LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TH-667440

Brahman

D. B. Campbell

February 17, 2015

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

Brahman

System Requirements Review

D. Campbell

1/30/2015

The Module Assignment from Fundamentals of Systems Engineering (SYS 625), a course offered by Stevens Institute of Technology through Lawrence Livermore National Laboratory, 2014.

Contents

Figures and Tables

Acronyms & Identification Numbers

AIM	Adversary & Interdiction Methods
AP	Assessment Plan
C#	Numbered System Constraint
D#	Numbered System Driver
E#	Numbered Sacred Stakeholder Expectation
FAA	Federal Aviation Administration
FFRDC	Federally Funded Research and Development Center
DFO	Director of Field Operations
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	Department of Transportation
DP	Deployment Plan
GS	Global Security
IT	Information Technology
LLNL	Lawrence Livermore National Laboratory
MS	MicroSoft
OC	Operations Coordinator
OL	Operation Lead
PI	Principal Investigator
R#	Numbered System Requirement
RCS	Refined Current Solution
S#	Numbered Scenario
SDBV	Syncplicity + Database + VBA
SDFV	Syncplicity + Data File + VBA
SL	Silverlight
SP	MicroSoft SharePoint
VBA	Visual Basic for Applications

Executive Summary

The Adversary & Interdiction Methods (AIM) program provides training and capability assessment services to government agencies around the country. Interdisciplinary teams equipped with gear and radioactive sources are repeatedly fielded to offsite events to collaborate with law enforcement agencies at all levels of government. AIM has grown rapidly over the past three years. A knowledge management system as evolved along with the program but it has failed to keep pace. A new system is needed.

The new system must comply with cybersecurity and information technology solutions already in place at an institutional level. The offsite nature of AIM activities must also be accommodated. Cost and schedule preclude the commissioning of new software and the procurement of expensive hardware. The new system must exploit in-house capabilities and be established quickly.

A novel system is proposed. This solution centers on a recently introduced institutional file sharing capability called Syncplicity. AIM-authored software will be combined with a dedicated institutional account to vastly extend the capability of this resource. The new knowledge management system will reduce error and increase efficiency through automation and be accessible offsite via mobile devices.

Mission Description

Background

The Adversary & Interdiction Methods program is composed of projects and programs focused on applying and evaluating tools and tactics associated with nuclear terrorism. As the name indicates, AIM addresses this issue from both the perspective of an adversary and the perspective of those tasked with interdiction. An emphasis is placed on application and fieldwork over theory and modeling. AIM is one of many similarly-focused efforts organized under N Program of Lawrence Livermore National Laboratory's (LLNL) Global Security (GS) directorate.

In simple terms, AIM is a service provider for its federal sponsors. The typical unit of service is called a deployment, usually consisting of support to a law enforcement training event. These events come in many varieties but typically last a few days to a week. Theoretically deployments could occur anywhere in the world, but historically events have been limited to the United States and its territories.

Each deployment could be viewed as a product with an associated lifecycle. Notification of a new deployment begins a planning phase which transitions into execution and culminates in an after action assessment. While the operational model is straightforward, each deployment can be complicated and involves the movement of personnel, equipment and radioactive sources. Additionally, the operational tempo is high and frequently new events are added with minimal prior notice. For reference, AIM conducted 42 deployments during the fiscal year 2014, including a deployment which occurred one week after initial sponsor notification. AIM maintains multiple teams and simultaneous deployments occur regularly.

AIM faces real coordination and logistics challenges due to the complexity of deployments and an elevated operational tempo. A patchwork system of problem-specific solutions has evolved over time as the program grew. For example, AIM established a MicroSoft (MS) SharePoint (SP) site for event scheduling and managing electronic files. While SharePoint adequately addresses file management, its calendar features are lacking and its compatibility with LLNL mobile devices leaves much to be desired. Efforts to extend SP capabilities to include automatic form generation and simple radioactive decay calculations have been scrapped. Instead of a central tool with an official record of transactions SP has become a disappointing planetoid with an expanding collection of Excel spreadsheets acting as orbiting moons. Information passed between each of these solutions is usually performed manually, a time consuming and error-prone process.

AIM will continue growing during fiscal 2015. The program will add three new staff members, purchase more equipment and operate at a higher tempo. The current suite of management tools is poorly equipped to meet current needs, let alone future demand. A new solution is desired, a single omnipresent solution audaciously dubbed Brahman. At a minimum, the new solution should:

- Provide a single official record of all AIM deployments;
- Provide inventory accounting;
- Automatically generate needed documents reflecting the official record;
- Perform needed radiation decay calculations;
- Allow context-driven knowledge management;
- Provide statistical breakdowns of operations for management and reporting;
- Be compatible with LLNL-supported mobile devices;
- Be compatible with LLNL Information Technology (IT) security requirements;
- Be adaptable and extensible;
- Be affordable and implementable with current resources.

The set of desired features listed above is not unique to AIM. One could argue that industry has confronted and solved these issues repeatedly over the last decade. The logical conclusion to this train of thought is a simple question. Why not use a commercial solution? The answer is organizational relevance. AIM is a small member ($6M annual) of a much larger organization: LLNL ($1.5B annual). Enterprise level solutions are tailored to the perceived needs of LLNL, not the specialized needs of AIM. As a result, the playing field for AIM is set by the institution; solutions must be found within the confines of LLNL connectivity and security restrictions.

Stakeholders and Expectations

The list of stakeholders for the Brahman project is diverse, driven by a complex operating environment and the use and transport of radioactive material. Stakeholders are depicted graphically in Figure 1 and are categorized as follows:

AIM

AIM personnel will be key stakeholders in the Brahman system. They will be the only users for the system and the only active stakeholders. Several named positions with administrative responsibilities exist. The organizational structure and associated responsibilities are detailed in a following section. While some system capabilities will be uniformly relevant, each AIM position will have a set of custom needs and tailored features.

Regulators

AIM exists in a quasi-government business space. LLNL is a federally funded research and development center (FFRDC). FFRDC's exist to meet a "special long-term research or development need which cannot be met as effectively by existing in-house or contractor resources."[1] The Department of Energy (DOE) is the sponsoring agency for LLNL. However, AIM is primarily funded by the Department of Homeland Security through a system called "work for other." In spite of the link to government, LLNL employees are contractors, not federal employees. This nuance must be considered for regulated activities such as transporting radioactive material, a realm where the Department of Transportation (DOT) and organizations such as the International Air Transport Association (IATA) hold sway.

Information Technology

Brahman will be an information technology solution. As a result, relevant IT organizations will be key stakeholders. Vendors and LLNL organizations, namely cyber security and connectivity (cell phone) groups, could shift policy with little to no regard for the ramifications of a small-scale IT solution. To avoid this scenario Brahman should hew closely to core institutional capabilities less likely to be lost or changed.

Management

The AIM management chain will undoubtedly be a stakeholder. As always, new or modified requirements will promulgate down the organizational structure. N Program management resides in closest proximity to AIM and will ultimately dictate the details of new institutional obligations. For example, N Program management could elect to prohibit the use of mobile devices for cost-cutting purposes. Brahman will need to be adaptable in order for AIM to remain compliant without creating new systems.

Vendors

LLNL employs a backbone of commercially available products to address its IT needs. AIM is required to exploit this technology stack to solve program-specific needs. Features, compatibility and interoperability will be an ongoing concern as hardware and software vendors modify their products. Syncplicity, Apple and MicroSoft will be key stakeholders due to their critical roles in LLNL's current IT strategy.

Shippers

AIM utilizes a collection of organizations to ship and recover its equipment and radioactive material. This is a mission-critical capability. Brahman will facilitate management and coordination of logistical

[1] 48 CFR 35.017 – Federally Funded Research and Development Centers.

efforts but will not directly interface with shipping service providers. As a result, shipping stakeholders are important but not categorized as key.

Customers

AIM customers drive mission needs and operational tempo and are hence listed as stakeholders. AIM works with scores of separate agencies at all levels of government. Specific examples will not be discussed in detail. Broad categorizations are shown in Figure 1 for illustrative purposes.

Sponsors

AIM sponsors provide funding and mission scope, dictating deliverables and prioritizing resource allocation. DHS is a principal sponsor and could easily prohibit funding of a capability deemed unnecessary or inefficient.

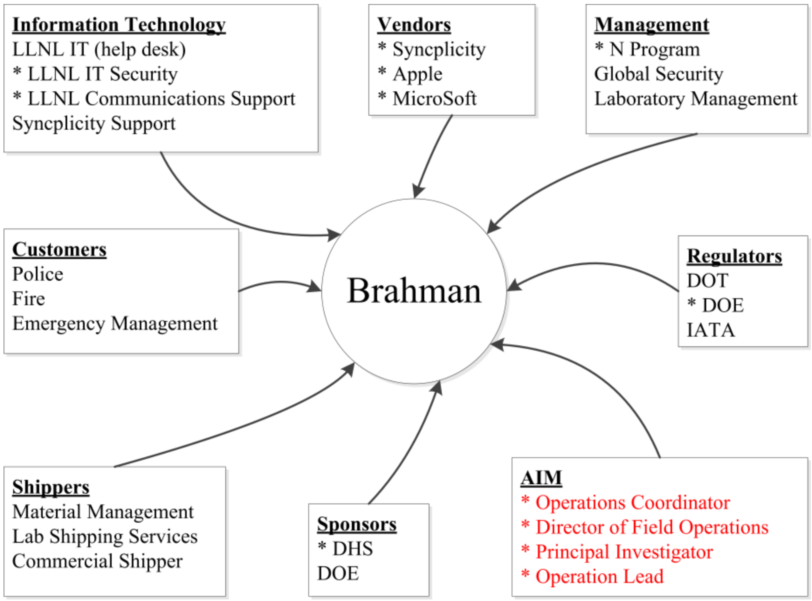

Figure 1: Stakeholder Diagram: A map of the stakeholders relevant for the Brahman project. Key stakeholders are identified with an asterisk while active stakeholders are shown in red. Some entities, such as DOE, are shown in more than one location to reflect multiple roles.

The ultimate success or failure of the Brahman project rides on meeting stakeholder expectations. As indicated above, numerous stakeholders exist. These organizations or individuals are categorized into two groups: active and passive. Active stakeholders will interact directly with the Brahman system while passive stakeholders will not. Additionally, certain stakeholders will have a disproportionate role in determining the success or failure of the system. These stakeholders are identified as “key.” A list of stakeholders and related attributes is provided in Table 1.

Stakeholder	Key	Active	Category	Role
Operations Coordinator	Y	Y	AIM	To coordinate AIM deployments; track gear and sources.
Dir. of Field Operations	Y	Y	AIM	To author AIM deployment procedures; manage field operators.
Principal Investigator	Y	Y	AIM	To sustain AIM funding and grow the program.
Operation Lead	Y	Y	AIM	One dedicated for each AIM deployment.
DHS	Y	N	Sponsor	Sponsor of AIM services (DHS regulations only applicable here).
DOE	Y	N	Regulators	Regulates LLNL operations on and off site.

Stakeholder	Key	Active	Category	Role
LLNL IT Security	Y	N	IT	Safeguards LLNL IT systems from attack.
LLNL Com Support	Y	N	IT	Supports the telephony infrastructure of LLNL.
N Program Management	Y	N	Management	Responsible for a collection of nuclear-centric programs.
MicroSoft	Y	N	Vendors	Provides integral software products (Office etc…).
Syncplicity	Y	N	Vendors	Provides LLNL-based cloud services.
Apple	Y	N	Vendors	Provides LLNL-supported mobile hardware and software.
DOT	N	N	Regulators	Regulates the transport of hazardous (radioactive) material.
IATA	N	N	Regulators	Regulatory body acknowledged by commercial shippers.
LLNL IT (help desk)	N	N	IT	Provides general computer help services to LLNL employees.
Syncplicity Support	N	N	IT	Product support services from the vendor.
GS Management	N	N	Management	Responsible for a collection of security-oriented programs.
Lab Management	N	N	Management	Responsible for operation of LLNL for DOE.
Material Management	N	N	Shippers	Ships and accounts for radioactive material for LLNL.
Lab Shipping Services	N	N	Shippers	Ships non-hazardous packages for LLNL.
Commercial Shipper	N	N	Shippers	Provides shipping services to LLNL (FedEx).
Customers	N	N	Customers	Consumer of AIM services.
DOE	N	N	Sponsor	Sponsor and steward of "work for others" funds.

Table 1: Stakeholder Breakdown

Each stakeholder operates with its own objectives, priorities and constraints. Key stakeholders hold the power to significantly impact the Brahman system. Everything from operational interruptions to system rejection could result from failing to meet the acceptance criteria derived from key stakeholder's expectations. Table 2 lists these criteria. Due to significant overlap, the acceptance criteria for AIM staff have been grouped under the heading AIM.

Key Stakeholder	Acceptance Criteria
AIM	• Performs document management and scheduling at least as well as the current SP system • Robust, not prone to crashes or downtime • Accurate, does not lose or corrupt information • Performs radiation decay calculations without the need for additional systems • Allows viewing and editing on mobile devices • Performs statistical breakdowns of program efforts for management and reporting • Simple interact mechanisms
DOE	• Must comply with DOE mandated security requirements
LLNL IT Security	• Must comply with LLNL systems implemented to meet DOE and management requirements
LLNL Com Support	• Must not utilize unsupported hardware
N Program Management	• Must not violate security or cost-management requirements
MicroSoft	• Does not violate core security features • Does not require unsupported capabilities
Syncplicity	• Does not violate core security features • Does not require unsupported capabilities
Apple	• Does not violate core security features • Does not require unsupported capabilities
DHS	• Must be defensible as an important and capable tool consistent with mission and funding obligations

Table 2: Key Stakeholder Acceptance Criteria

Not all acceptance criteria are created equal. Some have a degree of latitude. Some expectations simply must be met in order for the system to be successful. Acceptance criteria are combined into a set of prioritized sacred expectations shown in Table 3.

ID	Sacred Expectation
E1	The system must comply with security and information technology rules and be compatible with associated institutional systems. LLNL will not allow the implementation of a system which fails this expectation.
E2	The system must be reliable and accurate. Users will reject a new system viewed as untrustworthy.

ID	Sacred Expectation
E3	The system must exceed the capabilities of the current suite of solutions. Changing systems requires work. Users will reject switching between lateral systems.

Table 3: Sacred Stakeholder Expectations

System Operational Context & Reference Operational Architecture

AIM Organizational Structure

AIM is organized similar to the model for commercial aviation. Each AIM deployment is considered akin to an individual flight, e.g., Los Angeles to New York. A qualified AIM employee is assigned the role of Operation Lead (OL) for each deployment. The OL is responsible for the safe and successful execution of the deployment through all its phases: planning, execution, and final documentation. This role is comparable to a pilot under the commercial aviation model. The OL must operate in accordance with the policies and procedures established and maintained by the Director of Field Operations (DFO); similar to how pilots must follow the regulations established by the Federal Aviation Administration (FAA). The Operations Coordinator (OC) ensures individual deployments do not conflict with each other, much like an air-traffic controller oversees multiple independent flights. These roles are summarized in Table 4. The principal investigator (PI) performs typical program management and reporting duties and does not align well with an aviation counterpart.

Position	Role	Counterpart
Operation Lead	Ensure success of an assigned deployment	Pilot
Director of Field Operations	Ensure consistency and high quality for all deployments	FAA
Operations Coordinator	Avoid scheduling and resource conflicts between deployments	Air-Traffic Controller

Table 4: AIM Positions

Current System Architectures

The AIM program is not new. It has been meeting its obligations under institutional constraints for years. Whether through creation or modification, processes and solutions currently exist to address critical needs. Brahman, the system intended to replace these lifelines, will need to address the flaws of the current system while navigating the same constraints. AIM's current system architecture is divided into two sections. The Connectivity Architecture is governed by the institution's technology stack and security controls, see Figure 2. The Process Architecture consists of AIM's internal systems and process controls and is shown in Figure 3.

The Connectivity Architecture is beyond AIM's control. As shown in Figure 2, LLNL has a fairly typical cyber security configuration. Work performed on site utilizes a local area network behind a protective barrier, or firewall. IT systems connected to the protected network enjoy freedom to consume services or use institutional resources. This defensive posture is reinforced by limiting the systems where executable code can be run. For example, a software script for processing data cannot be run on institutional email servers. The same script could easily be executed on an employee's dedicated machine.

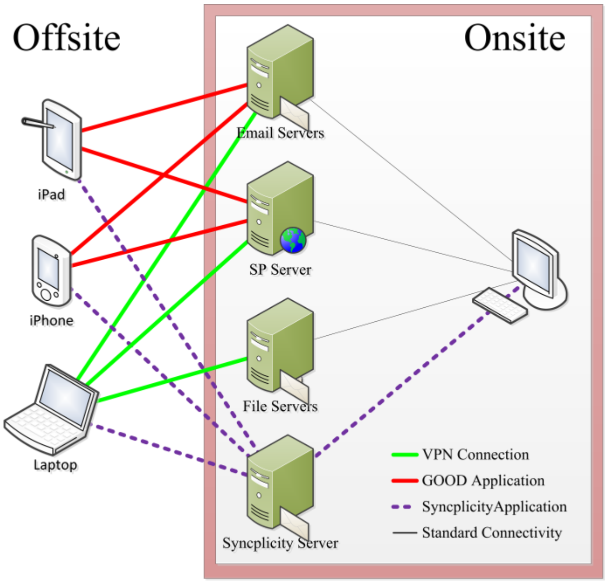

Figure 2: Current System Connectivity Architecture: Mobile devices must use intermediary software to access institutional resources, often with greatly diminished functionality.

Offsite work requires mobile devices. AIM utilizes laptops, iPhones, and iPads. These mobile devices are allowed access to institutional IT resources via software intermediaries. These cyber security sentinels offer connectivity but typically with reduced capability or increased burden. For example, Cisco's VPN client AnyConnect offers unperturbed capability for laptops at the cost of keeping track of a physical random-number token. Cellular devices such as the iPhone use an application called Good. Good allows email access and limited viewing of LLNL-based web content; however, file upload and executable code are strictly controlled. The SharePoint calendar feature is a prime example of reduced capability. Graphical representations of the SP calendar are not supported on iPhones or iPads. Instead a simple folder tree is depicted. Syncplicity is a LLNL-based cloud service for file sharing. While quite capable, it does not offer features outside of this narrow scope. The limitations of each of these offsite tools are shown in Table 5.

App	iPhone	iPad	Laptop
Good	Email; Reduced SP function; Reduced file sharing; Limited file upload	Email; Reduced SP function; Reduced file sharing; Limited file upload	NA
VPN	No Email; Reduced SP function; Reduced file sharing; Limited upload; Requires token	No Email; Reduced SP function; Reduced file sharing; Limited upload; Requires token	Full email; Full SP function; Full file sharing; Full upload; Requires token
Syncplicity	No email; No SP function; Full file sharing; Full upload	No email; No SP function; Full file sharing; Full upload	No email; No SP function; Full file sharing; Full upload

Table 5: Connectivity Architecture Mobile Application Limitations

AIM has no leeway with the Connectivity Architecture. Any proposed Brahman system must operate under these restrictions. AIM enjoys vastly more freedom with the second existing architecture, the Process Architecture. The diagram shown in Figure 3 is not complete. Given the fragmented nature of AIM's current set of solutions only core processes relevant to the Brahman system are shown.

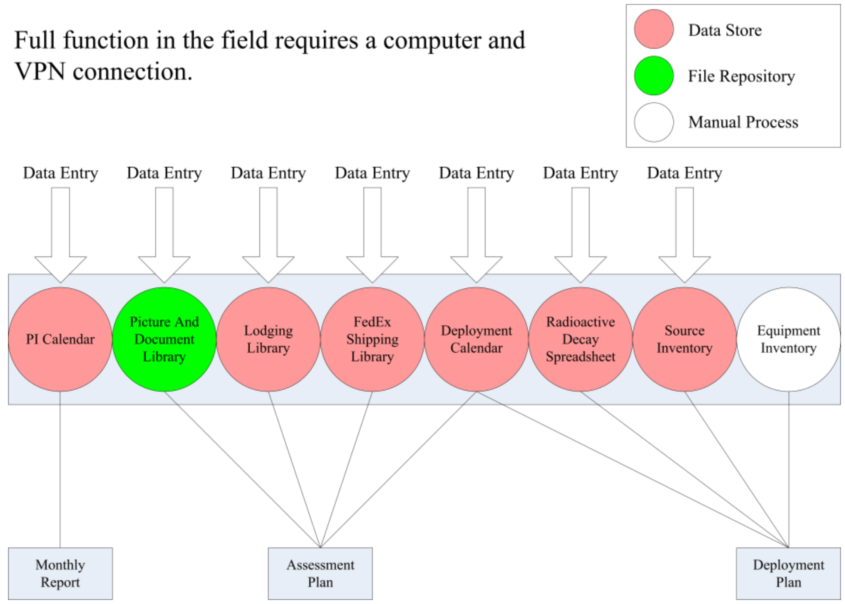

Figure 3: Current System Process Architecture: Data is stored in multiple locations which includes many inefficient and error-prone steps with human interactions. Utility in the field is greatly reduced due to the need for a computer and VPN connection.

Though an oversimplification, three critical products are produced by AIM in the current context. These products are referenced in Figure 3. A Monthly Report is a management tool summarizing efforts and expenditures. These reports are submitted to sponsors and laboratory management in order to provide regular program status updates. The AIM PI currently generates Monthly Reports via dedicated subsystems with information manually transferred from other AIM subsystems.

An Assessment Plan (AP) is a deployment-specific summary of activities and associated logistics. It is a snapshot of expectations generated a week in advance. It is subject to change as last minute requirements or requests regularly pop up. The sponsor and all deployment team members are provided a copy of the AP, to communicate rough expectations. The Operations Coordinator prepares each Assessment Plan primarily through a collection of SharePoint features, Excel spreadsheets, Word documents, emails, and discussions with the Operation Lead. The SharePoint site was originally envisioned to handle the process by automatically populating a template from a common calendar. This strategy was abandoned due to SharePoint limitations; namely poor form generation and size limits on key variables.

The Deployment Plan (DP) is the official record of sources and gear for each deployment. The Operation Lead uses the DP to perform inventories; ensuring all equipment and radioactive sources are returned to the laboratory. The Operation Lead generates the DP through substantial collaboration with the Operation Coordinator. Typically numerous iterations and several data stores are involved. Several steps require the manual entry or transfer of data. Similar to the Assessment Plan, attempts to use SharePoint to automate the creation of Deployment Plans were abandoned.

Brahman Architecture

The objective of the Brahman system is to consolidate the fragmented nature of the AIM Process Architecture. The numerous current data stores should be consolidated into a single official repository of programmatic information. Transactions, inventories, program management details, and historical data should be unified into a single program knowledge base. Essential products, such as the Deployment Plan, should be generated from the official record with no error-prone manual intermediary steps. Data entry should be controlled through mechanisms which provide quality control and consistent formatting. Additionally, full functionality should be achieved off site using the established Connectivity Architecture. The desired Brahman system architecture is shown in Figure 4.

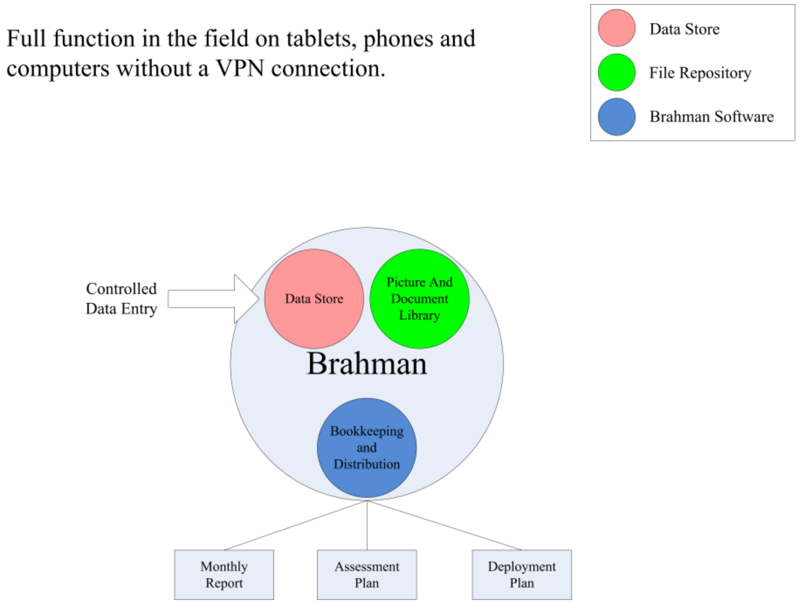
Full function in the field on tablets, phones and computers without a VPN connection.

Figure 4: Brahman System Architecture: A single data store is used which performs quality control during data entry, and full functionality is achieved on smart phones and tablets (calendar is no longer a data store, simply a graphical representation).

System Drivers and Constraints

As described earlier, certain drivers exist for the new system. The Brahman system must fit within current constraints, such as the LLNL Connectivity Architecture. Programmatic need provides the impulse for the new system. Desire for new capabilities provides even more motivation. Essential system drivers are articulated in Table 6.

ID		Driver	Description
D1		*Reduce Burden*	
	D1.1	Data Entry	Reduce time/effort required to enter data
	D1.2	Form Generation	Streamline the number of multi-user steps to generate common forms
	D1.3	Information Search	Reduce time/effort required to find historical products/data
	D1.4	Inventory Control	Establish a system for tracking gear – no manual lookup
D2		*Reduce Error*	
	D2.1	Unified Records	Only one official record of program equipment and events
	D2.2	More Automation	Reduce the dependence on manually-entered data
	D2.3	Quality Control	Perform quality control during data entry
	D2.4	Transaction Accounting	Maintain a history of user interactions
D3		*Increase Access*	
	D3.1	Tablet Access	Full system function and viewing on an iPad
		Smart Phone Access	Full system function and viewing on an iPhone

ID	Driver	Description
D4	*Simplify Processes*	
D4.1	Running Lanes	Allow clear running lanes for each user and their product
D4.2	Data Entry Forms	Provide entry electronic forms/templates for data entry
D4.3	Data Entry Tips	Provide hints or examples for data entry, e.g., file name formats
D4.4	Availability Checks	Interactively check availability for all assigned gear, sources, people
D5	*Utilize Information*	
D5.1	Historical Information	Provide links to relevant historical information to current interactions
D5.2	Contextual Information	Tie relevant references to current interactions, e.g., safety briefs

Table 6: New System Drivers

The proposed system must possess features which address the system drivers while adhering to the rules of the current system. These constraints primarily stem from AIM's position in a much larger organization and its financial stewardship responsibilities. Brahman must comply with the constraints shown in Table 7.

ID	Constraint	Description
C1	*Security Restrictions*	
C1.1	Firewalls – VPN	Cannot breach existing firewalls; must not circumvent VPN requirements
C1.2	Good Application	Cannot extend the functionality of the Good mobile application; must not violate application security measures
C1.3	Outlook	Cannot extend the functionality of Outlook or email servers; must not violate application security measures
C1.4	Syncplicity Application	Cannot extend the functionality of Syncplicity cloud servers; must not violate application security measures
C1.5	Executable Fencing	Must not require executable code in forbidden locations
C2	*LLNL Information Technology Stack*	
C2.1	Hardware	Cannot use unapproved hardware, e.g., new smart phones
C2.2	Software	Must not require new enterprise-level software
C3	*Cost*	
C3.1	Purchases	Must not include costly new purchases, e.g., a new $40k server set
C3.2	Labor	Must not include outside labor, e.g., consultants or vendor programmers
C4	*Schedule*	
C4.1	Operational Date	Must not take more the two months to deploy core features

Table 7: New System Constraints

Operational Scenarios

Operational Context

AIM currently maintains a patchwork information technology system; see the Process Architecture shown in Figure 3. This knowledge management system has grown in complexity as the program has grown in size and capability. Unfortunately, the number of error-prone subsystems has also grown, driving a matching increase in upkeep burden. The knowledge system plays a central role in AIM operations. Brahman should be a more capable and more efficient version of the knowledge system.

AIM personnel interact with the knowledge system at different times for different purposes. Some operations occur regularly. Others happen in a specific sequence for each deployment. Some operations only occur sporadically to meet temporary demands or new acquisitions. Figure 5 shows a graphical representation of a sample of critical AIM operational scenarios.

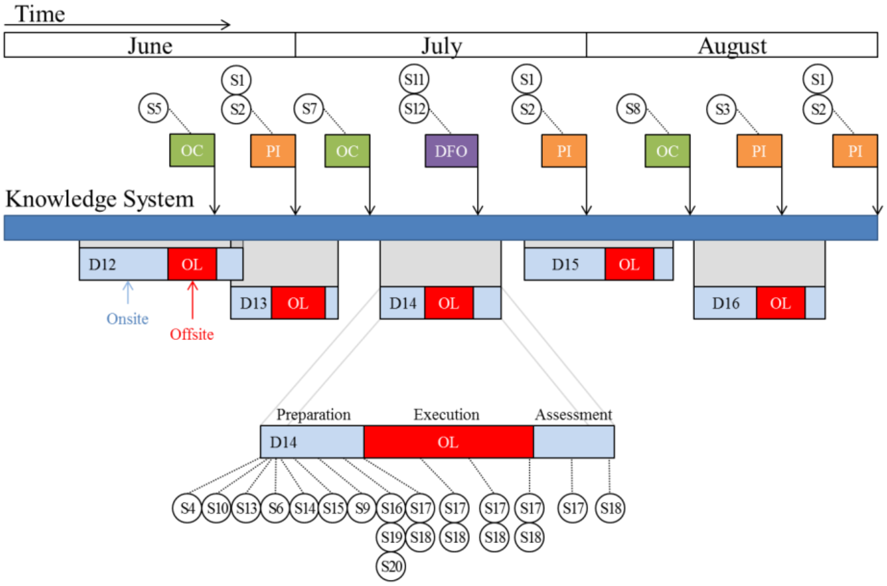

Figure 5: Operational Scenarios Diagram

Figure 5 shows hypothetical AIM operations over a three month span, June to August. Time flows linearly from left to right. The AIM knowledge system is depicted as a dark blue rectangle along the center of the diagram. AIM operations are shown as smaller individual rectangles whose widths represent duration. The primary system user for each operation is indicated by rectangle color and an internal label. Each operation requires one or more interactions with the knowledge system. Interactions are shown by connections linking operations with the knowledge system.

AIM deployments are depicted below the knowledge system in Figure 5 and are labeled sequentially from D12 to D16. Each deployment requires numerous interactions with the knowledge system. This elevated frequency is reflected by gray shaded connections rather than individual black connecting lines. Deployments have three phases: preparation, execution and assessment. The execution phase of each deployment takes place at a field location and is represented by a red segment.

Individual operational scenarios are shown as numbered black circles connected to the associated operation. For clarity, Deployment 14 has been expanded a representative example of typical scenarios for all deployments. Individual operational scenarios are articulated in Table 8 and discussed below.

Critical Scenarios

ID	Who	Scenario	Summary
S1	PI	Review	Review expenses and activities
S2	PI	Generate Report	Generate management reports for monthly obligations
S3	PI	Add Program Data	Add miscellaneous program data, e.g., supplemental reference data
S4	OC	Add Deployment	Add a deployment to the schedule
S5	OC	Set Warnings	Set conditions which trigger scheduling conflict warnings
S6	OC	Assign Sources	Assign special sources once notified of need by OL

ID	Who	Scenario	Summary
S7	OC	Add Sources	Add new sources to radioactive source inventory
S8	OC	Change Gear Status	Update gear inventory to reflect unavailable gear, e.g., out for calibration
S9	OC	Generate AP	Create an Assessment Plan, a summary of expected events
S10	DFO	Assign an OL	Select and notify an Operation Lead for a specific deployment
S11	DFO	Modify Procedures	Add new or update existing operations procedures or requirements
S12	DFO	Add Gear	Add new gear to inventory
S13	OL	Update Trip Needs	Update deployment sources, gear, and team needs based on planning
S14	OL	Add Hotel	Add a hotel to the lodging inventory
S15	OL	Add FedEx	Add a FedEx to shipping location inventory
S16	OL	Generate DP	Generate a Deployment Plan, official record of deployed gear and sources
S17	OL	Inventory	Perform an inventory of gear and sources assigned to the OL
S18	OL	Add Data	Add pictures, notes, and data to the AIM data store
S19	OL	Pack Sources	Document the load plan for shipped radioactive sources
S20	OL	Pack Gear	Document the load plan for shipped gear

Table 8: Operational Scenarios

Scenario 1: Review

Responsible: PI

Description: Perform a review of expenses and activities; Update key program metrics such as the number of deployments conducted and the number of customers supported; Project future costs and reconcile with current resources

Current Solution: The PI keeps a separate set of spreadsheets which are manually updated to reflect data found in multiple data stores such as the SharePoint calendar and various AIM reports

Desired Solution: Key program metrics should be automatically tabulated based on the official record of transactions

Scenario 2: Generate Report

Responsible: PI

Description: Monthly reports are generated for the sponsor; Similar data is entered into a Global Security project reporting system

Current Solution: The PI uses a dedicated set of spreadsheets to generate plots for monthly reports, then summarizes details and updates report templates; GS management reporting is done through the institutional system

Desired Solution: Key plots and reporting metrics should be directly linked to the official AIM record, not linked to duplicative spreadsheets

Scenario 3: Add Program Data

Responsible: PI

Description: Make reference data available to AIM personnel, e.g., bureaucratic procedure

Current Solution: The PI emails AIM personnel with an electronic file attachment then places the document on a server for reference; Server locations include SharePoint, a dedicated AIM server and the Syncplicity servers

Desired Solution: The PI uploads the new data file to one location: the Brahman system; notifications of new content occur automatically

Scenario 4: Add Deployment

Responsible: OC

Description: The operations calendar is updated to reflect the essential details of a new deployment: date, location, customer, federal lead

Current Solution: The OC, DFO, or PI updates the SharePoint calendar once notification occurs; Loose quality control is performed via forms with dropdown menu options

Desired Solution: The Brahman system is updated to include a new deployment; Tighter quality and format control is performed on entered data

Scenario 5: Set Warnings

Responsible: OC

Description: The system is used to avoid conflicts between deployments

Current Solution: The OC, DFO, and PI manually scan entered data looking for potential conflicts

Desired Solution: The OC places warning criteria on the system; Criteria are automatically evaluated regularly; Conflict warnings are transmitted automatically

Scenario 6: Assign Radiation Sources

Responsible: OC → OL

Description: Radioactive sources are selected for each deployment based on need and availability

Current Solution: Each OL enters the deployment need into the SharePoint calendar; The OC performs radiation decay calculations via a dedicated spreadsheet; The OC selects sources to meet the deployment need and assigns them to an OL

Desired Solution: Shift responsibility for source selection to the OL; Radiation decay calculations are performed via the Brahman system; Availability of individual sources is reconciled automatically by the Brahman system

Scenario 7: Add Sources

Responsible: OC

Description: New radioactive sources are procured then entered into the AIM inventory

Current Solution: The OC adds each source to both the SharePoint source inventory and the radioactive decay spreadsheet

Desired Solution: The OC enters new source data once: to the new Brahman system

Scenario 8: Change Gear Status

Responsible: OC

Description: Occasionally gear is not available, for example equipment is loaned or returned to a vendor for calibration

Current Solution: The OC makes a note of the disposition of unavailable equipment; A complete inventory of equipment does exist; An inventory of gear does exist for items tracked at the institutional level

Desired Solution: The OC modifies the official inventory of all non-consumable AIM gear in a manner that is preserved for archival purposes

Scenario 9: Generate Assessment Plan

Responsible: OC

Description: An Assessment Plan is created for each deployment

Current Solution: The OC assembles a final document via a combination of SharePoint automation and significant manual data entry and formatting

Desired Solution: The OC generates an AP from a template via Brahman automation; some final modifications may require human interaction but data contained in Brahman should not require manual reentry

Scenario 10: Assign an Operation Lead

Responsible: DFO

Description: The Director of Field Operations selects an Operation Lead for each deployment based on skill set, mission need, and availability

Current Solution: The DFO reviews the SharePoint calendar and email related to the deployment then notifies each OL via email or in person; The calendar is updated and a summary of assignments is communicated to the OC and PI

Desired Solution: The DFO reviews the need and Brahman calendar and makes an assignment; Notifications to OL, OC, and PI occur automatically

Scenario 11: Modify Procedures

Responsible: DFO

Description: The DFO manages the activities of operational personnel and maintains the procedures for deployments

Current Solution: The DFO creates or modifies a procedure then stores it in the SharePoint document management system; Notifications of new procedures are sent via email or other means of communication

Desired Solution: The DFO creates or modifies a procedure and places it Brahman; Notifications occur automatically via email with a summary of the change and a list of new obligations, e.g., reviews with signatures

Scenario 12: Add New Gear

Responsible: DFO

Description: New gear is added to the inventory

Current Solution: Institutionally tracked items are recorded in the LLNL system; No full inventory of AIM gear currently exists

Desired Solution: The new gear is entered into the Brahman system; Once entered, new gear is made available through the system for upcoming deployments

Scenario 13: Update Trip Needs

Responsible: OL

Description: The OL interacts with the federal lead for the deployment as well as the intended customers to generate an understanding of needs for gear, sources and personnel

Current Solution: The OL enters limited information into the SharePoint calendar and keeps a record in various file storage locations

Desired Solution: All details related to a deployment should be stored in the Brahman system; Specific needs should automatically be communicated to the associated positions, for example the OC should be notified of need for special sources automatically

Scenario 14: Add Hotel

Responsible: OL

Description: A history of hotels suitable for deployment needs is maintained

Current Solution: Lodging information is stored via SharePoint or communicated via email; The OC occasionally must hunt for lodging information while manually completing the Assessment Plan

Desired Solution: All lodging information should be stored via Brahman for automatic inclusion in the Assessment Plan; Assigned team members should be notified automatically of lodging details via email

Scenario 15: Add FedEx

Responsible: OL

Description: A history of FedEx locations suitable for deployment needs is maintained

Current Solution: Shipping information is stored via SharePoint or communicated via email; The manually entered into the Assessment Plan and the Deployment Plan

Desired Solution: All shipping information should be stored via Brahman for automatic inclusion in the Assessment Plan and Deployment Plan

Scenario 16: Generate Deployment Plan

Responsible: OL

Description: The Deployment Plan includes the official inventory of gear and sources taken on each trip; It includes load plans and packing information along with shipping locations and safety brief details

Current Solution: The DP currently undergoes a multistep collaborative process between the OL, OC and DFO; It is initially populated via the SharePoint calendar but manual data entry has become common due to limitations in SharePoint functionality

Desired Solution: All details needed for a DP should automatically be populated from the initial record; The creation of a DP after a change in load plan or assignment should be a quick and interactive process requiring only the OL; Notifications and summarizations of DP modifications should be communicated to the OC, PI, and DFO automatically via email

Scenario 17: Inventory

Responsible: OL

Description: The process of manually verifying the presence of deployed items

Current Solution: The inventory process occurs prior to each trip and on return; Additionally inventory is performed at the end of each shift; Inventories are performed via lists contained in the Deployment Plan

Desired Solution: The inventory list in the DP should automatically be generated to reflect the load plan and duration of the deployment

Scenario 18: Add Data

Responsible: OL

Description: Notes, images and sensor data are collected during deployments and added to the AIM knowledge base

Current Solution: Notes and images are collected via cameras, mobile devices, hand-written notes, documents authored on laptops, and reports collected during the event; Relevant information is added to the knowledge base once the OL returns to the laboratory

Desired Solution: The addition of deployment data to the knowledge base should occur during the deployment; Notifications of added data should occur automatically

Scenario 19: Pack Sources

Responsible: OL

Description: Radioactive sources are packaged according to DOT and LLNL policy

Current Solution: The generation of a radioactive source load plan is performed by the OL and manually entered into the Deployment Plan

Desired Solution: The radioactive source load plan should be reflected in the Brahman system and added to the Deployment Plan automatically

Scenario 20: Pack Gear

Responsible: OL

Description: Gear is packaged in a series of protective cases

Current Solution: The generation of a gear load plan is performed by the OL and manually entered into the Deployment Plan

Desired Solution: The gear load plan should be reflected in the Brahman system and added to the Deployment Plan automatically

Implementation Concepts and Rationale

Candidate Technologies

There are several possible technical solutions worth considering for the Brahman system. These solutions are described below.

Syncplicity + Data File + VBA (SDFV)

Syncplicity is a fairly new institutional service provided by LLNL. It provides cloud services comparable to those offered by vendors such as Google and Apple but with servers located at LLNL. Syncplicity offers uniform connectivity across all AIM devices, see Figure 2. This connectivity is the backbone of the SDFV solution.

In addition to the core capability, Syncplicity offers one more crucial feature. Mobile devices running the Syncplicity application can open and modify documents from the cloud service. This simple feature is surprisingly difficult to achieve via smart phone or tablet outside of Syncplicity. For example, accessing a document via SharePoint and Good (or SharePoint and VPN) is possible on an iPhone. However, editing and saving a file is vastly more complicated and sometimes not even supported. Cybersecurity restrictions and Apple system design conspire to make seemingly trivial operations unachievable. Syncplicity allows MS Word and Excel documents to be opened and edited on iPhones and iPads. The resulting files are then saved and synchronized with the cloud seamlessly.

Ubiquitous connectivity and access to files enables the second component of this solution: an official record contained in a data file. An Excel spreadsheet is a highly effective data store. Individual tabs can be dedicated to specific programmatic areas. For example, the gear and radioactive source inventories are easily organized into a spreadsheet. Financial data and radioactive decay calculations are already stored and managed in spreadsheets. The file is easily accessed and backed up.

The final component of the SDFV solution is Visual Basic for Applications. Custom software provides desired system features. Small customizable software scripts can generate forms, send emails, update files, and provided tailored services. AIM has several individuals with robust experience writing software scripts for data analysis and visualization. These scripts would not be permitted to run on enterprise machines but a dedicated "script server" could be deployed much like the AIM SharePoint server.

Syncplicity + Database + VBA (SDBV)

This solution mirrors the Syncplicity system described above with one key difference. The use of a file as an official record offers some challenges. A standard database solution warrants consideration. Rather than an Excel spreadsheet providing data to various AIM processes, a database solution such as Oracle or MySQL could be used.

One significant obstacle to the SDBV solution is the shortage of in-house experience with database administration. This lack of familiarity would require time to overcome.

Silverlight (SL)

The core capabilities of a SharePoint installation leave a great deal to be desired. However, SharePoint can be remarkably capable when paired with custom Silverlight applications. The SL solution would center on a new and more robust set of AIM SharePoint servers. Current system shortcomings would be addressed with custom Silverlight applications run via SP. The SL system would closely match more typical corporate solutions.

The SL solution has negative schedule and cost implications. AIM does not currently employ any individuals with Silverlight programming experience. Additionally, a new server configuration with redundancy and load balancing would likely cost upward of $40k. The sponsor is unlikely to support this expenditure.

Refined Current Solution (RCS)

While not optimal, the current system could be refined. Redundant data stores could be unified. Access and quality control could be enforced administratively. AIM procedures, nomenclatures and terminology could be bent to submit to current IT restrictions. Offsite capabilities could likewise be achieved via behavioral adjustments.

The RCS solution does little to expand the system. Instead it achieves quality control by placing additional constraints on system interactions. Short term gains by avoiding development cost are eventually lost due to reduced productivity.

Candidate Comparison

The proposed solutions are weighed against the system drivers and constraints in Table 9. Both Syncplicity solutions score well on drivers. However, the additional start-up time required to learn database administration causes a scheduling penalty for SDBV. Overall, the SDFV solution scores the highest, fitting all of the constraints. Due to the similarity of the two solutions, the SDFV could be migrated to a SDBV solution in the future, possibly with minimal cost.

	SDFV	**SDBV**	**SL**	**RCS**
D1: Reduce Burden	+	+	+	-
D2: Reduce Error	+	+	+	S
D3: Increase Access	+	+	S	-
D4: Simplify Processes	+	+	+	-
D5: Utilize Information	+	+	+	-
C1: Security Restrictions	S	S	S	S
C2: IT Stack	S	S	S	S
C3: Cost	S	S	-	-
C4: Schedule	S	-	-	S
Sufficient	4	3	3	6
Plus	5	5	4	0
Minus	0	1	2	5
Score (Sum)	5	4	2	-5

Table 9: Pugh Chart for Potential Solutions

Proposed System Operational Architecture

The Connectivity Architecture described previously is streamlined under the proposed solution. A new institutional user account is created with dedicated email and Syncplicity accounts: "Syncp-AIM." The SharePoint server is abandoned and files are consolidated on Syncplicity servers. Offsite email is still delivered via Good and VPN; however, data access and entry are achieved via Syncplicity for all platforms, see Figure 6.

In order to achieve Brahman's desired feature set a standard workstation is turned into a dedicated script engine. This machine is assigned to the Syncp-AIM user account and enjoys the same scripting privileges as any other user machine. Scripts are written to crawl the Syncplicity file structure and perform accounting and upkeep tasks. For example, daily summary emails could be easily generated for the PI assessing the status of needed deliverables. Similarly, a dedicated script could ensure the master data file is backed up nightly.

The Process Architecture described earlier is also altered. All data stores are unified in a single master spreadsheet. Data synchronization is performed via custom VBA code embedded in a series of smaller spreadsheets. Each AIM position has a set of these dedicated control spreadsheets. For example, the OC performs calendar updates with a dedicated file located in the Operations Coordinator folder on Syncplicity, see Figure 7.

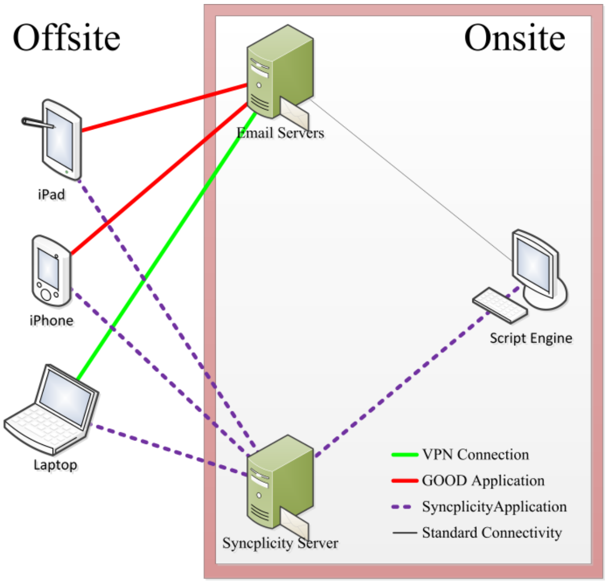

Figure 6: Proposed System Connectivity Architecture: The SharePoint and File Share servers are no longer utilized; Syncplicity stores data in one ubiquitously accessible location, form-generating and notification scripts run on a desktop linked to both the Syncplicity and Email servers.

Quality control occurs as data is entered through a control spreadsheet via user forms with auto-populated menus and automatic variable formatting. Control spreadsheets pull and push data to the Official Record. All transactions are recorded and a deleted or corrupted control sheet is easily recoverable. Control spreadsheets running VBA are not compatible iPads or iPhones. To address this issue, standard Excel files will be automatically generated and updated. Users of mobile devices will be allowed to edit the raw control files. The script engine will monitor control spreadsheets, detect modifications, then perform synchronization with the official record.

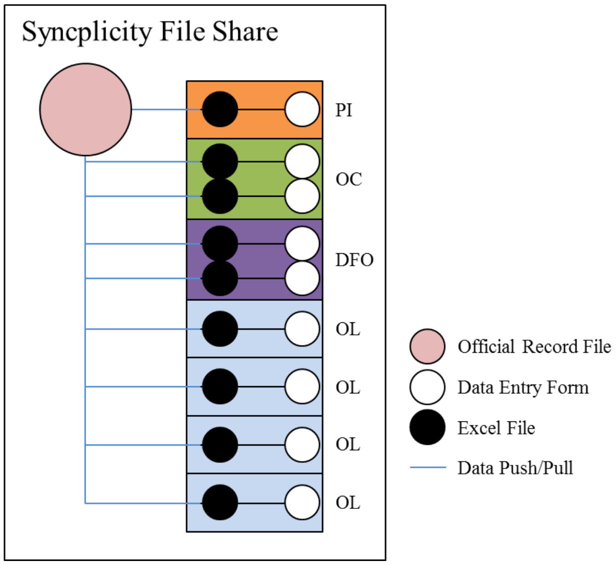

Figure 7: The Modified Process Architecture: All files are located on the Syncplicity servers. Interactions with the official data store are managed via dedicated spreadsheets located in the position-specific folders. Products such as the AP and DP are generated via VBA embedded in Excel files.

System Requirements

In order to gain acceptance as a valid solution, the Brahman system must meet certain requirements. These requirements are a reflection of stakeholder expectations and the constraints elaborated above. The system requirements are listed in Table 10.

ID	Genesis	System Requirement
R1	E1, C1	Must not require executable code in institutionally forbidden locations
R2	E1, C1	Must not require special exceptions to security policies
R3	E1, C1, C2	Must not require prohibited hardware
R4	E1, C1	Must not disable or circumvent established safeguards
R5	E2, D2	System failures must not corrupt historical records
R6	E2, D1	System down time must be comparable to down time already associated with institutional services
R7	E2, D1	Corrupted or lost files must be readily replaceable with information no older than the previous day
R8	E2, D5	Must maintain a historical log of transactions
R9	E3, D1, D2, D4	Must maintain an inventory of AIM gear deemed non-consumable
R10	E3, D1, D2, D4	Must maintain an inventory of AIM radioactive sources
R11	E3, D1, D2, D4	Must maintain in inventory of AIM lodging locations
R12	E3, D1, D2, D4	Must maintain in inventory of AIM-appropriate shipping locations
R13	E3, D1, D2, D4	Must perform standard radiation decay calculations automatically
R14	E3, D1, D2, D4	Must allow deployment needs to be updated at an interactive pace
R15	E3, D1, D2, D4	Must link inventory selection to official inventory; prohibiting manual entry
R16	E3, D1, D2, D4	Must allow the shipping configurations for radioactive sources to be generated/modified
R17	E3, D1, D2, D4	Must allow the packing configurations for gear to be generated/modified
R18	E3, D1, D2, D4	Must generate Deployment Plans automatically without modification to data contained in the system
R19	E3, D1, D2, D4	Must generate Assessment Plans automatically without modification to data contained in the system
R20	D5	Must link relevant sections of safety documentation with each Deployment Plan
R21	D5	Must link relevant gear manuals and specification sheets with each Deployment
R22	E3, D1, D2, D3, D4	Must provide full viewing and updating capability on mobile platforms
R23	E3, D1, D4	Must aggregate locations visited into a map graphic for monthly reporting obligations
R24	E3, D1, D4	Must track customer information
R25	E3, D1, D2, D4	Must provide an interactive updateable calendar depicting deployments spanning a fiscal year
R26	E3, D2, D4, D5	Must maintain a historical record of assignments for gear, sources, shipping drums and staff
R27	E3, D1, D2, D4	Must verify availability of gear, sources, shipping drums and staff prior to deployment assignment
R28	C3	Must not require new hardware costing greater than an individual work station
R29	C3, C4	Must not require more than two months to establish onsite capabilities
R30	C3,C4	Must not require out-of-group expertise for system maintenance; excepting those already committed to institutional security and IT stack administration

Table 10: System Requirements

Organizational and Business Impact

The desired result of adopting the Brahman system is a more efficient and streamlined organization capable of increasing its operational tempo even further. The system's implementation should be transparent to passive stakeholders but will impact all of the active stakeholders. Anticipated effects of the new system are summarized below.

- Tasks which currently require collaboration will become more tightly coupled to the position responsible for their completion. This should result in less confusion over responsibilities and fewer procedural bottlenecks as individuals are free to complete tasks independently.
- The burden associated with critical and repetitive tasks will diminish as time-consuming and error-prone steps are replaced with automation.
- Awareness of deliverables and schedules will increase as automated alerts and summary notifications are established.
- No adjustments to staffing are anticipated due to the use of in-house skills.
- Minimal retraining is anticipated due to the use of familiar system interfaces.

Risks and Technology Readiness Assessment

The replacement of a functioning core system is not without risk. Though fragmented and burdensome, the current collection of AIM processes is allowing the program to meet its obligations. The ultimate risk of switching to Brahman is system failure leading to missed deliverables. To mitigate this existential risk, Brahman must be run in parallel with the legacy system until full capability and stability have been validated.

The most vulnerable facet of Brahman is its reliance on custom software. These scripts will accomplish the bulk of the new features associated with the system. The software must be designed, authored, validated and implemented by AIM personnel in order to remain compliant with cost constraints. The modular nature of these scripts, each associated with specific tasks, should allow core capabilities to be emphasized. Less essential features can be added once fundamental features are demonstrated to be robust.