliance with those policy requirements will be included as part of the overall controls audit reports.

SAIC will fully integrate with VITA and its Customers' existing authoritative sources of User identity information as well as designated Third Party Vendor systems approved by VITA, such as Microsoft Active Directory. Any data natively maintained by Third Party Vendor–owned identity access management platforms (e.g., Microsoft ForeFront Identity Manager) will be assessed and, as needed, a copy of the data imported to SAIC. We will connect to these identity data sources using software connectors to create a multidimensional view of each User and his or her associated access. Identity and access information will be imported from those authoritative sources (because integration with SAIC's IAM platform is not permitted). Reusing existing authoritative sources will minimize interruption during implementation. Furthermore, we will leverage various SailPoint and CyberArk software-provisioning connectors to integrate and provision IBM and Unisys mainframe technologies, network devices, UNIX, Linux, and Mac Operating System (OS) X operating systems and Third Party Vendor applications. Federated identity supporting all federal assurance levels as defined in NIST.SP.800.63 and single sign-on will be supported across on-premises and external cloud applications.

SAIC will integrate this IAM solution with VITA's Physical Access Control System to control and manage physical access to VITA and its customers' facilities by using the individual's personal identity verification card (FIPS 201–compliant) to verify whether the individual has authorized access. Physical access privileges for personnel (i.e., supplier, STS) will be removed on departure from the ITISP, in accordance to VITA rules and the SMM. In the event that a Customer uses a Physical Access Control System that does

not support an electronic integration, a process will be put in place to route change requests from the Service Desk to the Customer representative responsible for administration of that Physical Access Control System.

Using threat analytics technologies and real-time monitoring and recording of privileged sessions, our integrated SailPoint and CyberArk platform will generate alerts on potentially compromised accounts and suspicious sessions and automatically rotate the impacted credentials. Such threats, including all account identity, access and authorization activity, and system activity, will be maintained in a centralized logging service and correlated with other forms of actionable threat intelligence on the Splunk platform. The log data will be retained as part of our enterprise backup in accordance with VITA Rules and the SMM. Furthermore, this log data will supplement audit trails and forensics analysis to facilitate tracking of User accounts, access entitlements, and activity across VITA and its customers' resources. SAIC will document and review audit records to provide VITA and its customers with evidence of activities on both physical and logical IT resources. Through recurring analysis, SAIC will identify activity that did not trigger an alert, warranting the implementation of more stringent monitoring to properly safeguard VITA and its Customers' resources.

> **National Aeronautics and Space Administration (NASA) Enterprise Applications Service Technologies (EAST)**
> ◆ Provided identity management services for 118 applications
> ◆ Supported approximately 60,000 agency users across 10 NASA field centers and NASA's Washington D.C. HQ
> ◆ Led a key cybersecurity initiative with the redesign of Identity Framework 2.0
> — Improved cybersecurity capability
> — Defined business rules, business processes, and a business workflow model
> — Solution manages all identity attributes for more than 100,000 active identities that have an affiliation with NASA

6.7   Supplier IT Operations

SAIC will use the Joint IT Operations Center in collaboration with STSs to integrate monitoring tools with Keystone Edge as described in Section 6.3 Event Management. Further, as described earlier, this Joint IT Operations Center will coordinate the major IM process as needed, assisting and coordinating with STSs and Third Party Vendors.

7.0 CONTINUAL SERVICE IMPROVEMENT

The SAIC Team understands VITA's desire to present the best-quality services to Customers using a flexible marketplace of choices. To do so requires the entire suite of IT services be built with the latest applicable technology using the IT service industry's best practices for managing and maintaining those services. To provide faster and more responsive services accessing the newest technology, we invest in the most robust service delivery technology using top industry certification-based processes and a practice of continuous improvement to those services and technology. Our solution provides a well-integrated technology solution that enables and automates industry best practice processes and procedures to deliver quality services to VITA's Customers while providing excellent visibility across all aspects of service delivery. Continuous improvement is informed by analysis of current performance data, identifying optimization opportunities and enabling improvement through technology and processes.

SAIC implements the ITIL Continual Service Improvement Framework by overlaying Deming's "Plan-Do-Check-Act" quality assurance model and the ITIL seven-step Continual Service Improvement Process as depicted in **Figure 7.0-1**.

We tailor and apply ITIL V2011 and SAIC's PAL, providing ISO 20000-1:2011 (ITSM service alignment) and ISO 9001:2008–certified frameworks and processes as needed to support SMM development and implementation. The SAIC Team will integrate these with VITA's governance framework to build a cooperative CSI program. CSI efforts underway will be incorporated into our approach, including all stakeholders and suppliers across the ITISP reporting directly to VITA for their understanding and oversight.

As shown in **Figure 7.0-2**, the SAIC Team's approach offers significant benefits to COVA. We will build a culture of improvement within the organization based on

Figure 7.0-1. Continual Service Improvement Integration

Kaizen. SAIC has developed a strong Kaizen culture through our work with Toyota, where we have realized the benefits of understanding that no potential improvement is too small to be tracked and built into the system. All personnel involved with a process or service can, and are encouraged to provide recommendations for improvements of any size and type for review. All recommendations are documented, evaluated, and made visible to ITISP, VITA, and the stakeholders. If a recommendation is approved, it will be managed to implementation using standard program management tools and practices

to ensure visibility and quality completion. Such a culture will provide a foundation for always meeting VITA's business objectives and clients' needs.

Strengths of our Service Delivery and Improvement Approach	Benefit to COVA
Based on best practice industry-recognized certifications	Lower risk to VITA
Incorporates W. Edwards Deming's Plan-Do-Check-Act approach	Time tested method to reduce cost and improve service
Builds a Kaizen culture of improvement	Extends improvement benefits and participation to the full depth and breadth of the ITISP
Built on Keystone Edge and CENTER	Comprehensive industry-leading suite improves service responsiveness while reducing cost and complexity, resulting in a faster, more responsive service
Fully integrated solution	The Users will have a single pane of glass marketplace of choice experience rather than a variety of systems with different locations and means of access with STS integration built in

Figure 7.0-2. Our CSI Approve Provides Significant Benefits To VITA

In addition to the methods described above, we will also identify CSI opportunities through activities such as:

◆ Meetings that review what happened and recommend improvements
◆ Reviews of workplace, team, and individual performance
◆ Policies and procedures that allow the CSI team to systematically review and improve the quality of products, services, and procedures
◆ Comparing performance to industry benchmarks
◆ Seeking and considering feedback from all stakeholders

For the U.S. Army Program SAIC applied our continuous improvement processes and identified a significant problem with the existing on-line request system. As a result, we were able to retire a legacy outdated workflow system, replacing it with enhanced functionality using the Service Catalog. This resulted in a 60% reduction in maintenance activities as well as a reduction in time to onboard new employees from 10-days to 3-days. Additionally, ten new processes were implemented to streamline areas such as account requests, maintenance of official documentation and aircraft tracking.

7.1 Service Review and Reporting

The power of Keystone Edge as the system that provides SMS functions and workflow automation is that it is also the aggregation point for capturing STS information. It will be the single data source supporting data analytics, dashboards, Problem Management, and reporting. As described earlier, performance data from all ITIL processes will be captured and available via Keystone Edge, notably Problem and Incident data. This innovative approach provides a great level of efficiency and ensures the accuracy and timeliness of information displays and reporting while

> **USDA RMA**
>
> ◆ Improved application time to market by 1,200%
> ◆ Improved on-time/on-function delivery by 150%
> ◆ Decreased production defects by 66%
>
> The SAIC Team resolves more than 18,500 work orders annually to keep systems operational, provide for continuity of business processes, and support end users. Using USDA SDLC guidance, we maintain dozens of mission-enabling business applications and interfaces, which support $117 billion in insurance liability across 1.17 million policies.

reducing complexity and cost. With SAIC as the MSI, this data is collected from and available to all stakeholders as reports and through User interactive dashboards accessible through a web browser. Keystone

Edge is a highly efficient integrated portal that provides a flexible single point of focus for all Users and enables role-based access to data views, dashboards, and reports.

Leveraging its open interfaces to other tools in the SMS software used in the environment and by the STSs, Keystone Edge will, as part of Problem Management, keep trends, variances from targets, repeat issues, and other performance indicators for all time frames readily available for Users and managers relying on this information to inform their business decisions. It will yield real-time visibility into all service delivery processes (including CSI), provide the status, progress, and owner to allow VITA to understand the next steps for any improvement opportunity. These real-time data will support all Exhibit 3 (Reporting and Service Level Management) requirements. The Keystone Edge dashboard displays the following:

◆ SLA Status
◆ Operational Level Agreement Status
◆ Key Service Performance Measures
◆ Key Process Performance Measures
◆ Risk Analysis
◆ Key Issues
◆ Lessons Learned
◆ Opportunities for Improvement

7.2 Process Evaluation and Currency

Strong, current, and relevant processes are necessary to ensure quality services are being delivered to VITA and other Customers. As the MSI, SAIC will manage a program of process evaluation and currency to keep processes compliant, efficient, and to manage risk. All processes will have established and documented performance measures including baseline and performance expectations that will inform future CSI efforts as well as measure their effectiveness.

Process evaluation will be triggered when metrics trend negatively, repeat Incidents or Problems are identified through Problem Management, or processes fail to deliver results. Additional reviews will be triggered by the QA Plan created for the ITISP, which includes an audit schedule that prioritizes process audits by risk to the program and involving VITA and STS for review and feedback in a quarterly report. The QA Plan for process evaluation and currency also addresses process audits by:

◆ Providing a review schedule for all processes
◆ Focusing on both service results and the steps to provide service
◆ Updating processes regularly driven by ITISP needs and focusing on processes that are performing below expectations
◆ Ensuring all processes are reviewed at least annually

As described in Section 6.4, Problem Management plays a key role in identifying repeat issues, new unknown issues, and issues with significant impact to the environment. Our Problem Management process is designed to identify these areas of opportunity, drive resolution through root cause analysis, and track remediation through implementing permanent resolution and process improvements.

Whenever an opportunity for improvement is identified, an improvement plan will be documented and tracked using standard Project Management practices and tools, ensuring repeatability and transparency. All audit results and improvement efforts are tracked and reported to VITA and ITISP Governance through Keystone Edge.

All process currency efforts are managed as Projects within Keystone Edge using standard Project Management, Change Management, and SACM components. Our Keystone Edge Change Management Module manages the workflow for changes including planning, scheduling, implementation, verification, and review. It also controls approval gates, documents business benefits, maintains plans, and builds a log of all actions taken. Owners for all process documents are assigned within the SACM system, ensuring

that all have owners and any change in ownership will follow the automated change process. Reports built into Keystone Edge provide ongoing visibility into the process and status across all suppliers.

7.3 Service Measurement

SAIC defines high-quality measurement as focusing on the measures which best align with the objectives and needs of the organization, the quality of its services as viewed by the customer, and which measures reduce the overall program risk and cost. For COVA, this would include VITA and all supported Customers. Without high-quality measurement, we

U.S. Army Reserve Command
We implemented our concept of high-quality service measurement with approximately 100 actively maintained programmatic measures.

cannot determine the success or focus accurately on where, what, and how to improve. As MSI, we will implement a measurement program that provides a framework for VITA to validate that the ITISP and all its STSs perform in accordance with objectives, performance standards, and acceptable quality levels.

This measurement program will define a full suite of service measurements using the ISO maturity assessment and gap analysis done during the ITISP Implementation. These service measures will have the following characteristics relevant to CSI:

◆ Focus on VITA business needs (e.g., improving service delivery, evolve offerings, control cost)
◆ Reduce risks within ITISP
◆ Use ITIL and industry-standard measures
◆ Encompass the entire services life cycle and provide the ability to measure how well a service is serving the Customers
◆ Support all suppliers and STSs in collecting relevant information

Measures are baselined through a trial period before being established in production and coordinated with the STSs and OLAs. Once measures are established, we will conduct regular quality surveillance of the program though these measures. Modern ITSM operational and monitoring tools data will feed directly into Keystone Edge and provide capabilities for 100% inspection, analysis, reporting, and dashboard/online display.

Key metrics are analyzed against measurement targets and trends. Where targets are missed or trends indicate a negative situation, recommendations are made for correction. A Process Improvement Plan is created for each missed target. Each process improvement is managed as a change within the Keystone Edge system.

USDA RMA
SAIC designed, developed, and maintained RMA systems that process more than 1.17 million insurance policies a year.

To ensure efficient and effective service measurement, SAIC will implement a comprehensive QA program that will iteratively apply the Deming model of Plan-Do-Check-Act for continual service improvement. By planning for quality, measuring quality, monitoring and inspecting during execution, and taking corrective and preventive actions to address existing or potential issues, we achieve the level of performance required for VITA's ITISP.

A comprehensive quality program categorizes practices into three groups—quality control (QC), QA, and quality surveillance—that, along with CSI, support the complete program life. QC activities integrate into the processes and ensure the performance requirements of services being delivered; QA is independent to ensure adherence and compliance with defined policies and processes; and quality surveillance provides insight and oversight activities performed to monitor performance, deliverables, and Customer satisfaction.

While SAIC performs MSI activities, our QA manager measures, inspects, and audits services and deliverables across the program, focusing on ITISP business results. This oversight includes reliability,

speed, cost-effectiveness, security, and Customer experience and satisfaction. The QA team verifies that services are compliant with ITISP standards, delivered on schedule, and client-ready when delivered.

For any non-conforming or negative performance, regardless of detection method, we analyze the root cause. This will lead to either a Preventive or Corrective Action Plan. This quality approach is a closed-loop system that enforces a culture of continual improvement (**Figure 7.3-1**).

All SAIC's MSI QA activities will be plan–driven with full visibility into the design, documentation, implementation, and viability of activities across the ITISP. Our auditing will verify every STS's compliance with the QA program. This plan will be an integral part of the overall framework to test and validate results and determine the level of improvements. Findings will be reported monthly to VITA and other stakeholders.
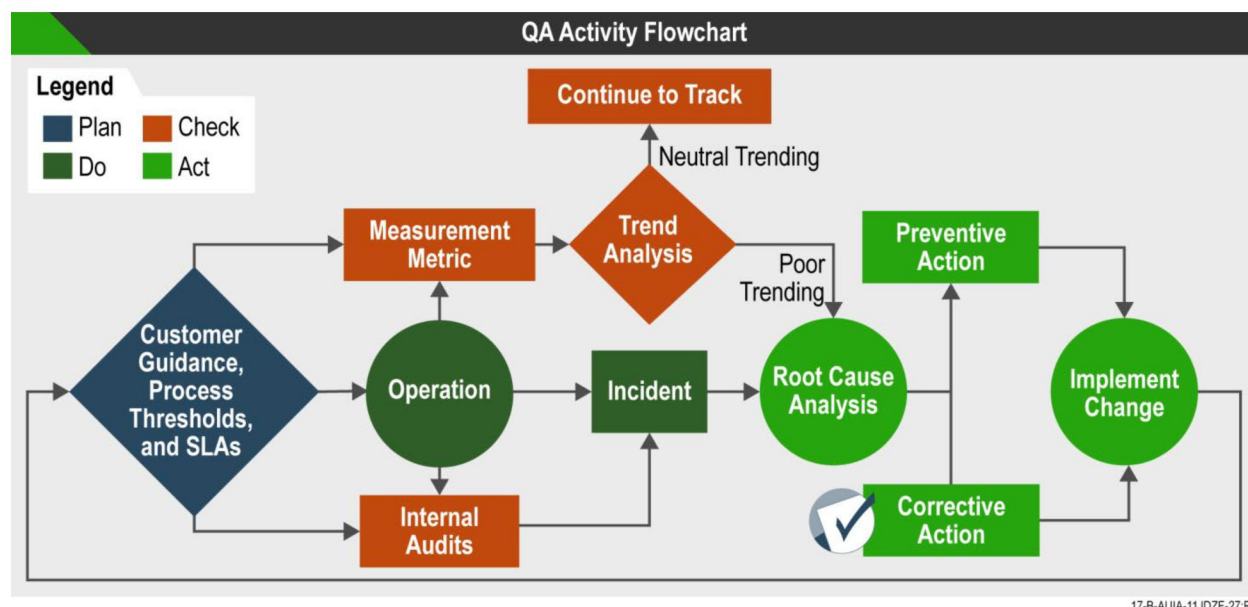

Figure 7.3-1. Our QA Activities Help Ensure That Quality Procedures Are Applied and That Quality Is Built In

7.4 Improvement Planning

Service improvement will be an ongoing effort to ensure that provided IT solutions continue to be efficient, effective, and innovative. The primary source for service improvements will be output from CSI activities including findings from Problem Management, Root Cause Analysis, trending of KPIs and analysis of data in Keystone Edge, and to address Performance Improvement Plans. Additionally, the STS, Customer, VITA, and other parties may request improvements. Regardless of the source of identification, improvements may provide access to newer technologies, reduce costs, or add to the marketplace of choices. To ensure effective implementation, improvement must start with effective planning. As the MSI, the SAIC Team works with ITISP Governance to build a joint Service Improvement Plan for all ITISP suppliers and STSs. This Plan provides a method to capture all stakeholders' input into the framework and will inform regular progress reviews. We build on the visibility provided through the Keystone Edge interface to provide framework reporting to all participants. Such reports give real-time understanding of the status and success of

> **Department of Homeland Security**
>
> For DHS, we used our United Solutions PAL innovative processes to consolidate two data centers into one. By applying our ITIL-based best practices, including CSI, we achieved significant cost savings, maintained user satisfaction, and doubled storage capacity, while reducing servers by 15%, network devices by 50%, and SANs by 50%.

all process improvement activities and assist in review and approvals that will then drive plans for future

improvements. SAIC develops and coordinates all aspects of the continual service improvement cycle across all relevant stakeholders and holds at least quarterly meetings to incorporate VITA, ITISP, and STS input.

7.5 Technical Innovation

SAIC will coordinate technical innovation across all suppliers to improve IT service quality. We leverage our expertise working across government, IT operations, IT innovation, and systems integration to lead the VITA supplier community in innovation that delivers improved services.

We will lead a comprehensive technical innovation program as illustrated in **Figure 7.5-1** and support the Service Innovation Governance Forum. As shown in the figure, multiple inputs must be considered when identifying the appropriate innovation target. These include demand management forecast and business strategies that provide insight into future technology needs. Current delivery performance may identify areas with opportunities for improvement. The Technology Plan and service strategy inform whether service needs should be fulfilled through an application of innovative technology.

SAIC will support VITA in leading a culture of collaboration among suppliers to support process improvement and technology inno-vation. This leadership role will be enabled by our expertise and over-all MSI approach. SAIC will drive the biannual supplier improvement sessions to deliver technical innovation recommendations designed to serve the needs of the Customers and informed by our technology expertise to validate and coordinate the recommendations of the STSs.

Figure 7.5-1. Technical Innovation Process

Keystone Edge, as the system of record for all data on service performance and assets, provides key input to our innovative approach. In addition, all technical innovation Projects will be tracked and coordinated through the Project Portfolio Management module of Keystone Edge.

As a leading technology integrator having provided full life-cycle services and solutions to the government for over four decades, SAIC is in an excellent position to guide this process. We maintain a robust investment program in internal research and development, including areas focused on core MSI service areas: IT Service Management and cybersecurity. Additionally, we research significant, key areas relevant to the overall environment, such as data center automation, cloud computing, software-defined networking, virtual desktop, mobile application development, enterprise agile application development, and big data. Our research programs, coupled with our real-world experience supporting multiple large clients, gives us the organizational capability to drive effective innovation for VITA.

7.6 Technical Currency

Technical currency is a function of evaluating vendor release cycles and technology trends to avoid technological obsolescence and security and operational risks. SAIC will coordinate the creation and maintenance of the integrated Refresh and Currency Plan, and oversee the execution of refresh and software currency Projects.

> **County of Orange**
>
> We recommended and implemented Solid-State SAN providing better performance and lower total cost of ownership than the solution that incrementally expanded the existing SAN to meet the demand management forecasts for the County's Enterprise Resource Planning (ERP) system.

Figure 7.6-1 shows several key inputs for the technical currency process. These inputs are available in Keystone Edge and include asset inventory information (including Third Party Vendor end-of-support dates), Capacity Management, Availability Management, Service Level management, and event management.

SAIC goes beyond the basics of planning and overseeing refresh Projects to maintain service performance and avoid support issues. We leverage our technical expertise and background when creating the VITA Technology Plan to ensure technical currency is maintained in the most cost-effective manner that meets the business functions. In fulfilling the MSI role, we will validate the choice between a simple technology refresh versus a new technology option. These recommendations will be documented in the Refresh and Currency Plan.

Figure 7.6-1. Technical Currency Process

SAIC is experienced with the large portfolio of refresh Projects that a customer of VITA's size and scope must manage, and has done so for many clients including the DOS on the Vanguard contract, USDA RMA, and U.S. Army Reserve, as discussed in Appendix B. We use standard Project tools and approaches described in Section 2 to manage these efforts. Through our Solution Design (see section 4.1) and Change Evaluation (see section 5.2) efforts, we will also oversee the integration of supplier technical currency activities to maintain the availability of the services and avoid implementation conflicts.

7.7 Cloud Broker for SAAS, IAAS, and PAAS

With the continued evolution of computing practices, integrated hosting decisions must be made, matching requirements with the rapidly evolving capabilities of the available environments, both in the cloud and on premises. SAIC will incorporate Cloud Broker Integration (CBI) into our overall MSI services to reduce redundancy and streamline workflows in measurable and repeatable ways. CBI and MSI integration points are detailed in **Figure 7.7-1**. SAIC will provide CBI services to fulfill industry standard (NIST and Gartner)–defined functions: service intermediation, service aggregation, service arbitrage, integration, and customization will provide VITA and the Commonwealth a flexible and adaptable path to cloud computing. Our approach incorporates our leading technology, experienced team, and proven methodologies to facilitate the integration and comprehensive management of multivendor cloud services that provide choice, access to the latest technologies, and cost optimization. SAIC will design and provide a marketplace of choices for cloud services that is centrally managed in Keystone Edge and can easily evolve when offerings and needs change. The marketplace will allow solutions to be indexed and selected by key attributes using rules-based configurations. Where practical, SAIC will provide multiple cloud alternatives while maintaining consistent enterprise standards.

MSI Function	CBI Integration
Business Relationship Management	CBI will leverage BRM processes to initiate cloud solutions. Advise customers about the best solutions based on understanding the business requirements and potential solutions. We will provide budgeting guidance, and procure and manage multiple cloud services.
Program Management	CBI will support the needs of ongoing VITA programs and track user demand to develop new cloud capabilities, migrate workloads to the cloud via Cloud Migration Edge, and provide lowest cost alternatives for application hosting.
GRC	GRC will control the CBI operations within the context of the overall program and MSI contract. CBI will support and accommodate the needs of the various regulatory and compliance needs while providing access to cloud-based resources. GRC will also establish, rationalize, and implement cloud policy and standards.
Service Desk	CBI processes will be integrated with standard ITIL practices for request, incident, problem, change, release, and service-level monitoring. As new hosting options are introduced, CBI will ensure that the standard ITIL practices will not be impacted and new service types or categories are added to the service catalog.
App Tower	CBI operations will complement the VITA application SDLC process. As VITA cloud capabilities are enhanced, DevOps and DevSecOps capabilities will be introduced to improve application environment provisioning, automate testing, and improve security compliance.
Security Tower	In conjunction with the GRC processes, CBI will enable consistent security operations regardless of the data center or Cloud Service Provider (CSP), including IAM, data content security, and encryption.
Server & Storage Tower	CBI has the potential to provide enterprise-wide benefits for standardizing hosting services through a common tool set that is hybrid cloud-capable. To the extent that the server and storage towers are managed as "private cloud" providers, they will be integrated with the CBI processes for consistency.
Cloud Solution Providers	Popular CSPs (e.g., AWS, Azure) will easily be added into CBI and Service Desk processes due to their ease of integration (e.g., REST APIs), high levels of automation and provisioning, compatibility with our technology suite, and robust monitoring and reporting capabilities.
Monitoring	All CBI solutions will be monitored and integrated with enterprise event management and security incident tools and processes.

Figure 7.7-1. CBI and MSI Integration Points

SAIC's approach is based on our proven life cycle methodology—*Cloud Migration Edge*^{TM} *(CME)*. CME is built on SAIC's decades of engineering experience applied to cloud computing technologies. Based on the ITIL life cycle and our United Solutions best practices, Cloud Migration Edge will be tailored to include VITA's system design life cycle (SDLC) gates and artifacts. The methodology details the cloud migration process into standardized, repeatable steps that identify technology components and enables the use of standard configurations to address specific requirements without having to reinvent solutions for each project. SAIC has formalized a cloud computing knowledge base and has built tools supporting systematic collaborative evolution that applies each new experience to an improvement in the methodology and work products.

By design, CME achieves IT cloud service management through a phased adoption, based on five repeatable processes: Phase 1 - Strategy and Assessment, Phase 2 – Design, Phase 3 – Transition, Phase 4 – Operations, and Phase 5 – Improvement. CME enables us to tailor application migration to any cloud deployment model based on the scope of the engagement, integration with current efforts and customer needs to effectively modulate transition, and reduce risks and costs.

To implement CME, we use our extensive library of templates, and processes as accelerators for cloud adoption and application migrations. CME tools, example artifacts, and technical information support the

development of cloud-enabled architectures and associated engineering and management work products. These are a culmination of real-world project experience, coordination with SAIC business alliance partnerships, and continuous improvement from internal research and development campaigns to adapt to evolving industry IT business demand changes and needs. Technologies are tried and tested in the SAIC Enterprise Services Laboratory to validate functionality and determine feasibility of solutions. A library of configuration models and design documents are available for internal and external use that address support for overall reference architectures for common cloud solutions, such as software-defined data center, software-defined data network, virtual desktop infrastructure, and using automation and orchestration from a "single pane of glass." SAIC and our partners have used CME and the proposed toolsets for multiple federal agencies, including USDA, RMA, and MCEITS.

SAIC will assess the current state of maturity, establish a baseline capability, and build maturity through continual service improvement (CSI). SAIC will research various industry solutions that best meet COVA requirements, leveraging our relationships with industry-leading cloud providers such as Amazon

Cloud Broker Integration Benefits
◆ Integration with Keystone Edge
◆ Integration with hyper-scaler CSPs (e.g., AWS, Azure)
◆ Integration with converged infrastructure providers (e.g., Dell/EMC, Cisco)
◆ Integration with multiple hypervisors (e.g., VMWare, RHEV, Hyper-V)
◆ Integration with multiple storage providers (e.g., EMC, NetApp)
◆ Integration with other technology providers (e.g., F5, Infoblox)
◆ Compatibility with OpenStack
◆ Robust set of APIs and plug-ins
◆ Robust business management suite for cost optimization and billing
◆ Compatibility with existing data center infrastructure

and Microsoft, and leading technology providers that enable hybrid cloud evolution, such as VMWare, Red Hat, EMC, NetApp, and Cisco. SAIC CBI will add value to public and private cloud services on behalf of VITA customers to foster reuse and provide more tailored and enhanced enterprise capabilities.

SAIC will provide CBI–enabling tools to deliver faster, more responsive service. Our Keystone Edge integrated toolset, including the vRealize suite and DigitalFuel for financial management, will enable us to deliver predefined services across both public and private cloud providers, as shown in **Figure 7.7-2**.

SAIC CBI operations will provide cloud broker and administration resources; manage the use, performance, and delivery of cloud services; and facilitate upgrades and enhancements to support innovation and currency strategies. In addition, SAIC will blend CBI into the overall functions of the MSI to reduce redundancy and streamline workflows that are both measurable and repeatable, as highlighted in **Figure 7-7.2**
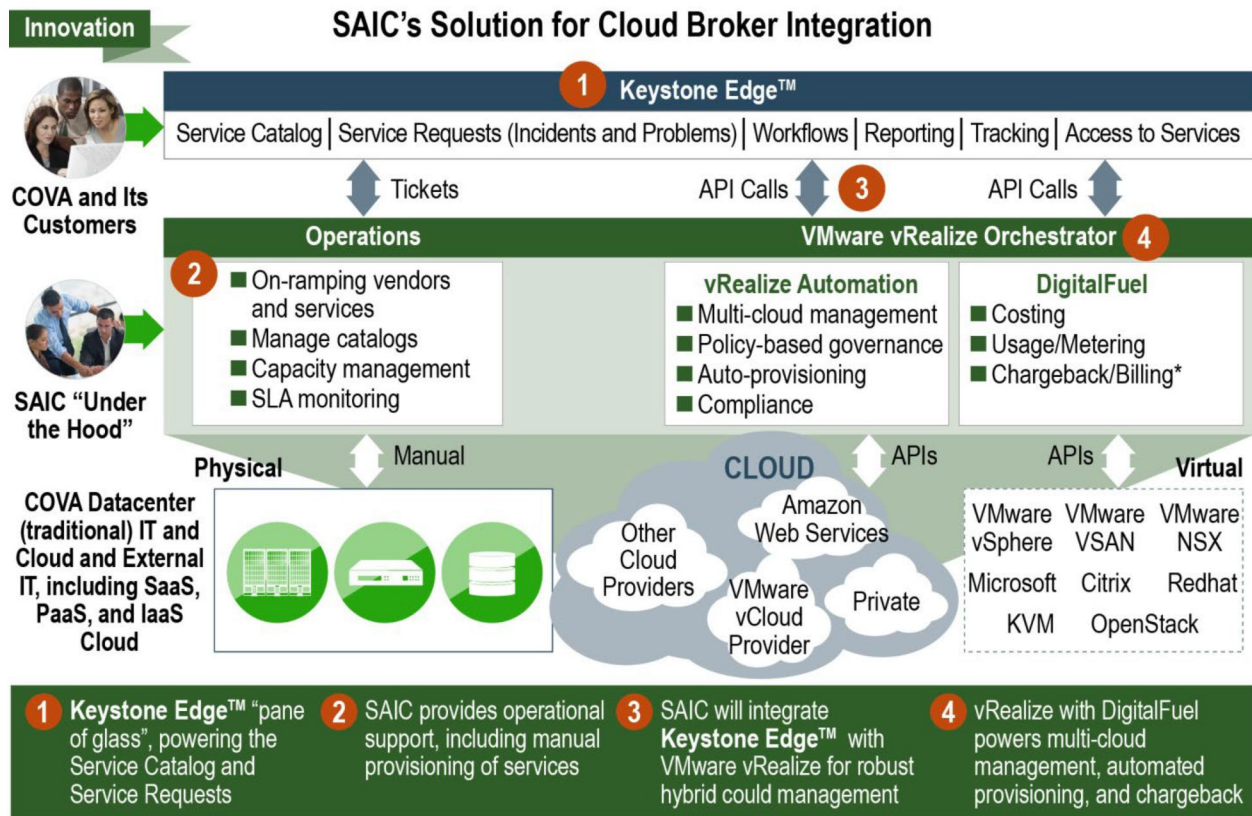
Figure 7.7-2. Cloud Broker Integration Tools and Processes

SAIC will manage cloud migrations via its Cloud Migration Edge process framework that is ITIL based and would be initiated through standard MSI processes for requests and projects, and governed through the Program office. Size, scope, complexity and analysis of alternatives will be considered on an application-by-application basis, as well as a review of currently available alternatives. If no acceptable solution currently exists, then those capabilities would need to be developed through a standard project effort.

Introduction of Cloud Services into the ITISP

As the Cloud Broker for VITA, SAIC will manage and maintain the catalog of VITA-approved cloud service offerings. These services include maintenance, administration, continual improvement, and when appropriate and approved, retirement of cloud services offered through the catalog. Our services also include the introduction of new cloud services into the catalog following our phased Cloud Migration Edge process framework.

Strategy and Assessment

New Cloud Services will be initiated through one of two paths: either via request from customers in the form of a Request for Solution, or through the proposal of a Service Tower Supplier for a service they believe would provide value to the Commonwealth. In both cases, the request or proposal will be routed to SAIC's Architecture group. The Architecture group will work with the originator to ensure that all requirements are captured, and a business case supporting the new service has been completed.

A critical aspect of business case development is the identification of the preferred contractual relationship with individual Cloud Service Providers (CSP). For any given cloud service, VITA may choose

to establish a contract directly with the CSP, or it may request that SAIC establish and administer a contract with the CSP on VITA's behalf. SAIC's solution fully supports both forms of contractual relationship:

◆ **VITA contracts directly with the CSP**: SAIC will identify and document within the business case any requirements for integration and authority delegation to be included within the contracts that VITA establishes.

◆ **SAIC contracts with the CSP**: SAIC will verify and document within the business case its capabilities for direct contract with the CSP, and any requirements for integration and authority delegation to be included within those contracts.

The business case and requirements will be submitted for VITA approval prior to chartering the design phase of the new service project.

Design

Upon VITA approval of the business case, the technical, service and business design of the new service will commence. During this phase, the SAIC architecture team will coordinate STS and external resources as required to develop a technical architecture and Service Design Package (SDP) compliant with Commonwealth standards and IT Security Requirements. The SDP will also include evaluation and recommendation for additional components required to meet service requirements to include, at VITA's discretion, monitoring services, service desk support, automated provisioning, billing integration, and integration with other ITISP services. The SDP will document the service components required, and the entity (e.g. SAIC, the CSP, an existing STS, or VITA) responsible for performing each component.

Based on this design, SAIC will develop and document within the SDP, a Resource Unit (RU) definition that details the ongoing billing metrics and costs for the service, and where applicable, and one-time fees associated with the stand-up of the new service. The technical architecture will be presented for approval to the VITA Architecture and Security Groups. Following technical approval, the final SDP will be presented to VITA and the originating customer for approval to initiate Service Transition.

Transition

Service Transition for new Cloud Services will follow the standard SMM process for Change and Release Management. This phase of the project includes:

◆ Training and support processes for the Service Desk and other support groups;
◆ Inclusion of contact, escalation, routing, SLA, and other performance management data, if applicable, within Keystone Edge;
◆ Communication to the user community about the new service, along with any applicable training materials or instructions;
◆ Technical integrations between the new service and the CBI system;
◆ Any additional training, staffing, or technical integration work as defined in the Service Design Package;
◆ Any data migration required as part of a service implementation (for migration projects);
◆ Inclusion of the new Service in the Service Catalog for Authorized Users;
◆ Acceptance Testing and Validation of the new Service.

Operations

Once the new Cloud Service has been accepted, it will fall under day-to-day service delivery and operational support. This includes ordering via the Service Catalog along with support options as defined in the SDP and as part of the Resource Unit. Each Cloud Service will include a complete description of what is included along with the pricing and any pricing options within the Service Catalog.

Continual Improvement

All Services, including Cloud as well as premises-based solutions provided by STSs, will be included in the overall Continual Service Improvement program outline in Exhibit 2.3.1 Section 7. Metrics will be collected on each Cloud service based on the requirements defined within the VITA-approved SDP for that service. This information, along with industry trends and experience from across the ITISP and SAIC's general experience base, will be used to formulate assessments and recommendations for the ongoing improvement of services to meet performance requirements and emerging requirements as business use and needs change over time. CSI improvement recommendations will be included in the overall ITISP CSI register and prioritized based on value to the customer and business outcomes.

8.0 ESIGNATURE MANAGEMENT

The eSignature and Digital Transaction Management platform will be used for providing the capability to support digital signatures and certificates from multiple certificate authorities. The MSI will work with the DocuSign Vendor to create an account for the Commonwealth of Virginia within the eSignature Cloud based infrastructure. The MSI will establish a parent account and configure it to manage multiple child accounts within the organization's container defined by the vendor. Role based accounts will also be created by the MSI to allow certain users permissions to manage user memberships, access controls, and other administration tasks. The MSI will also work with the DocuSign Vendor to establish integrations with the MSI authentication/account management tools to allow only authorized access to the eSignature environment. The MSI will also define notification, regional, retention and security settings. The MSI will also provide ongoing direct agency and user support & issue resolution for Software as a Service solution.

This Service Design Package describes the environment associated with the Multi-Sourcing Service Integrator's (MSI) MSI eSignature and Digital Transaction Management Solution. The MSI eSignature and Digital Transaction Management service consists of core systems and processes to enable service management, delivery, and operations.

The eSignature and Digital Transaction Management service is a platform for providing the capability to support digital signatures and support digital certificates from multiple certificate authorities. The Service enables users to be able to sign using a digital certificate in the cloud without having to download to a local machine. Accessible through both the web and mobile applications, the service can send the documents to multiple recipients simultaneously with the capability of tracking each, and controlling who can see certain documents within a package. Reporting capabilities for tracking progress of transactions and analytics are available to end users.

The MSI will deliver a platform for performing eSignature and Digital Transaction Management to support digital signature and digital document transactions.

DocuSign lets agencies prepare agreements using existing document types like Microsoft Word, Excel, PowerPoint and PDF. Flexible workflow capabilities let them share agreements with designated people in a specific order and define roles for each recipient, automating the process. Multiple levels of authentication increase the thresholds required of signers to prove their identity before given access to documents. Automated email reminders are set up for signers to complete the signing process and add deadline notifications to expire untouched documents or transactions.

Authorized Users will be assigned an account that will allow them to access the parent Agency's account. External Recipients signing a document do not consume an account. Permissions for external users is set by the sender or administrator assigned to the Tenant account. DocuSign ensures the enforceability and non-repudiation of our customers' documents.

- AES 256-bit encryption at the application level for customer documents to ensure confidentiality
- Access and transfer of data to/from DocuSign via HTTPS
- Use of Security Assertion Markup Language (SAML)
- Signers to authenticate when they sign
- Certificates of completion after all parties have participated in the signing process
- Signature verification and unalterable capture of signing parties' names, emails, public IP addresses, signing events, timestamps, signing location and completion status
- A digital audit trail for every envelope that captures the name, email address, authentication method, public IP address, envelope action, and timestamp

DocuSign does not currently allow exporting of log data to a SEIM so that functionality is not included in this service or pricing.

The Customer will provide all applicable licenses, install and configure any client desktop components of the application.

9.0 LOW CODE APPLICATION PLATFORM SAAS FOR DSS

The Low Code Application Platform (LCAP) SaaS will be used by DSS to rapidly build and deploy custom web and mobile applocations with limited need for custom coding. The MSI will work with the LCAP provider, Salesforce, to provision licenses as needed. Multiple licensing types will be provided. The MSI will setup, configure, and implement any required authentication structures and any security policies. MSI will ensure complete integration with Okta and Splunk (SIEM). MSI will mirror the below architecture to ensure a successful deployment.

Authorized users (DSS) will be provided a framework for developing dynamic web apps for mobile and desktop devices. Solution will meet the following requirements:

- Low Code: Ability to rapidly build and deploy custom web and mobile applications with limited need for custom coding

- Model Driven Development: Capability to use graphical models to define application data models, business logic and user interfaces.

- Reusability: Capability to promote reusability via an app store populated with out of the box templates, modular components, connectors, etc.

- Cloud Native: Support cloud native deployment – allowing for automated deployments and scaling, without needing to manage the complexities of underlying infrastructure.

- Integrations: Integration with enterprise identity directory and other required platforms for governance and security.

- Deployment workflows: Orchestration of pages, business processes and business rules

10.0 EVA KEYSTONE EDGE INTEGRATION

Integrate ServiceNow into the Customer's existing electronic procurement system (eVA)

Technical Approach:

Integrate ServiceNow into the eVA system. The MSI's instance of ServiceNow is referred to as Keystone Edge (KSE).

Initial Build Out:

Integrate the eVA system using the custom method process in the SAIC MSI Keystone Edge Integration document. KSE target environments are only Dev, Test and Production.

Develop a new bifurcated workflow to replace the primary and secondary workflows currently within KeyStone Edge. This workflow will integrate with the eVA punch-out for all items that present with a cost. Workflow in eVA punchout can push up to fifteen (15) attributes from ServiceNow to eVA via cXML integration for the "priced" catalog item. One (1) URL routing to a page designed to display the ServiceNow "priced" catalog. Stand up of Integration Hub pro to enable connection between Key Stone Edge and iValua. One cXML integration that allows iValua to send one (1) update to ServiceNow per request specifying "approve" or "reject".

This will allow for configurations and approvals to now take place within eVA and then be ingested back Into KeyStone Edge to follow the current provisioning workflow. Ensure that existing key features within the current workflow are evaluated and included if necessary to provide the existing functionality.

Ongoing Maintenance:

• Catalog Maintenance – MSI will update on an as needed basis to ensure catalog updates are properly displayed in KSE and eVA

• Workflow Maintenance - Maintain newly created workflow covering tasks for requests through fulfillment. Maintenance will include any updates to the workflow to include testing.

• Upgrade Maintenance – Ensure upgrades to KSE and/or eVA do not impact the customers' ability to submit requests through fulfillment.