Technology Solution

Section 11.0

FP reference: 4.1.11, Technology Solution, Page 52

RFP. Vendor should demonstrate how the proposed components integrate to support operations, workflow and achievement of specified service levels, and are maintainable and supportable. Vendor should describe their development and operating environments and facilities, and how support services are provided. Services described should include data center/operations support, help desk/customer support, facility security, training and ongoing education, systems analysis/architecture/design, system development and testing, and ongoing data reconciliation. The vendor should complete the checklist columns of Appendix 2 – Detailed Business and Technical Requirements, Section B.

Deloitte will host the DW/DSS and maintain a secure site and secure back-up site within the continental United States. The Vendor must be responsible for all costs associated with supporting the facilities and ensuring that the facilities comply with legal requirements.

Deloitte is pleased to propose a comprehensive Data Warehouse and Business and Clinical Intelligence solution that delivers value and flexibility to BMS that is necessary for a rapidly changing health care environment. Our proposed Technology Solution is comprised of the following components:

- Secure Tier III Hosted Data Centers (Primary and Disaster Recovery) which includes best-of-breed hardware, software and network components
- A Data Acquisition and Data Quality Platform
- A Data Warehouse (DW) Platform
- A Business and Clinical Intelligence (BI) Platform
- A Managed Meta Data Environment (MMDE)
- A System Construction and Testing Approach
- A comprehensive approach to Security, Privacy and Confidentiality
- A Business Continuity Plan

The Deloitte proposed Technology Solution provides a unified, fully functional MMIS Data Warehouse along with a Business and Clinical Intelligence solution.

Infrastructure and Hosting

To deliver this DW/DSS solution to BMS, Deloitte has teamed with one of the leading global technology delivery organizations, IBM to provide the hosting facilities, high availability technology platforms and managed service. IBM is uniquely positioned to provide a solution that helps meet both business-critical and technological requirements, such as:

- A hosting model that provides a high quality of service clearly supports both BMS' near-term and long-term technology requirements

- A hosting provider who is invested in the managed services portfolio allowing BMS more time to focus on delivering quality medical services to the West Virginia residents
- A proven solution carefully configured according to IBM standards, employing leading-edge processes and tools for an optimal solution

IBM is an industry leader in hosting and is recognized as such by industry analysts Gartner and IDC for vision, ability to execute and lead from a U.S. hosting market share perspective.

Facilities

IBM managed hosting services leverage fully hardened, fault-tolerant data centers, which have been designed to accommodate a wide variety of application platforms and networking equipment. Their data centers, located in Sterling, VA (Primary) and Mesa, AZ (Secondary-DR), are Tier III certified and are built to universal business code standards and offer security-rich facilities from both a physical and logical standpoint. These hosting facilities offer an environmentally controlled application hosting environment that is connected directly to Tier-1, Internet Service Provider (ISP) networks. The following information provides details about the Applications on Demand (AoD) hosting centers' environmental controls and processes.

Electrical Power

Two diversely routed public utility circuits provide electrical power. Each circuit has its own dedicated switchgear and transformers located on the property. The main switchboards within the facility control both of these circuit sets through a tie main, which allows switching from one circuit to the other. The main switchboard provides continuous power throughout the facility by feeding redundant uninterruptible power supply (UPS) systems and other distribution panels.

The UPS systems consist of redundant racks of batteries, redundant UPS cabinets, a UPS control cabinet, and a maintenance bypass cabinet. The batteries provide continuous operation of the critical systems in case of a commercial power failure. Parallel configuration allows maintenance without impairing the systems' ability to sustain power should an outage occur.

After 1.5 seconds without commercial power, automatic switches activate the diesel engine generator sets. Within 30 to 45 seconds, the generators can supply the necessary power to maintain the facility. The diesel engine generators and fuel supply are situated to eliminate vibration and noise in the building. These generators can run indefinitely and the facility has enough fuel stored for up to three weeks at all times.

Environmental Support Systems

The data center's structural design provides environmental independence between the general office area and the specialized computer operations areas. Electrical power, telecommunications, and environmental conditioning are redundant. Heat, smoke, and fire detection and suppression systems are located throughout the building. An advanced system monitors temperature, humidity, and other environmental conditions. The system's video monitors display all alarm conditions.

Fire Protection/Suppression

The main control panel for the facility fire detection, alarm, and suppression system is located in the operations command center, with a remote enunciator panel in the security station. Both of these areas are manned 24 hours a day, 7 days a week, including holidays. The system consists of multiple 4-inch dry pipe pneumatic sprinkler valves. The valves are fully automatic and have their own air compressor.

The system uses overlapping smoke and rate-of-rise detectors located both under the raised flooring and in the ceilings throughout the facility. The automatic sprinkler system is enhanced by a combination of portable dry chemical fire extinguishers strategically placed throughout the facility.

Facility Grounding

An electrical ring grounding system encircles the entire facility. This system consists of deep-driven stainless steel rods at each of the corners of the facility, and shallow-driven stainless steel rods located in pairs between the corner rods. The rods are connected through a continuous ground circuit of buried copper cable. The resistance of the deep-driven rods has tested at zero (0) ohms.

All electrical panels, power distribution equipment, computer equipment, and raised floor systems in the facility are connected to a common ground bus. This ground bus is connected to the ring grounding system at a corner deep-driven rod.

HVAC

The facility uses a cooling system to provide proper air conditioning to the hosting environment. Computer machine rooms have been plumbed to facilitate additional air handler units or compressors, as additional cooling becomes necessary. Air handlers and compressors connect to a redundant closed loop, which is supplied from two 410-ton cooling towers that are supplied by redundant city water sources. In addition, the facilities have installed a private well on the property to provide emergency backup for the city water supply.

Operating Platform

Deloitte will leverage a virtualized Managed Hosting Service where IBM provides dedicated server instances with installation, maintenance and managed service support up to and including the OS. IBM managed services infrastructure services provides hosting services for server capacity allocated from IBM Power and IBM System systems for Windows applications, middleware and database software. Our clients order entitlements to virtual server instances based on the processing power, memory and storage which their clients, their systems integrator, or their software vendor determines is necessary for them to install and run their software. IBM manages everything from the data center, common core infrastructure, local area network, security systems, storage area network and backup systems up through and including the operating system and associated system software tools.

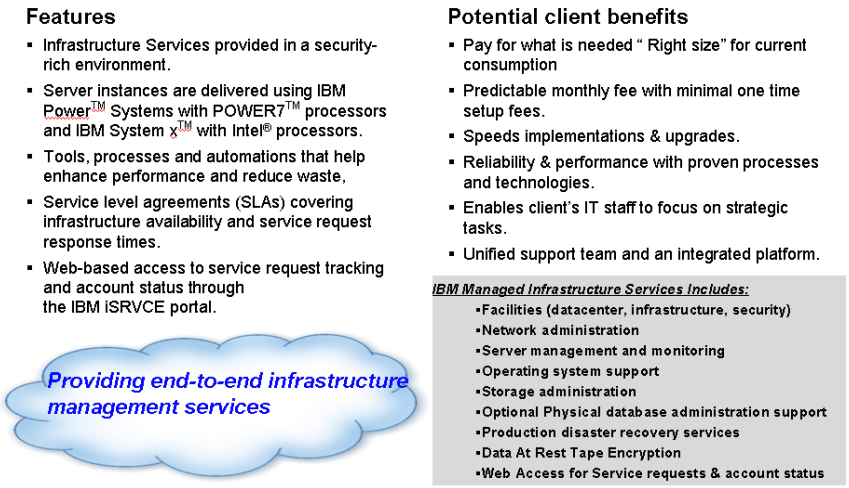


Figure 11-1. IBM Managed Services.

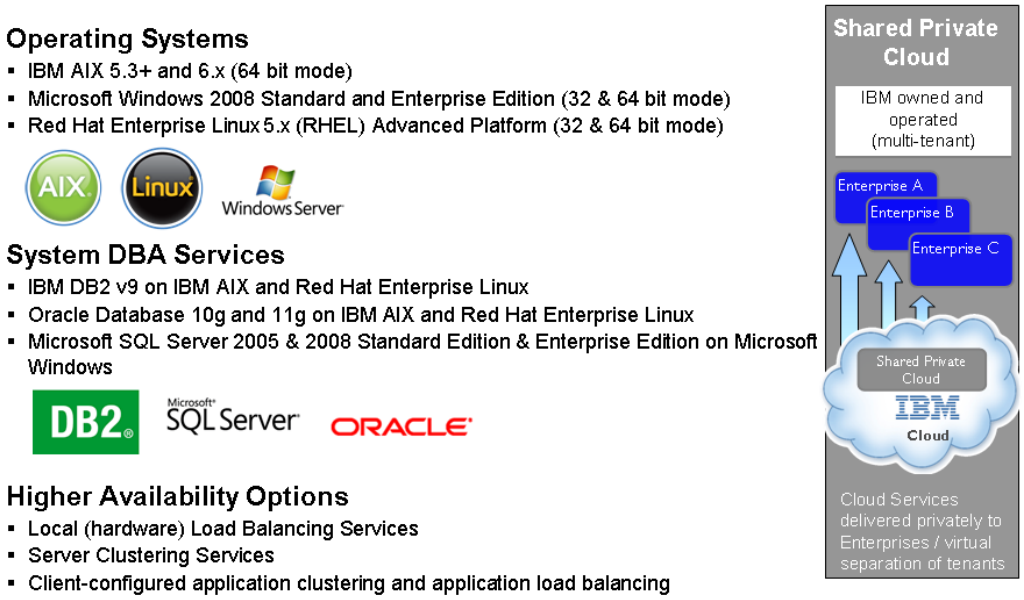


Figure 11-2. IBM Managed Services Infrastructure Services.

Deloitte will leverage a virtualized managed hosting service where IBM provides dedicated server instances with support up to and including the OS. IBM will provide secure telecom lines from the IBM datacenters leveraging Sprint's Frame Relay Service, as shown in the following figure.

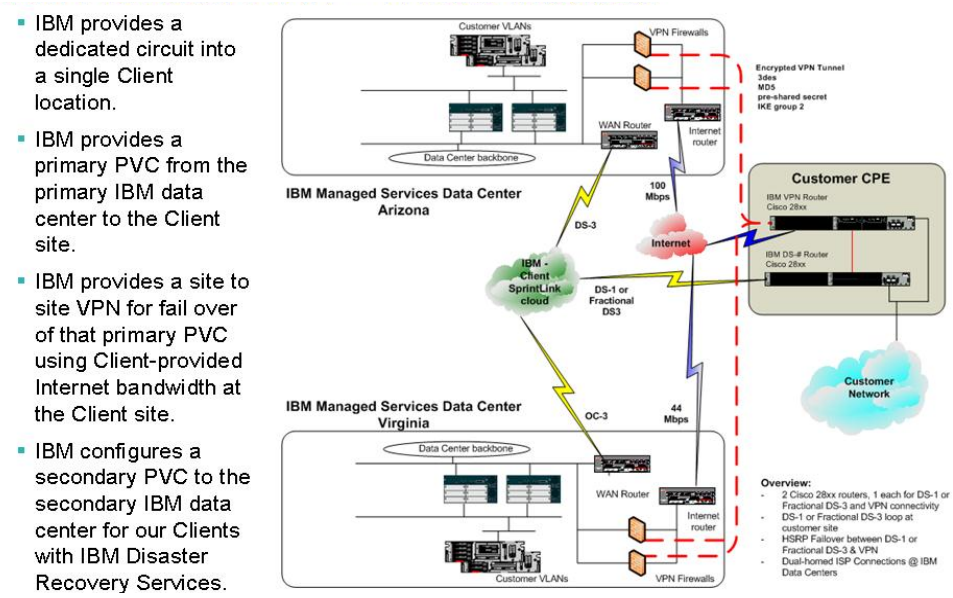


Figure 11-3. IBM Provided Wide Area Network.

Operational Support

The Deloitte hosting solution includes the following standard services:

- **Service level agreements.** Helps provide accountability for the availability of the DW/DSS solution

- **Server Management.** From setup and configuration to ongoing steady state operations, IBM will take care of the day-to-day tasks
- **Systems Monitoring.** This includes monitoring DW/DSS servers, operating systems and the network infrastructure and proactively resolving problems
- **Networking Services.** Including security-rich and redundant connections to the DW/DSS environment from multiple Tier 1 backbone providers
- **Security Services.** Including firewalls, network intrusion detection and anti-virus scanning
- **Robust Storage.** Providing security-rich, fully managed SAN (storage area network) storage for the DW/DSS data in either a RAID 5 or RAID 0+1 configuration
- **Data Backup and Restoration.** Managed, reliable encrypted tape backup of the data and system images, with offsite tape storage for added protection
- **Operations Help Desk.** Expert technical resources available 24x7x365
- **Web Portal.** Provides online access to alerts and warnings, status reports and management resources

Deloitte's proposed solution also includes IBM's iSRVCE tool, which is a Web-based central command and control system that can give both BMS and Deloitte visibility to, and control over, the hosted DW/DSS environment. The iSRVCE system offers a customizable information dashboard, online service request entry and tracking, ad hoc reporting capabilities, online service-level agreement (SLA) metrics, and an indexed, searchable repository of shared documents, which includes project collaboration features that can be used to manage critical materials such as Sarbanes-Oxley documents. With iSRVCE technology, Deloitte will have the power to make well-informed decisions regarding the DW/DSS operations and can communicate in real-time with IBM when necessary.

Physical Security

Deloitte with its IBM hosting teaming partner will designate a Physical Security Officer and Facility Manager for the DW/DSS facilities. The responsibilities of the Physical Security Officer and Facility Manager will include:

- Supervise the assignment of security credentials and security access for access to the DW/DSS Data Centers
- Periodically review physical security policies and processes to see if updates are necessary
- Oversight of the security guards that monitor the facility as well as the equipment (i.e., cameras, etc.) used
- Reviewing the physical access logs regularly
- Preparing an incident report for the ISO in the event of a real or suspected violation of the Physical Access Policy
- Perform audits to confirm policy is being implemented. The frequency of the audits will be annually at a minimum

Facility Structural Security

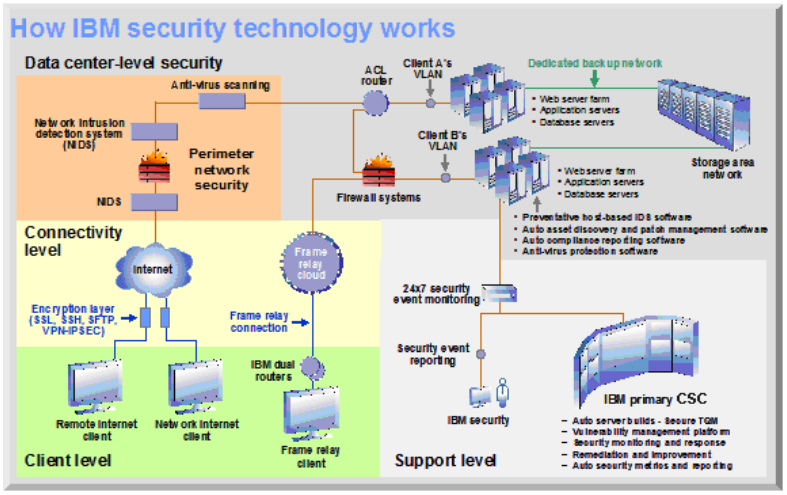
The proposed hosting facilities are located in Phoenix AZ and Sterling VA - and in - with the following addresses:

Phoenix, AZ (DR Location) IBM – AOD Operations 811 South 16th St. Phoenix, AZ 85034	Sterling, VA (Primary Location) IBM – AOD Operations 22860 International Drive Sterling, VA 20166

Physical access to IBM facilities is protected by badge access. Badge access to the facilities is only granted to IBM personnel and authorized contractors. All IBM critical infrastructure including servers, security infrastructure, and networking equipment is housed in IBM's facilities. These are protected by steel cages, double door entry ways, hallway cameras, and authorized personnel are restricted through the use of badge access and are required to show government-issued identification to receive that badge at the security desk (e.g. driver license). Employees are screened prior to being hired. They are given a security badge (the badges have pre-defined access rights) to enter into secured areas of the building to perform their work functions. Upon termination, the facility is notified of their termination and all right and privileges are revoked. IBM limits access to the building by a single card-key controlled entrance adjacent to the security station. Security features include:

- Entrants use the biometric hand scanners for data center access
- Electronic Card Key Access
- “Man Trap” with Biometric Palm Scan and Individual Personal Access Code
- 24 x 7 on-premise security officers
- Facilities command station
- Continuous closed circuit video surveillance through Stationary and 360° Cameras (interior and exterior)
- Security breach alarms
- The Data Center is staffed on a 24 x 7 basis, as well as a 24 x 7 Security Guard at the security desk. Aside from regular staff movement around the Data Center, the Security Guard conducts hourly rounds of the facility.
- Cabinets have dual power sources, as does all server equipment.
- IBM permits clients to visit the data center, but they must first, register at the security station and are then escorted during their entire visit. Visitors must wear a “visitor” badge and be escorted at all times. Before a visitor enters into the facility, an employee must submit the proper paperwork to Security identifying the visitor and expected arrival and departure times. All visitor tours must be facilitated by a tour coordinator. At no time are they allowed in the data center without an escort. The double doors are alarmed according to standard Data Center procedures.
- Facility Director/Manager performs regular internal audits on employee, vendor and visitor access. Every year, a third party audit firm conducts a site visit and reviews current processes/procedures and performs tests to verify that security policies are followed. These third party audits have not identified any material issues over the past two years.

IBM’s unified security framework is illustrated in the figure that follows.



WV_DW_DSS-068

Figure 7-4. How IBM Security Technology Works.

Infrastructure

Environments

Deloitte is proposing four physical environments (i.e., production, development, test, and disaster recovery) that support the requirements outlined within the RPF. These environments will have a similar look and feel with the majority of user based software available as necessary to support those environments. Below is a table that maps our physical environments to the logical environments outlined in the RFP.

Physical Environment	Logical Environment
Production	Production
Disaster Recovery	Disaster Recovery Backup Failover
Testing	User Acceptance Testing (UAT) Training
Development	Development Unit Testing

As outlined below, the production DW/DSS environment fully satisfies BMS requirements for both production operation and failover. In addition, Deloitte has architected a series of supporting environments to support BMS's requirements for disaster recovery and business continuance, failover, testing, user acceptance testing, training, and development.

Production Environment

Hardware	Software
Database Server (x 2): High Availability (HA) 2 x 4 Core Intel Xeon 2.66 GHz, 32 GB Memory	Oracle 11g, Real Application Cluster, Diagnostic Pack, Tuning Pack, Configuration Pack, Change Management Pack, Provisioning and Patch Automation Pack, and ASG-Rochade SCANORAC

Hardware	Software
ETL Server (x 2): 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Informatica PowerCenter 9.1, Informatica Data Quality 9.1, Oracle Weblogic Server Enterprise Edition, Weblogic Server Management Pack, Webcenter Suite and Management Pack, and ASG-Rochade Scanner for Informatica
Application Server (x 2): 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Cognos 10 Business Intelligence, and ASG-Rochade Scanner for Cognos
Web Server (x 2): 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Cognos Connection 10, ASG-Rochade WebAccess
Storage Area Network	Initial Configuration: 1 TB (usable), RAID configuration

Disaster Recover Environment

Hardware	Software
Database Server (x 2): High Availability (HA) 2 x 4 Core Intel Xeon 2.66 GHz, 32 GB Memory	Oracle 11g, Real Application Cluster, Diagnostic Pack, Tuning Pack, Configuration Pack, Change Management Pack, Provisioning and Patch Automation Pack, and ASG-Rochade SCANORAC
ETL Server (x 2): 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Informatica PowerCenter 9.1, Informatica Data Quality 9.1, Oracle Weblogic Server Enterprise Edition, Weblogic Server Management Pack, Webcenter Suite and Management Pack, and ASG-Rochade Scanner for Informatica
Application Server (x 2): 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Cognos 10 Business Intelligence, and ASG-Rochade Scanner for Cognos
Web Server (x 2): 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Cognos Connection 10, ASG-Rochade WebAccess
Storage Area Network	Initial Configuration: 1 TB (usable), RAID configuration

Testing Environment

Hardware	Software
Database Server: 1 x 4 Core Intel Xeon 2.66 GHz, 32 GB Memory	Oracle 11g, Real Application Cluster, Diagnostic Pack, Tuning Pack, Configuration Pack, Change Management Pack, Provisioning and Patch Automation Pack, and ASG-Rochade SCANORAC
ETL Server: 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Informatica PowerCenter 9.1, Informatica Data Quality 9.1, Oracle Weblogic Server Enterprise Edition, Weblogic Server Management Pack, Webcenter Suite and Management Pack, and ASG-Rochade Scanner for Informatica
Application Server: 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Cognos 10 Business Intelligence, and ASG-Rochade Scanner for Cognos
Web Server: 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Cognos Connection 10, ASG-Rochade WebAccess
Storage Area Network	Initial Configuration: .5 TB (usable), RAID configuration

Deloitte proposes a consolidated, multi-purpose environment to satisfy BMS's requirements for User Acceptance Testing and Training. Providing economies of scale, this environment can support multiple independent domains and workspaces, to allow simultaneous, independent activity in each area with no resource contention. This environment provides full scale capability and as such is a mirror image to the production environment only with a single stack platform and where the SAN will have half as much usable storage.

Development Environment

Hardware	Software
Database Server: 1 x 4 Core Intel Xeon 2.66 GHz, 32 GB Memory	Oracle 11g, Real Application Cluster, Diagnostic Pack, Tuning Pack, Configuration Pack, Change Management Pack, Provisioning and Patch Automation Pack, and ASG-Rochade SCANORAC
ETL Server: 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Informatica PowerCenter 9.1, Informatica Data Quality 9.1, Oracle Weblogic Server Enterprise Edition, Weblogic Server Management Pack, Webcenter Suite and Management Pack, and ASG-Rochade Scanner for Informatica
Application Server: 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Cognos 10 Business Intelligence, and ASG-Rochade Scanner for Cognos
Web Server: 1 x 4 Core Intel Xeon 2.66 GHz, 16 GB Memory	Cognos Connection 10, ASG-Rochade WebAccess
Storage Area Network	Initial Configuration: .5 TB (usable), RAID configuration

Deloitte proposes an economical but capable DW/DSS development environment that leverages LPAR technology to represent the core topology of the production and test environments.

Software Component

Deloitte will employ a Relational Database Management System (RDBMS) or Object Oriented Database Management System (OODMS), a data infrastructure that is easily configurable, role-based with 24 X 7 access to data, and use best in class analysis tools. Deloitte proposes database management component will use Oracle Database 11*g* as the relational database management system. Oracle 11g Release 2 Enterprise Edition delivers industry leading performance, scalability, security and reliability running on the Windows platform. It provides comprehensive features to easily manage the most demanding data warehouse and business intelligence applications. The benefits of using the Oracle platform including:

- Protects from server failure, site failure, human error, and reduces planned downtime
- Secures data and enables compliance with unique row-level security, fine-grained auditing, transparent data encryption, and total recall of data
- High-performance data warehousing, online analytic processing, and data mining
- Easily manages entire life cycle of information for the largest of databases

Data Acquisition and Data Quality

Modern knowledge systems must be designed to respond to changing business environments with the latest and best information and technologies available. Waiting months or years to incorporate new data into a system or to deliver new data to decision makers is no longer an option.

Section Highlight

- A robust, fault-tolerant ETL solution that is always up and always on
- Continuous, flexible sourcing from any source and publication to any target, at any time
- Centralized data transformation and quality control to get the data right and provide a single version of the truth
- Designed to capture, convey, and leverage metadata across the solution

Waiting days or weeks to obtain access to available data is no longer acceptable. Inflexible, fixed-format, technology-dependent data delivery can no longer support customer's data requirements. These are some of the factors that must be considered when designing data warehouse architecture.

The immediate objective of the ETL architecture proposed is to provide the functionality that meets the requirements of the RFP, the first of which is the population of the Data Warehouse/Decision Support System (DW/DSS) with four years of Medicaid data (3 historical and 1 current) and subsequent monthly updates. The long-term objective of this architecture is to lay the foundation for a data acquisition and delivery platform that will be used to implement future phases of the DW/DSS as well as to meet unknown future information needs of the BMS and DHHR overall. This architecture has been designed for performance, quality, flexibility, scalability, and dependability and will allow BMS to integrate all its internal data and to merge data from external sources. The platform will provide timely, accurate, enhanced Medicaid information to increasing numbers of end-users, in a wide variety of formats, for many years to come.

ETL

The following software will be used in the construction, maintenance, and day-to-day processing of data in the DW/DSS solution.

Informatica PowerCenter

Informatica's PowerCenter is an enterprise data integration hub that integrates many diverse tools - and the various user groups - that populate today's enterprises. It enables large organizations to easily transform legacy, relational and other data into reliable information for strategic business analysis and decision making. PowerCenter is responsible for extracting data from operational sources, enriching it for decision support, cataloging it for use and re-use, and delivering it to powerful business intelligence and analytic applications. End users thus will have the power to make more strategic, informed business decisions with comprehensive, accurate, and current information in their hands. PowerCenter is the industry's first metadata-driven product to deliver the essential requirements of an enterprise data integration hub, including:

- Consolidation, cleansing and customization of data
- Integration of operational and analytical resources
- Centralized management of distributed resources

It is a repository-based, graphical, ETL tool which will be used for high-speed movement of data between heterogeneous systems. It is a highly scalable, highly available, high-performance software for accessing and integrating data from virtually any business system, in any format, and delivering that data throughout the enterprise at any speed. PowerCenter has been implemented, and continues to be maintained and expanded in data warehouse solutions in the Health and Human Services sector. It is worthwhile to mention that these implementations have far exceeded client expectations.

Informatica is an industry leader in the ETL tools market segment. PowerCenter represents a new generation of ETL tools that have many advantages over the older, second generation tools. The key advantage is that PowerCenter does not require the development of source code programs to extract data from the source systems. PowerCenter's robust transformation engine does the work of extracting the data from the source

systems and transferring it to the staging area. The transformation engine allows for the creation of complex transformation rules and hence will mostly alleviate the need for creating custom programs. We understand that some of the source data might be stored in proprietary databases and file structures. In these cases, the host systems' bulk load/unload utility will be used to create flat file extracts. These flat files can be transferred to the staging area and then read by the transformation engine. Additionally, PowerExchange, Informatica's other product can also be used to provide fast native connectivity, mission-critical reliability, and secure access to a broad range of data sources and formats. Metadata capture is also made easier by the use of PowerCenter because it will allow metadata to be collected during the transformation process.

Data Quality

Informatica Data Quality

Informatica's Data Quality is a repository-based, graphical data profiling and cleansing tool that allows analysts and developers to derive data rules which can be used to generate set-based or procedural-based profiling, cleansing and auditing mappings. It allows analysts and developers to profile, validate, measure, correct, and audit the quality of their data. In addition, they help automate the creation of role based or procedural-based profiling, cleansing and auditing mappings. The tool also generates valuable metadata that can be made available for reporting, load auditing, alerts, and notifications.

ETL Staging Area

The ETL Staging area consists of physical and logical data structures and the services, applications, and transport mechanisms that allow data to be moved from the source systems to the targets. The proposed DW/DSS architecture is depicted below.

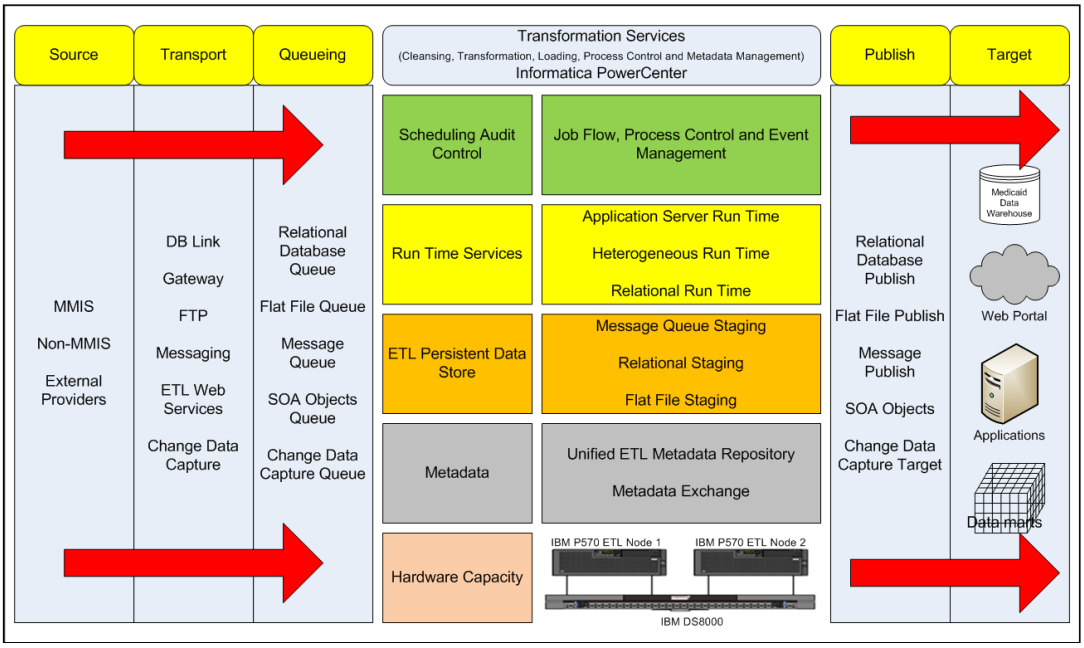


Figure 11-5. BMS DW/DSS ETL Platform.

Queuing (Extraction)

The staging area queue consists of flat files, relational tables, SOA objects, and message queues that store data extracted from heterogeneous sources housed on remote servers. Data will be moved into the queue using various transport methods and accumulated until it is ready to be moved to the transformation area for the main processing. A separate, independent, queuing area provides the following advantages:

- It spares the source systems from intensive transformation processing that can seriously degrade operational performance
- It isolates the transformation processes from network and external database and server failures and eliminates performance degradation associated with transforming data across the network
- It decouples sourcing from transformation thus allowing source formats to be changed with minimal effect on the transformation mappings
- Data can be extracted while transformation and publish processes are executing
- It provides a platform for auditing source data before it is released to the transformation process

Transformation Services (Cleansing, Transformation, Loading, Process Control, and Metadata Management)

Transformation Services consists of source and target tables, ETL repositories, custom process metadata, and services used in the transformation process. Batches of data will be moved into the transformation schema where it will be validated, cleansed, transformed, loaded into target tables, and audited. After transformation completes successfully, the data will then be introduced into the primary publish tables. The following are the advantages of a separate, independent transformation area:

- Improves performance by limiting the sizes of the source and target tables to a single batch and allows the ETL to apply transformations to consistent, point-in-time, snapshots of data
- Validation, cleansing, and transformation are performed only in the transformation area by code that has been designed to for reuse - “Transform once”
- The transformation area promotes the concept of “ETL all the time”. Batches can be transformed as soon as all the necessary source data arrives but held in the publish area until the DW/DSS is ready to accept the data. This will be important as the number of external feeds increases.
- If a transformation fails, trouble-shooting can be performed on the data that caused the problem and not on an ever-changing source. After the errors are identified, the transformation can be corrected and the entire process restarted, thus eliminating the need for error-prone back-out procedures.
- It insulates the data store in the publish area from ETL failure and bad data. Data is not moved until the ETL completes and the data passes auditing.

ETL Persistent Data Store

The ETL Persistent Data Store houses “batch-sized” representations of the queue and publish objects, error tables, process metadata, auditing metadata, and runtime metadata repositories. This Data store will also contain intermediate tables to house the results of the validation, cleansing and multi-step transformation processes.

Run-Time services (Cleansing, Transformation, Loading)

Run-time services move data between external data stores and the staging server, perform the cleansing, transformation, and loading steps within the staging database, provide the platform to run ETL metadata browsers, and support the request, reporting, and notification applications that make up the data delivery sub-system. The most important run-time services used in data are cleansing, transformation, and loading.

Cleansing

The staging area will use Informatica's DataQuality to validate and cleanse the data using pre-built routines.

Transformation and Loading

All transformation and loading will be performed using PowerCenter. PowerCenter transformations will be used to build the majority of the complex code needed for structural transformation and aggregation and final loading. In almost all instances, these transformations can be tuned to improve the performance needed to transform and load the large amount of historical data as well as the rapid transformation needed for the ongoing load.

Scheduling, Audit, and Control

Data acquisition for the DW/DSS will be implemented by hundreds of programs. These programs must run successfully, in the right order, at the right time, every time, so that data is correct and complete. Audit and control services consisting of a combination of tools, and metadata-based audit programs will used to track the execution of jobs. DW/DSS data acquisition will be packaged as multiple self-contained, sub-processes (extraction, cleansing, transformation, loading, and publishing) that can be consistently audited, easily monitored by operations and, if necessary, restarted with minimal operator intervention. These sub-processes may be triggered by events or timing. When they fail they will be configured to notify appropriate personnel.

Each sub-process will consist of one or more complex job flows. These job flows will contain multi-branch execution streams with complex dependencies between execution objects such as PowerCenter mappings, shell scripts, SQL steps, PL/SQL, FTP's, and file events. They can be configured to handle error conditions, abort the job stream, and send notifications in case of failure. The ETL processes will capture metadata about data quality, exception conditions, and database load failures. After each sub-process completes, the ETL will also perform comparisons between inputs and outputs of these processes. This metadata will be interrogated before control is passed to the next step. If one of the audit tests fails, the load will be aborted.

ETL Metadata Management

The staging area metadata layer consists of repositories and services used to collect information about the ETL processes. ETL metadata falls into two categories: detailed design metadata that is primarily useful by ETL developers and runtime metadata that is used in process control. The ETL tools create most of this metadata. Some of this metadata will be collected by the metadata tool and loaded to the managed metadata environment. PowerCenter repositories contain the source metadata used to generate the code for mappings, and workflows. These objects include source and target definitions, transformation rules, packages, procedures, schedules, logs, data lineage, impact analysis, and user supplied narrative.

Data Quality

Introduction

The DW/DSS and the information contained will be used to make decisions that affect the well-being of hundreds of thousands of individuals and the financial well-being of the state. As a result, it is critical that the data delivered by the data warehouse be absolutely right. Data quality is critical to the success of the DW/DSS and its aim of becoming “one version of the truth”. DataQuality is the first and foremost goal of the ETL and it consumes a large percentage of the ETL effort. ETL data quality concerns itself with the correctness of individual data elements, consistency of the data between entities, and the completeness of the data loaded. The following describes the approach that will be used to insure data quality in the DW/DSS.

Relational tables will be included in the Unified ETL metadata repository to capture detailed information about erroneous data and process failure. Each instance of a defect or process failure will be documented in these tables with the location of the element or process, before and after pictures of the data, a description of the problem, and the action taken by the ETL process. These tables will be populated with mappings generated by Informatica DataQuality that will be included in the PowerCenter job streams that execute the historical and ongoing loads. Statistics about data quality will also be collected by the data profiling tool, ETL tools, and auditing processes.

Data Profiling

Data Profiling consists of a collection of defined and ad hoc techniques that look at the data contained in data sources with the goal of determining its correctness, consistency, and completeness. Data profiling collects statistics about data which allow the business to determine whether the data is all there and to derive rules about whether and how questionable data should be included in the data store. These statistics also allow the business to track data quality over time. Data profiling will be used to verify functional requirements of each phase of the project and to assess the risk involved in adding any new data source to the warehouse. Historical data, subsequent load data, and data from external sources will be profiled so that the data can be validated and corrected. The following examples describe the types of methods that will be used in the data quality process.

- Identifying source grains and validating these grains against the data model
- Identifying duplicate data
- Identifying data with missing grain information
- Determining the cardinality and domain values of each data element and matching the domain values against their parent tables
- Identifying missing relationships between dependent entities and establishing a range of default values that accurately describe the problem
- Verifying that the existing data supports the functional requirements and proposing alternatives where it does not
- Identifying correlated data (e.g. Zip code, diagnosis and procedure codes)

- Identifying missing source data by comparing the number of rows and/or records across time periods (e.g., 1M claims occur for Dec. 2008 and 5M claims occur for Dec. 2007).
- Uncovering outlying values

Data profiling is a tedious, iterative process. Informatica DataQuality will be used to automate the simpler profiling tasks. The ETL architect and ETL lead will also use SQL and PL/SQL code to evaluate more complex relationships among the data sources that cannot be addressed by the tool.

Data Quality Reporting

Metadata captured by the DataQuality, audit, and exception mappings will be made available through the portal so that ad hoc queries, canned reports and custom reports can be written to provide information about data quality. The reports can be written to provide summaries with drill-down to the detail level. They can include trending information. The results can be presented in tabular or graphical format. The data access layer can also be used to send alerts when data quality degrades and notifications when a load fails. These reports will be will be exposed through the portal as part of the data delivery process and can be subscribed to and scheduled by internal and external customers. These reports will be used to meet the SLA's described in Appendix 7, Section 3 of the RFP. In addition, DataQuality provides a rich set of tabular and graphical data quality reports containing descriptions of the profile and individual profile objects as well as analyses of aggregates, data types, distinct results, referential integrity, and unique key candidates. Most of these data profile reports provide drill-down capability so that the analysts can view the underlying data.

Data Quality Assessment Techniques

The most commonly used and simplest way to assess source data quality is to calculate the percentage of defective rows in a given data load or the percentage of errors for each element in a given data load. These basic defect percentages are useful measures of quality but they do not assess the overall quality of data on a given row or take into account the relative severity of a particular error. While marital status of a recipient may be a useful element to capture, its omission is far less damaging to claims analysis than a missing date of birth. The following are examples of additional techniques that can be used to gauge the quality of the data in the DW/DSS.

- Percentage and number of rows with errors broken down by type of error (domain value errors, format errors or missing data elements)
- For each data element, the percentage of errors broken down by type of error
- For each data element, the percentage of instances that fall outside defined upper and lower boundaries
- Average number of defective elements per defective row
- Percentage and number of rows in a given table with undefined foreign key relationships
- Percentage of rows with data inconsistencies within the row (e.g., a 3-year old who is married)
- Checks on the numbers of rows and claim amounts over time to determine whether historical data is complete
- Categorizing defects as high-, medium-, and low-impact so that the relative severity of defects can be estimated

The data profiling and address cleansing tools will be used to provide many of the above assessments as well supply statistical information such as median values, average values and standard deviations. In a few cases, complex queries and procedural code may be needed to provide some of these measures.

Error/Exception Handling

Data errors and process failures can be minimized by well-architected ETL but they cannot be entirely eliminated. Some problems, such as surprise changes to external data sources, are out of the control of the DW/DSS. Errors and exception conditions will be categorized as those that can be corrected, those which would cause the individual row to be excluded, and those which would cause the entire load to fail. The business analysts and data owners will determine how these errors should be handled. DataQuality can be used to generate many of these mappings from data profiling results and derived data validation rules.

Audit and Control

The DW/DSS acquisition will be packaged as multiple sub-processes that correspond to extraction, cleansing, transformation, loading, population of internal analytical data marts. After each ETL sub-process is completed, the metadata gathered by the ETL run-time repositories and data validation mappings will be used to determine whether the data can be delivered to the next step. ETL analysts and business analysts will set criteria for determining whether a load is good or not. These will minimally include comparisons of source and target row counts, summarized amounts, uniqueness of grains and keys and referential integrity. Business analysts may also set “go no-go” thresholds based on the expected number of rows in the source and maximum allowable number of defects. The data profiling tool provides functionality that can be used to automate some of the auditing process.

Data Access

Deloitte’s approach to data access leverages a complete IBM Cognos solution. Cognos provides an intelligent and easy to use Business Intelligence (BI) Portal that provides all users a central access point to the BCI-DSS application. The Cognos 10 platform is flexible, extensible, scalable and maintainable and offers an array of analytical capabilities including standardized reporting, ad hoc querying, multi-dimensional analysis, dash boarding, score carding and predictive modeling.

Web Portal

Deloitte will implement the Cognos Connection Web Portal to meet BMS DW/DSS data access related requirements, referred to as the Information Portal (i-Portal). Cognos Connection is an integral part of IBM Cognos BI suite and provides a set of tools and services enabling us to create, manage, and deliver reports. Cognos Connection also provides the ability to:

- **View Public Reports.** Cognos Connection maintains a library of all reports organized based on usage and security.
- **Create and Edit Ad Hoc Reports.** Cognos Connection provides the ability to create, save, edit and share ad hoc reports that are built on shared/custom queries.

- **Schedule and Distribute Reports.** Cognos provides a Scheduler component that can set specific execution times and formats for any reports.
- **Personalize the Portal.** Cognos Connect can be personalized for each business user to store reports in a hierarchical manner, set up personal alerts, change report icons and set up access permissions.

Cognos Connection will be installed on the web-server and will be monitored to validate uptime and accessibility. Cognos Connection provides its own set of systems logs for administrators to review for preventive purposes. Cognos Connection is customizable and can be deployed to meet any standards regarding the look and feel of the web.

Business Intelligence

Deloitte proposes the Cognos Business Intelligence 10 Suite solution enterprise-scale reporting, analysis, score carding, and event notification. Cognos leverages platform independent, industry proven technology, such as Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), and Web Services Definition Language (WSDL).

The Cognos 10 BI architecture features a consistent Web-based user interface for viewing, creating, and administering reports, analysis, scorecards, and events. It has a common dispatcher and supports leading relational databases as well as Online Analytical Processing (OLAP) and dimensionally modeled relational cubes. It confirms dynamic load balancing and provides failover recovery for continuous operation. It also provides a single point of administration, as well as Web-based delegated administration.

The figure that follows depicts all the components of Cognos 10 BI Suite that will be accessible from Cognos Connection Web Portal.

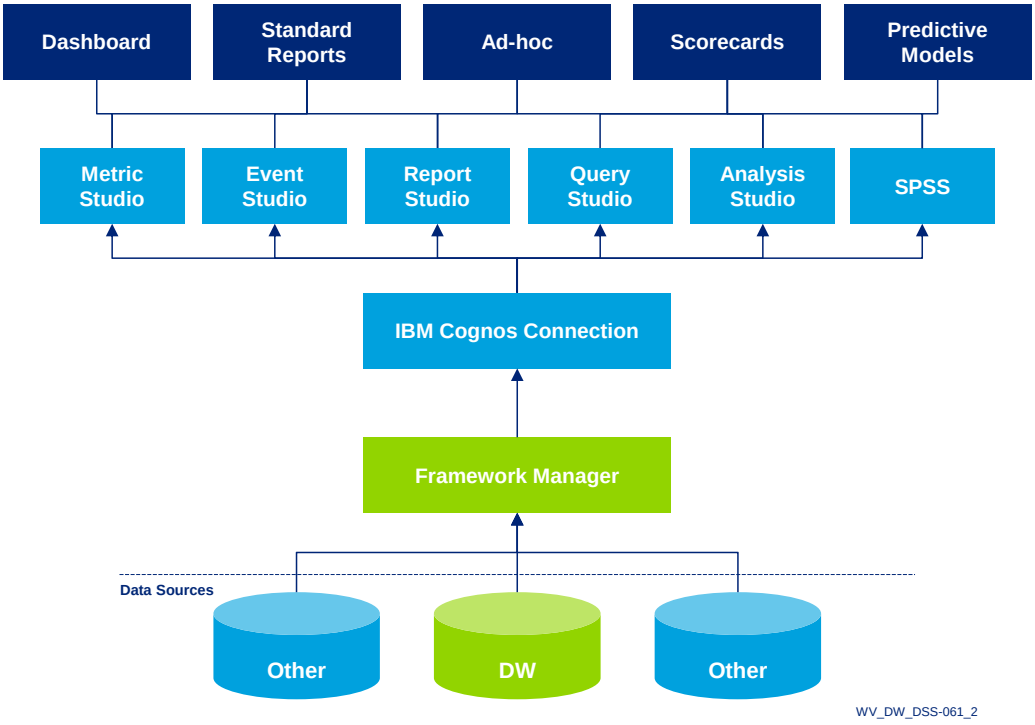


Figure 11-6. Cognos 10 BI Suite Components.

The Cognos 10 BI Suite has number of integral features that will help meet the requirements for the BMS DW/DSS system.

- **Cognos Data Manager.** This component is used for data integration and to connect to an industry standard compliant data source, i.e. Open Database Connectivity (ODBC). With data manager, data can be extracted from source systems and data files, transformed and loaded into the DW/DSS system. This would confirm that BMS is able to access data from external sources in their native forms. Deloitte will implement this tool to help BMS meet all the requirements listed in the RFP (i.e., Appendix 2, Section B.3 – REQ# TEC AC4.1 - TEC AC4.9).

1. **Cognos Administration.** This component is a central management interface that contains the administrative tasks for Cognos BI. It provides easy access to the overall management of the Cognos environment and is accessible through Cognos Connection. Cognos Administration is organized into three sections.
    - **Status.** This section provides links to monitor activities, server status, and system metrics, and change some system settings.
    - **Security.** This section provides links to define users, groups, and roles for security purposes, configure capabilities for the interfaces and studios, and set properties for the user interface profiles (professional and express) that are used in Report Studio.
    - **Configuration.** This section provides links to set up data source connections, deploy IBM Cognos BI content from one content store to another, create distribution and contact lists, add printers, set styles, manage portlets and portal layout, start or stop dispatchers and services, and change system settings.
2. **Framework Manager (FM).** This component is the metadata model development component for Cognos 10 that can be used to create easy to use reports and business presentations of metadata that is derived from more than one source, such as cubes, files or the data warehouse. The metadata model is then published as a package and can be used for query generation. This package will allow users to import a list of data items from different tables and use these as parameters or filter criteria against published DW/DSS data.
3. **Report Studio.** This component is used to create, edit, and distribute a wide range of professional reports. The report authors can define corporate-standard report templates for use in Query Studio, and edit and modify reports created in Query Studio or Analysis Studio. This powerful and easy to use product enables users to create ad hoc queries, cross tab reports, list charts, and graphical reports by just a click and drag functionality. Reports built with this tool can be printed, saved, emailed or faxed in various different formats such as Excel, HTML, PDF, CVS and XML.
4. **Query Studio.** This component is used to quickly design, create and save reports to meet reporting needs not covered by the standard, professional reports created in Report Studio. This tool is most commonly used to meet ad hoc reporting needs as it captures the metadata information. Users can drag and drop data elements to Query Studio and see the underlying table data.
5. **Analysis Studio.** This component is used to explore, analyze, and compare dimensional data. Analysis Studio provides access to dimensional, OLAP, and dimensionally modeled relational data sources. Analyses created in Analysis Studio can be opened in Report Studio and used to build professional reports.

6. **Event Studio.** This component is used to set up agents to monitor data and perform tasks when business events or exceptional conditions occur that must be dealt with. These agents can publish details to the portal, deliver alerts by email, run and distribute reports based on events, and monitor the status of events and system logs for preventive purposes.
7. **Metrics Studio.** This component is used to create and deliver a customized score carding environment for monitoring and analyzing metrics through different business processes. Users can monitor, analyze, and report on time-critical information by using scorecards based on cross-functional metrics.
8. **Map Manager.** This component is used to create custom maps that can be used in reports to display key business data in geographic context. This mapping software can import maps from third party sources into Report Studio and provide multi lingual map support. Drill downs on regions add to the usability and impact of the reports. Map Manager can be integrated with GIS (Geographic Information Systems) software to provide geographic dimension to the location related business data.
9. **SPSS Modeler.** This component is used to create predictive models to discover trends and patterns in both structured and unstructured clinical and diagnostic data to better understand what factors influence positive outcomes.
10. **IBM Cognos Quick Tour.** This link is provided on the Cognos Connection Web Portal that provides all helpful documents, glossary of terms and learning sessions for all features integrated in the Cognos BI Suite.
11. **IBM Cognos Homepage and Tool Bar.** The Cognos tool bar has various tools to help users organize their reports structure, define report output formats, choose report delivery formats, manage report folders, etc. Cognos Home page serves as a library of all reports and queries with options to perform various actions on one or all of the reports. These actions could be scheduling the report, defining run formats, executing the reports or launching them in respective studios for making any updates.

Data Delivery

The ultimate purpose of a data warehouse is to make information readily available to the people who need it in a format that they can use to for decision making. While BMS maintains the data that supports the West Virginia Medicaid program, other agencies or outside vendors may need subsets of this information so that they can integrate it with their own data for specialized reports and analysis. The immediate goal of the proposed data delivery architecture is to provide transformed historical and ongoing data on a timely basis to BMS and their users. These downstream feeds include internal analytic systems, and flat file extracts for external entities.

Section Highlight

- A better, more accurate, more efficient method for serving internal and external data requests
- Data however you want it, whenever you want it, wherever you want it

The long-term objective of this architecture is to build a data delivery platform that will get BMS out of the extract business. In order to best serve both internal and external requests for “large volume” data requests, Deloitte proposes the following.

Request

All requests for data delivery will be made through the Cognos Connection Portal described in the Data Access section above. Authorized information consumers will be able to access a web page that directs them to the Automated Tracking System (ATS) application. ATS allows users the ability to define the content of their data extracts, select the format in which the extracts are to be delivered, and request a scheduled run date. The content may specify data elements, aggregations, and filters. The formats may include flat files, comma-separated values (CSV) files, Microsoft Excel and XML. ATS captures requestor information, time of request and allows the requestor to assign a priority to the data request.

Assign

Based upon the priority and due date, the data request is assigned to an analyst to develop the required Structured Query Language (SQL) to fulfill the request. The analyst will schedule this SQL to run during off hours (i.e., overnight) as to not impact performance of the BCI-DSS environment. The result set will be thoroughly tested by the analyst before final submission back to the requestor. During the development and test period, the analyst will continue to update ATS to keep the requestor informed of progress.

Notification

Once the data is in the required format, the analyst will contact the requestor to inform them and determine the delivery mechanism of the data. Upon receipt and validation of the data by the requestor, the request is closed out in ATS.

Request Reporting

ATS provides reporting functionality that provides details on all requests, requestors, request priority, dates along with other descriptive components of the request.

Managed Metadata Environment

Managed Metadata Environment

Deloitte proposes leveraging ASG Rochade as the metadata solution for the DW/DSS initiative. Rochade will enable BMS to capture and view business requirements, transformation logic, and business rules in the integrated metadata environment. Rochade will provide BMS with the agility required to facilitate fast business decisions while delivering on the key drivers.

- **Traceability.** The ability to track the lineage of key information objects, their definitions and to determine the origin, transformation and current location of those objects in support of directives.
- **Usage.** The ability to track metadata related to data life cycle events such as when metadata is created, read, updated and deleted in a single book of record will make it easier to monitor data usage.
- **Data Integrity and Quality.** Rochade's Metadata Management allows BMS to diagnose and pinpoint data integrity and quality issues.

ASG-Rochade is a proven “industrial strength” [redacted]. Rochade can capture, store, configure, and relate information assets from many diverse systems and platforms including mainframe and distributed platforms, applications, ETL processes, enterprise models, BI and business processes and terms. It can also disseminate information in online views, reports, graphics and pop-up definitions while in any desktop application.

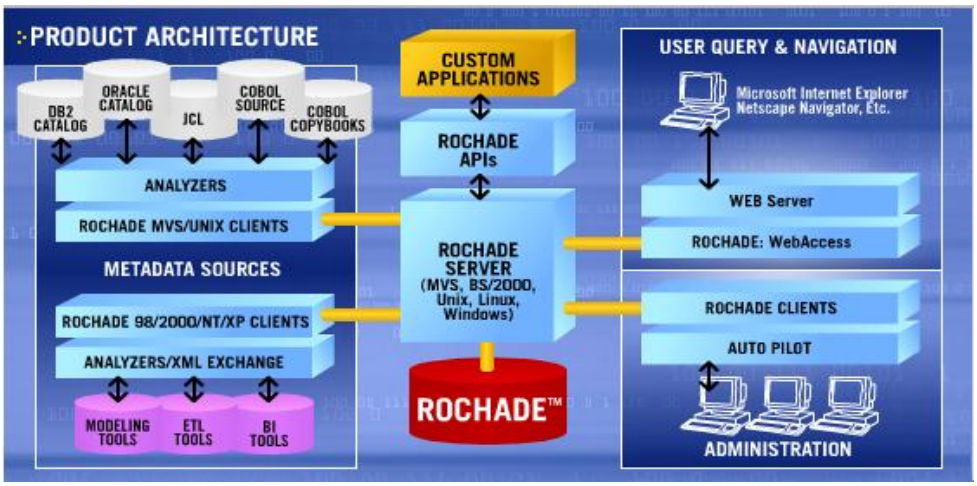


Figure 11-7. Rochade Solution Architecture.

Rochade’s broad set of tool-agnostic interfaces for information exchange do not depend on third party vendors for upgrade support. The database is extremely portable, open, and provides an ODBC connection as well as federation capabilities. Due to the increasing demand for business metadata support, Rochade also includes an easy-to-understand user-interface for non-technical business users. Rochade has an extensive array of information collection, viewing, and reporting capabilities available to support complex heterogeneous environments. Inevitably, new projects may introduce additional requirements to gather information from sources that have not been encountered before. Rochade provides a range of methods for creating innovative collection interfaces. ASG is continually improving these features through the adoption of new interface definition standards as they emerge.

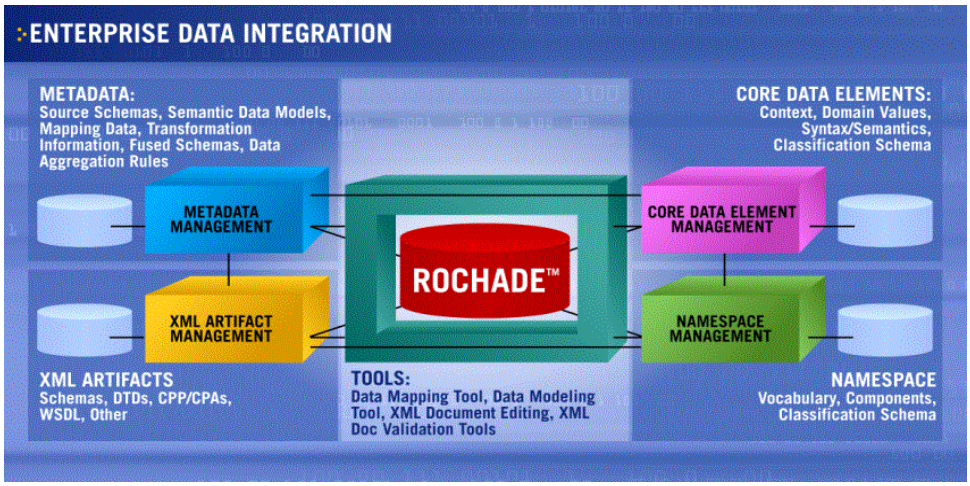


Figure 11-8. Enterprise Data Integration.

Rochade optimizes the value of business-critical Data and is a powerful metadata management system that supports both business and technical metadata throughout the enterprise. It provides a common user interface semantically geared towards the language of your organization and is supported by an integrated database of information systematically gathered and synchronized from source and target systems throughout the enterprise. Powerful core features target the consumption of logical and physical information and relate these elements to business glossaries, KPI's, and data privacy rules. All metadata in Rochade is managed and integrated by means of a repository schema or metamodel, called a Repository Information Model (RIM).

This network/object network database is optimized for metadata management in a preference to a relational DBMS. The reason for this is that unlike a typical data structure within a relational DBMS, the metadata structure within a repository includes complex interrelationships among its hundreds of thousands (often millions) of items. Users must be able to navigate these relationships in any direction, from any point, at any time. Relational databases are optimized for data storage integrity, and all relationships are implicitly defined through foreign keys. Although this sometimes minimizes the workload for creates or updates, it maximizes the workload at retrieval or query time. To compound this issue further, the implicit foreign key relationships are in a single direction, so that at "ad hoc query time" all backward relationships must be derived without any key information.

The underlying database structure is object-based, fundamentally managing information within the repository at the attribute level. Each attribute object is linked with its parent item and to all items referenced within the content of the attribute. Storing objects at the attribute rather than at the record level gives the database much more flexibility for reconciliation and versioning. The application of the "reuse wherever possible" objective is supported in that if any given attribute value is actually the same among two or more objects, then that attribute value is only physically stored in the database one time and shared by all the objects which have that attribute value in common.

Rochade's repository management functions are powerful, robust, and designed to handle vast quantities of metadata, harvested from multiple sources, linked in scores of ways, while administering and maintaining security, versions, configurations, and user interfaces. Rochade is ideally suited for integrating diverse tools, repositories, and data stores feeding an metadata repository so that all metadata is managed in a cohesive manner that helps confirm integrity and consistency.

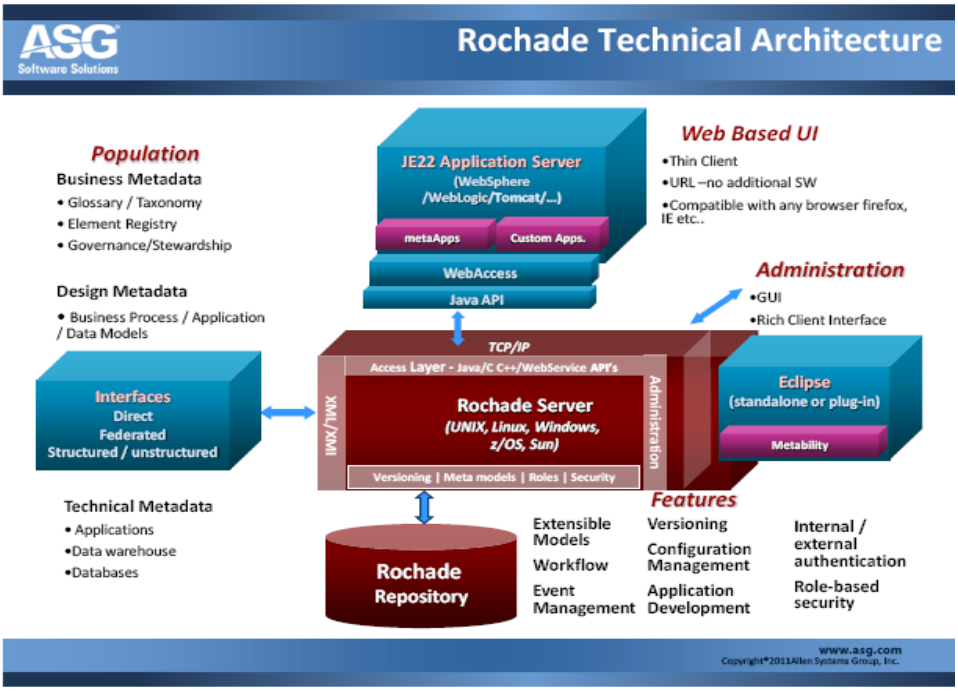


Figure 11-9. Rochade Technical Architecture.

Rochade is further unique in its ability to support business/technical user understanding across the enterprise by providing a customizable abstraction layer on top of the repository. Users can use this to find information using context structured taxonomy with which they are familiar. Users never need to know they are interfacing with a repository, which not only empowers these users, but also removes support burden from the IT staff. It is common for Rochade customers to have thousands of users interfacing with the product. Rochade's Web-based interface supports full role/permission-based read and write access to the repository, opening up many options for updates and other work to be easily accomplished from anywhere a Web browser exists.Rochade allows application access functionality being grouped and granted by business role or job function. Following security features are supported in Rochade:

- Each user in Rochade is identified with unique user id and password. Users belong to groups such as administrators, deputies, users, etc.
- Rochade supports Role-based Access Control (RBAC), which allows granting privileges for user's role and job function.
- Rochade supports different levels of authorization. A Rochade account can be assigned to a group of users (group authorization) or single user (individual authorization).
- Rochade supports LDAP/Active Directory for authentication.

Data Model

Deloitte proposes using Computer Associates' Erwin product for all data modeling activities during development, implementation, operations and enhancements. ERwin provides the following features and benefits:

- **Visualization of Complex Data Structures.** Provides a simple, graphic display to visual complex database structures in an easy-to-manage interface.
- **Design Layer Architecture.** Flexible to create multiple model layers, from logical to physical, to even higher-level models. Users can create logical and physical models that are completely separate, or create logical and physical models that are linked, allowing you to choose the implementation style best suited to your needs.
- **Standards Definition.** Reusable standards improve an organization's ability to develop and manage their information assets in a cost and time effective manner. ERwin supports the definition and maintenance of standards through reusable model templates, the domain editor, the naming standards editor and the data type standards editor.
- **Large Model Management.** Manage large enterprise-level models through subject areas and diagrams. These graphical views and model visualizations facilitate information exchange and collaboration among the different stakeholders in an organization. In addition, advanced features such as auto layout, on-demand user interface components, and "bird-eye" navigation allow you to easily visualize large models.
- **Complete Compare.** Automates complete bidirectional synchronization of models, scripts and databases, compares one item with the other, displays any differences and permits bidirectional selective update. If model changes are targeted for a database, ERwin can automatically generate a database ALTER script, as desired.
- **Database Design Generation.** Create database designs directly from visual models, increasing efficiency and reducing errors. Industry-leading database support includes optimized referential integrity trigger templates and a rich cross-database macro language, allowing modelers to customize triggers, scripts and stored procedures. Customizable templates facilitate the generation of a model's complete physical design and definitions.
- **Data Warehouse and Data Mart Design.** Supports data warehousing-specific modeling techniques (such as Star Schema and Snowflake dimensional modeling), thereby optimizing the data warehouse for your performance and analysis needs. It also captures and documents a rich set of information about the warehouse, including data sources, transformation logic and data management rules.
- **Integration and Metadata Exchange with Other Tools.** Integrate ERwin with other projects and tools with import or export from a wide variety of sources, including BI tools, MDM hubs, other data modeling tools, ETL tools and Unified Modeling Language (UML) tools.

System Construction and Testing

Our BMS DW/DSS project approach to system construction and testing your solution is to provide BMS with the platform to be a leader among its peers. That is, we will work in a collaborative style to shape innovative solutions throughout the life of the BMW DW/DSS project.

Construction and testing collaboration is critical to the success of the BMS' DW/DSS solution. Deloitte will work closely with BMS in implementing our construction and testing approach to focuses on building sustainable and predictable, end-to-end processes to support the delivery of our high quality solutions. This collaboration will allow BMS and our team to shape the testing phases of the engagement and to innovate for the future.

Construction

Construction is the culmination of all the project work completed through the requirements and design process, and it utilizes the inputs from various phases to begin creating the DW/DSS solution. Construction exists as a phase in the overall project management methodology, [redacted].

Intertwined in this project is the need for the generation of new ideas and forward-thinking by bringing together IT professionals that provide experience and insight from their focus areas. Deloitte processes are Capability Maturity Model Integration (CMMi) Level 3 certified and we bring this experience, along with our certified project managers and Information Technology Infrastructure Library (ITIL) professionals, to the DW/DSS solution implementation. Many of our professionals have worked on information management projects in our State Health practice to deliver DW/DSS integration solutions. All these talents combined into one project will allow us to deliver the best solution for BMS.

The RFP lays out a series of requirements that help define how the development process will integrate with the overall project and drive the creation of the DW/DSS solution. We believe that our project team will accomplish these goals along with fulfilling BMS's needs for development through the following mechanisms:

Component	Purpose
Scalable Environments	We believe that planning for growth is important and we also understand that BMS has a specific need to scale the DW/DSS. Therefore, we are planning hardware, software, and storage scalability factors into the development environment and other areas of our proposed DW/DSS solution.
Standardized and Extensible Coding Platform	Deloitte has invested time and effort in developing application frameworks to support development projects such as the DW/DSS. We bring these frameworks to our clients as a set of foundational classes that support the coding process and provide a common base of code from which a development project can begin. When our project is complete, we leave these frameworks with our clients so that they can continue to benefit from the framework as they continue their coding efforts into the future.
Collaboration with BMS Staff	Deloitte believes heavily in keeping our clients involved in the development process. This allows our clients to support construction of a better product, keeps "surprises" to a minimum, and fosters better knowledge transfer to our clients. We will actively work with BMS to define people needs and skills from your staff, including code reviews and testing coordination, so that the DW/DSS project is a success.
Coding and Documentation	Integration of a development framework also serves as a set of standard coding practices for the DW/DSS project, thereby providing a higher level of quality in the development of software components. We will discuss how the guides and documentation will lead to more detailed system documentation and higher quality deliverables.

Component	Purpose
Requirements Traceability	One of the tenets of the CMMi process for Level 3 compliance is the ability to trace back to requirements from code or system changes. This provides greater transparency and the ability to assess the impact of system changes when requirements are altered. These processes thereby increase the overall quality of the solution by providing enhanced insight into what needs to be tested, changed, or investigated when requirements change.

Employing these leading practices allows for our team to create planned and testable code that can be directly tied to a test plan and test cases for the DW/DSS solution.

Testing System Requirements

As with any technology solution similar to the one proposed for the DW/DSS project, preparing and testing the features and functionality of the new solution early in the development life cycle not only improves quality and performance, but also dramatically cuts the cost of finding and fixing errors and associated service delivery problems. Our testing approach is part of the larger quality management thread within our project management plan and is repeatable to accommodate the multiple phase strategy.

A Medicaid Data Warehouse must also account for the processes and procedures of the supporting Medicaid Management Information System (MMIS), in order to provide a fluid, accurate, predictable and reliable data set. Many of the difficulties arising in a project of this type come from communication gaps and misunderstandings over data. These difficulties then often manifest themselves in the testing process, when they are often much more difficult and time consuming to correct. This is why we believe that testing is a process that begins with the initiation of business requirements and requires extensive coordination.

Testing Approach

Managing a testing effort using a multiple release strategy requires a highly disciplined, methodology-based approach to quickly and efficiently recognize, track and resolve issues that may arise. An effective framework for the execution of testing is as important as documented processes and standards (best practices) which must be leveraged and deployed consistently. Our approach to testing revolves around the recognition that quality should be built in, not tested in.

Testing Process

Organizations often struggle to attain their desired level of testing maturity due to a number of factors ranging from lack of executive support to too broad of an approach. We address these factors through the implementation of our project management methodology, a core component of our overall approach to quality that is based on industry standards and best-practices for project delivery. Leveraging this methodology provides a solid foundation with proven results in order to develop testing capabilities quickly and effectively. The methodology comes equipped with pre-existing process flows, templates, samples and procedures that enable quick setup of the testing process. These templates include Medicaid Data Warehouse implemetations that our team has worked on in previous engagements, such as the PROMISe Data Warehouse for Medicaid claims and pharmacy in the Commonwealth of Pennsylvania.

Our approach to quality begins in the upfront phases of the development life cycle. Our testing practitioners will work with BMS partners and subject matter experts during the early stages of the project to make sure requirements traceability is designed into test planning and test execution activities. When requirements are complete, they will be used as critical input for drafting user acceptance testing scenarios. These scenarios

will be used by the development team and the testing team for test case creation. The requirements and test case traceability must be supported through a tight change management process that integrates with other facets of the project control process.

During test execution, test results will be logged and the associated defects will be identified and traced back to test cases and hence requirements. In past engagements, we have experience using a number of tools and we can work with BMS to select the best tool that fits the needs of the project. Given the nature of Medicaid data and a focus on data accuracy, we believe that the initial deployment of the DW/DSS solution should use production data to test the deployment of the ETL mappings.

The following figure provides a detailed depiction of the test phase in Deloitte project management methodology. This shows how testing is an integrated component of the larger project, rather than just a self-contained phase in the methodology. Proper testing requires up-front planning and setup, input and oversight from the quality management processes, and test execution in multiple environments. This process is key in Medicaid Data Warehouse development projects that extract from multiple data sources in disparate systems and therefore must have verified data loads.

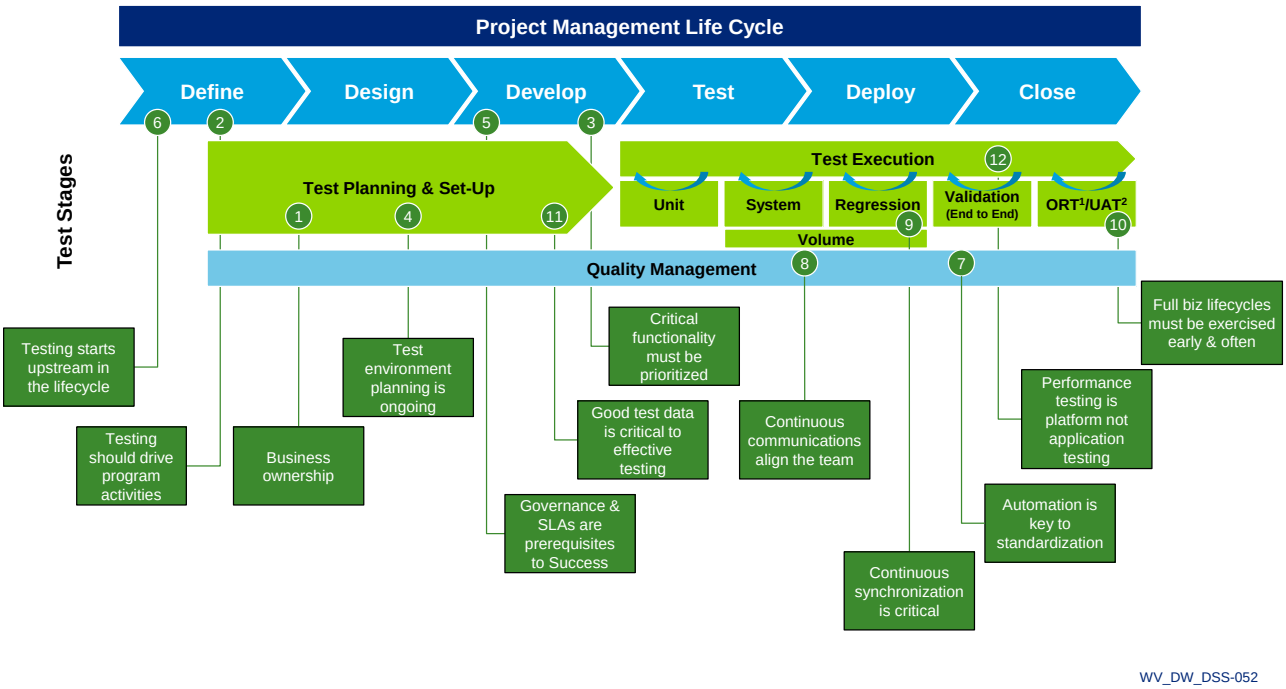


Figure 11-10. Integrated Testing Process.

Our testing approach focuses on building sustainable and predictable, end-to-end processes to support the delivery of high quality solutions in each phase. As shown in Figure 11-10, our testing framework within the project management methodology has been developed with flexibility in mind and demonstrated to be repeatable and consistent. The framework is independent of platform and business models and is flexible enough to be customized to any delivery model or platform. In addition, our framework is based upon industry leading testing practices and has been continuously updated based on previous experience and knowledge gained through years of successfully managing large-scale integration and testing initiatives.

Creating Effective Test Plans

Deloitte will work jointly with BMS to develop a detailed test plan that describes the framework that will be followed to support the preparation, execution, and management of test phases and activities, tailored specifically to DW/DSS deployments. The test plan document is developed as an output of the preparation process and is required to be approved before entering the test execution stage. This test plan is a component of the larger quality plan and provides specific details on how testing will support overall quality in the project. The test plan should contain elements similar to the following five areas:

Section	Description
Test Phase Overview	This section describes the purpose of each test phase, the definition, scope, and the entry and exit criteria for the test phases
Test and Quality Management	This section outlines the overall test schedule, team and organization, test environment requirements, communication plan, test tools and configuration, test training plan, test case management, issues and defect management, and the configuration management schedule; including providing a mechanism to coordinate the testing efforts into the overall project Quality Plan
Re-Testing Procedures	This section focuses on the processes that examine, re-define and re-initiate testing procedures that have not met the established criteria for completion during a test case. Included in this process will be updates to the detailed design models, definitions, metadata and other system components that occur as a result of testing changes
Test Cases and Scripts	This section defines the organization and layout of the test cases and scripts for the testing process.
Templates	This section includes the standard templates that will be used for reporting and test case management, as well as reporting the number of defects encountered during unit and system testing with the cause for each defect. Included in these templates are the checklist components describing the procedures and outcomes for the successful completion of unit and system integration tests
Definitions and Acronyms	This section will document basic test definitions and acronyms specific to this environment

We make testing a success by bringing together strong proficiency, tools, and methods; deep industry knowledge; and insight into your operations and systems. Prior to the commencement of testing, we will submit to BMS a test plan for BMS's review and approval. Having a thorough and comprehensive test plan is a key factor for measuring the success of testing.

Test Cases and Test Scripts

Test cases are derived functional tests that validate business requirements or scenarios from the stated design of the system. A test case or several cases verifies the output of the construction process aligns with the stated design, which in turn meets stated requirements and therefore produces the desired outcomes. A test case includes the purpose of the test, any specific setup or configuration needs, detailed test steps (i.e., test scripts) of how to perform the test and the expected results or success criteria for the test.

Test scripts should include detailed technical information for execution of the test, such as log-in credentials, SQL statements, report IDs, portal page, or other fine-grained information. While test cases define the business requirement or scenario addressed, the test script provides evidence that the stated functionality is adequately addressed.

Test cases are developed using input from the requirements and design teams in terms of business rules, specifications, use cases, system logic, processes and procedures defined for the system. Once these items have been harvested, the testing team meets with BMS to layout the planned testing and gathers feedback on additional testing to perform. Once the scope of this testing is defined, the testing team can then begin to

use automated testing tools to develop the steps for each test script assigned to the test cases. The test scripts may be simple steps for logging into the portal and verifying the security access, to much more detailed ETL processing logic developed through SQL statements and coding logic to verify transformations are performing correctly. In this manner, tools to support the development and collection of test scripts vary by the test case, but the test cases and scripts themselves are centrally stored and managed for reporting on status.

As test scripts are finalized, our team will work with BMS to validate the size and scope of the test scripts, in order to determine their testing effectiveness for the stated functionality. Prior to the commencement of testing, we will submit to BMS the test cases and test scripts for BMS's review and approval. There should be a test case tied to every requirement to confirm that all requirements were designed, developed, and subsequently tested, thus giving traceability of the system functionality.

Testing System and Dedicated Test Environments

The RFP has stipulated the need for a dedicated testing environment that is used for specific functions associated with the testing process. The testing environment should be tightly controlled as to not introduce any variation into the test results. If a test case is run more than once, with nothing changing, then the result should be the same each time. Therefore, it is critical to the testing success to have an adequate environment to support the multiple levels of testing. To accommodate all testing phases, we advise the following environments be available. In the following table we list the requirement provided in the RFP for these testing environments and a description of how we will meet the requirement.

Testing Execution

The entrace criteria to begin testing is BMS approval of a test plan, test cases, and test scripts. Once these approvals are received, Delotite can begin executing and recording test results.

Testing will focus on verifying the interface of discrete modules with one another. In other words, the purpose of testing is to validate that different system components "talk" to each other, pass data to each other as designed, and process return codes as designed. These tests will check if the data is being correctly processed and transmitted across various tiers of the system. Sometimes these components may be outside the system boundary (e.g., an interface with a legacy system.)

Manual test scripts will be written to test multiple integration blocks. An integration block is a series of code modules that act as one and interface with other code modules. Some examples of manual test scripts are:

- Tester enters data on a web page and clicks a button to run the data. The tester should receive correct notification of a successful completion of the data. The Tester should be able to retrieve the data and verify that the results are correct. This test validates that presentation code modules can "talk" to application layer code modules which in turn can "talk" to database code modules.
- Tester invokes a batch job to create data for a provider. The Batch Monitor should correctly invoke the batch job and show batch status. After the batch job is done, the Tester should be able to verify that the data created for the provider matches that in the database.
- Tester enters invalid address on a web page. The system calls an address validation software API and gets error information. The error information is displayed on the web page.

Execution of these test scripts will be done by the testing team to validate the different interface components are interacting together correctly and produce appropriate results. The testing actions will be recorded using an open source testing tool such as Eclipse. Eclipse is open source software that Deloitte has used on other projects. Eclipse is a development and testing platform comprised of extensible frameworks, tools and runtimes for building, deploying and managing software across the life cycle. Moreover, because Eclipse is open source, there are no associated license fees. This tool also provides the capability to centralize the storage and reporting of testing results to users, therefore allowing our team and BMS to jointly review testing progress. During test execution, weekly and possibly daily meetings will be established at appropriate times in the schedule to review testing procedures, manage issues and resolve defects. At the completion of testing Deloitte will develop a test summary report for submission to BMS. This summary will also provide an opportunity to develop a mutually agreed upon mechanism for measuring the successful execution of all testing. The test summary report will summarize:

- All testing has been performed in accordance with the approved test plan
- The number of test cases, test scripts that were written, executed and outcome of all tests
- What data was loaded into the test environment
- That all defects discovered during testing and ranked as critical have been resolved to the best of our knowledge
- Our methodology for documenting and ranking defects and deficiencies discovered
- The process for updating and finalizing the test summary prior to implementation

Logging Defects

Through the course of testing, quality analysts will leverage Deloitte's Automated Tracking System (ATM) Test Defect Report (TDR) module. Defects may be filed during development or during subsequent testing phases by project resources. Tracking of defects is primarily accomplished through ATS via a TDR form tailored to capture relevant information about a suspected system deficiency. For the purposes of defect prioritization, the defect form includes a severity and environment field. The severity field indicates the level of impact on system functionality while the environment field associates the defect with the environment in which it exists. These two fields are used together as the primary source for determining the priority of the defect.

Once the TDR is created, the defect is tracked through a field that indicates the defect's status. The status represents the progress being made to understand and resolve the defect. Chronological history of changes to each defect is tracked by ATS and available for review. In addition, a notes tab is available within the TDR, which provides responsible parties the capability to capture detailed information, clarify findings and resolutions, and attach external reference material. When defects are addressed by the development team, the defect is updated and the associated test case(s) and test script(s) are reinitiated through the testing process. This process validates that all tests are processed and addressed in the testing cycle to an acceptable level of satisfaction.

During User Acceptance Testing (UAT), BMS participants will be given access to ATS in the event that defects are discovered during UAT activities. UAT participants will be given an overview of how to use the ATS tool, how to document a perceived testing defect, and how to rank or prioritize the level of the defect.

As part of our testing approach, the testing team will hold weekly status meetings and review defects discovered during the testing process, the severity of the defect, proposed solution for resolving the defected and timing for retesting.

User Acceptance Testing (UAT)

Deloitte understands that the ultimate goal of the system is to meet users' expectations as defined in the requirements and design phases of the project. Our team will work towards providing BMS users the opportunity to use the system in a separately controlled environment so that they can provide their feedback on the quality of the system. An initial test summary will be provided, in accordance with the approved test plan, to BMS before the commencement of UAT.

Our team will work with BMS to support your development of user acceptance test cases, supporting BMS' resources using the testing tools defined for the project. Our team will provide BMS with the test cases developed for other phases of testing to support the development of UAT cases. User acceptance test cases will be run by BMS in a separate, tightly controlled environment. BMS representatives will report each problem detected in the testing process through ATS, as referenced above, through the same process as the testing team utilizes. The BMS team will validate problem report fixes once they are resolved by the development team. Our experience with building applications of similar size and complexity demonstrates that buy-in from our clients is reinforced when their resources actively engage in the testing development and testing implementation process.

Summary

Deloitte knows that testing is critical to the acceptance of a complex project. It literally is the place where "the rubber meets the road" in terms of the business requirements being met by the developed solution. We believe our testing methods, tools, and experienced personnel provide a significant value proposition to BMS and that in working with BMS we can test and deliver a DW/DSS project that meets BMS's needs for the 21st Century.

Security, Privacy, and Confidentiality

Deloitte will comply with all security policies and procedures of BMS and the WV Office of Technology. Also, Deloitte will comply with the baseline security controls for moderate impact information systems as put forth in National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 3, as updated May 1, 2010.

The security design for the DW/DSS solution and associated policies and procedures will address all areas of the final HIPAA Security Rule and the elements of the HITECH Act that are currently in effect. Functional and technical security requirements will be developed based on mandatory requirements from the RFP, requirements that we recommend based on Federal and State regulatory requirements, and security leading practices such as National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) and International Organization for Standardization (ISO) standards.

Approach

Deloitte's DW/DSS security, privacy, and confidentiality plan will be developed based on the requirements stated in the RFP and additional areas based on regulatory laws and security standards from NIST and ISO 27001/27002. The approach to the security solution is outlined below by each applicable security area as defined in the RFP. Deloitte has extensive experience in developing security solutions and takes a risk management approach to designing this security solution. Some design elements to address Health Information Technology for Economic and Clinical Health (HITECH) regulations not yet finalized and in effect, such as the final rule for accounting for disclosures, which will be designed to acceptable risk levels as jointly approved by BMS and Deloitte.

Deloitte, in proposing to design, develop and implement BMS' DW/DSS solution, would accept the responsibility to be the custodian of State of West Virginia ePHI. This information is covered under the Health Insurance Portability and Accountability Act (HIPAA) and the Electronic Health Record provisions of the HITECH Act.

Deloitte recognizes that with the passage of the HITECH Act, business associates are required to comply with the HIPAA Privacy and Security regulations as if they were a covered entity. Deloitte will implement a security program encompassing logical and physical security of the data entrusted to us. Logical security efforts include network, data and application security.

Deloitte will assign roles and responsibilities in order to implement and maintain the DW/DSS security solution. Two key positions that will shape the security framework are the Information Security Officer and the Project Security Architect. The definitions of the responsibilities for each position are outlined below:

- DW/DSS Information Security Officer (ISO):
  - Develop, manage and maintain the Security, Privacy and Confidentiality Plan
  - Develop and implement information security policies, standards, and procedures to protect the information maintained in the DW/DSS solution
  - Work closely with project team and BMS personnel to facilitate that security measures are implemented to meet requirements
  - Confirm appropriate information security awareness training is included in all training plans and communicated to all DW/DSS users, administrators, and where appropriate third party individuals
  - Set up metrics to track compliance with the Security, Privacy and Confidentiality Plan and report to the DW/DSS Project Manager
  - Report any security and privacy non-compliance to DW/DSS Project Manager
  - Evaluate new security threats and counter measures that could affect the DW/DSS solution and make appropriate recommendations to the DW/DSS Project Manager
  - Investigate and report security incidents as defined by the DW/DSS and BMS incident response plans
  - Confirm that appropriate actions are taken if security violations occur
  - Be aware of laws and regulations that could affect the security controls and classification requirements of DW/DSS information

- Security Architect:
  - Collaborate with key BMS and project team personnel to design the security solution for the DW/DSS environment based on approved security requirements
  - Assist the DW/DSS ISO to develop and implement information security policies, standards, and procedures to protect the information maintained in the DW/DSS solution
  - Work with the DW/DSS Project Manager to develop the security section (i.e., security related tasks) of the overall project schedule
  - Develop security related test cases that map back to security requirements
  - Lead security related testing processes in conjunction with the DW/DSS project testing team
  - Assist the ISO in developing security related training material
  - Develop the security section of the DW/DSS implementation plan
  - Develop security section of the turnover plan

Data Security

The final HIPAA security rule requires that electronic Personal Health Information (ePHI) transmitted over open networks must be encrypted. To qualify for the HITECH Act's "safe harbor" provisions, in order to avoid reporting data breaches, requires that ePHI in motion and at rest must be encrypted using FIPS 140-2 compliant algorithms and processes. All certificate and key management processes for encryption of data at rest and data in motion will be FIPS 140-2 compliant where possible to qualify for the HITECH safe harbor provisions of the Breach Notification Law.

Data in Transit

Encryption of data in transit occurs through three different processes:

- Portal through HTTPS (SSL)
- Virtual Private Network (VPN) through either SSL VPN or IPSec Tunnel
- SSH File Transfer Protocol (SFTP)

Encryption for all data in transit processes will use FIPS compliant algorithms, where possible, to comply with HIPAA regulations and qualify for HITECH "safe harbor" provisions of the Breach Notification Law.

Data at Rest

A mandatory requirement in the RFP was to encrypt sensitive data at rest, including in the DW/DSS databases in all environments (i.e., production, test, development and disaster recovery). This will be accomplished by deploying Oracle Transparent Database Encryption (TDE) to encrypt sensitive fields in the DW database. Oracle TDE is Oracle's solution for transparently encrypting Oracle database data before writing it to disk, protecting sensitive application data from direct access at the operating system level and on removable and backup media. Laptops and desktops that will extract data from the data warehouse will need to have hard drive encryption software installed, which will be a requirement of the BMS' MIS department to

address and deploy. Deloitte will review this requirement with the MIS department, to confirm its solution is FIPS compliant. If not, Deloitte would recommend deploying Microsoft Bitlocker, according to FIPS (NIST) guidelines, in order to qualify for the HITECH safe harbor provisions. It is not recommended to store ePHI on removable media except to support backup operations. Backup drives will employ a FIPS 140-2 compliant encryption solution so that sensitive data residing on backup tapes is encrypted. A Business Associate Agreement (BAA) must be signed with the vendor that handles the offsite storage of backup tapes indicating that the vendor will comply with all HIPAA and HITECH regulations in regard to transporting and storing the backup tapes containing ePHI data.

Data Access Control

The integrity of the DW/DSS's data is maintained by a combination of tools and processes. Access control to data is managed by three major components:

1. **Database Controls.** Data integrity in the DW/DSS Oracle 11g Database will be enforced through the use of Oracle Enterprise User Security (EUS), database roles to grant access to tables, restricted access roles to filter access to restricted data using Oracle Virtual Private Database (VPD), and themes that are used to provide a "container" for a collection of oracle object (i.e., tables and views) privileges.
2. **Identity and Access Management (IAM) Suite.** Oracle IAM products will provide identity and account life cycle and role management, web access management (i.e., authentication and coarse-grained authorization) and Directory Services to store user related information.
3. **ETL.** Referential Integrity (RI) is a database concept mandates that all values of a specific table attribute exist in a corresponding code table or parent table. When RI is enforced, only existing RI attributed values of can be inserted into RI columns. This insures consistency between related tables thus improving the quality of the data and the results of operations performed on the data. Since a data warehouse often has little control over the data that feeds it, the ETL must include programs that address RI problems. RI changes and problems can be identified within several components – Data Model, ETL, Metadata, and BI models. Changes and corrections to RI must be identified and propagated to the end user reports and queries as quickly as possible in order to insure their integrity.

Security Audit

Security Audit to include auditing, logging, monitoring, and reporting are key processes that need to be properly designed to comply with the HIPAA Security requirements and the HITECH Breach Notification Law.

Deloitte will deploy a central log correlation and Security Information and Event Management (SIEM) system. This will be implemented to provide centralized log collection, log normalization and analysis, real-time alerting on security events and provide HIPAA compliance reports. Deloitte will establish a logging and log management policy and associated procedures that outline what must be logged for each type of device, server, or application, how the logs are collected, stored, and secured, and how frequently the reports are reviewed (i.e., audited), and how the logs are archived.

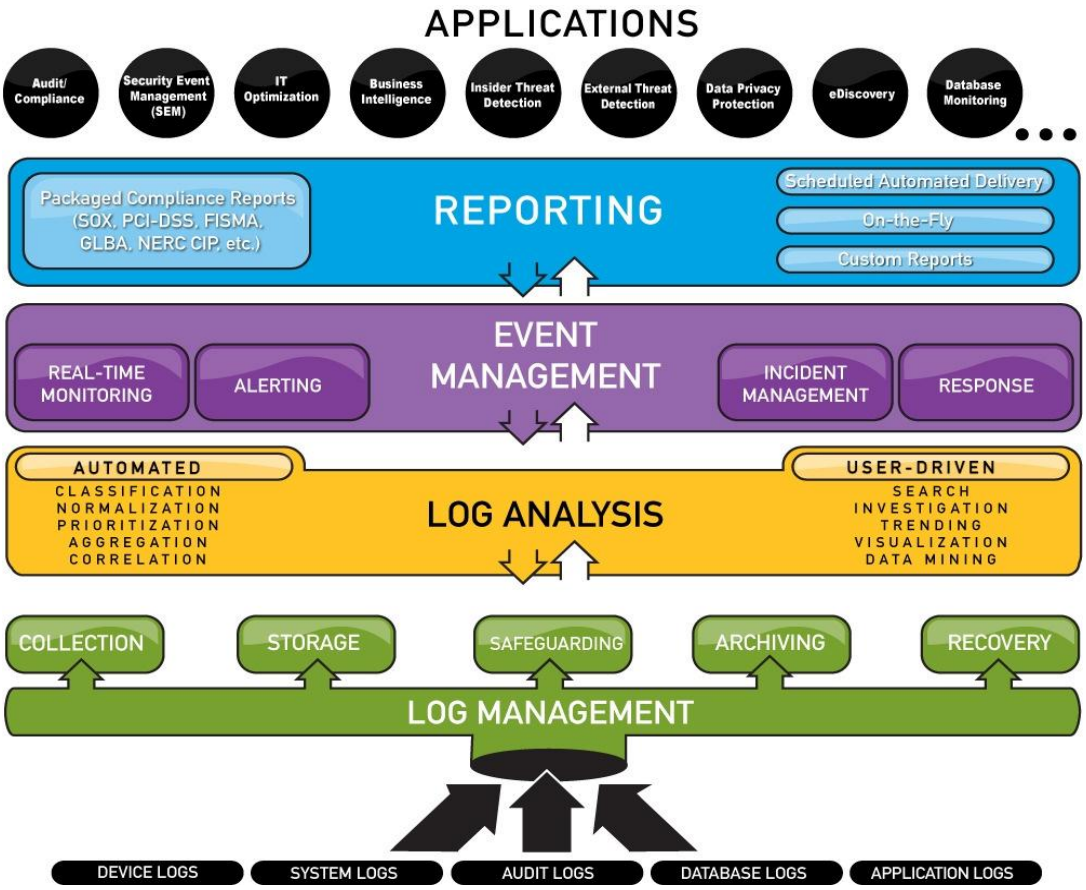


Figure 11-11. LogRhythm SIEM Conceptual Solution.

Deloitte will deploy EMC Ionix modules, or a similar product, for enterprise monitoring for availability and performance of the DW/DSS infrastructure. Ionix will be used to capture SNMP traps of devices and servers in order to generate real-time alerts to administrators based on defined triggers and provide a dashboard to monitor uptime and performance of the DW/DSS solution. This will be a key component of the DW/DSS solution in order to determine and report on the KPIs defined in the RFP.

Incident Response

Deloitte will collaborate with BMS to develop and incident response policy and incident response plan for the DW/DSS solution. The DW/DSS Physical Security camera footage, alarms, SIEM system alerts and reports, availability monitoring solution alerts, calls to the help desk or anonymous callers to the ethics and integrity hotline will serve as inputs to the DW/DSS incident response plan. The incident response plan will be a critical component of the overall security solution due to the HITECH breach notification law requirements and to mitigate risk of unauthorized access to DW/DSS sensitive data.

Security Related Change Management

Deloitte will develop a change management policy and associated procedures that align with the DW/DSS change management procedures. There are several aspects of change management that will be addressed.

- System configuration tracking
- Database configuration tracking
- Source code changes for custom code
- Test results, defects, and break/fix tracking
- Patch management

Deloitte will deploy a suite of change management tools (e.g., RequisitePro, ClearCase, and ClearQuest). Deloitte typically deploys BMC Remedy which can be used for the DW/DSS help desk trouble ticket management and for configuration management. Oracle Source Control and the IBM Rational suite of products can be used for source code management, change request tracking, requirements tracking, test case and test defect/test results tracking, and change management. The integration design of the above products will be determined based on defined requirements gathered during the requirements phase of the project.

Network Security

The Network Security solution design is divided into 5 focus areas. Deloitte uses a trust-zone architecture to establish a defense-in-depth approach.

Perimeter and DNS Security

Border Router Access Control Lists (ACLs)

Border router routing tables and ACLs will be the first line of defense for the perimeter of the DW/DSS solution. The routing tables and ACLs will only allow network traffic from other appropriate networks. This router will be managed by IBM, the hosting and circuit provider. The border routers will run Border Gateway Protocol (BGP).

Network Segmentation – Trust Zone Architecture

Deloitte will deploy a segmented network using a trust zone architecture. The network will be divided into a three-tier architecture with tier 1 consisting of the DMZ, tier 2 consisting of the application tier, and tier 3 consisting of the data tier where the DW/DSS database will reside.

A dual-firewall configuration will be in place to create tier 1, a demilitarized zone (DMZ). Services such as external DNS servers, web servers (accessed through HTTPS), and Network Time Protocol (NTP) servers will reside in the DMZ. These firewalls will be configured for the DMZ and protect the internal, trusted network from external networks.

Firewalls will also be used to separate the DMZ from the internal, trusted network which consists of tier 2 and tier 3. Firewall rule sets will be developed for each firewall to restrict network traffic so that only traffic from authorized networks or network segments can access DW/DSS resources.

Intrusion Detection System/Intrusion Prevention System (IDS/IPS)

IDS/IPS devices will be deployed as part of the network defense in-depth strategy. These appliances provide deep packet inspection services to detect and prevent security threats at layer 7 of the Open Systems

Interconnection (OSI) network model. They employ multiple intrusion prevention technologies working in tandem to monitor, detect or block these classes of network threats.

- Application attacks
- Attack obfuscation
- Cross-site scripting attacks
- Data leakage
- Database attacks
- DoS and DDoS attacks
- Drive-by downloads
- Insider threats
- Instant messaging
- Malicious document types
- Malicious media files
- Malware
- Operating system attacks
- Peer-to-peer
- Protocol tunneling
- SQL injection attacks
- Web browser attacks
- Web server attacks

IBM's managed IDS/IPS services will be used for monitoring the IDS/IPS logs in order to generate and provide real-time alerts to the DW/DSS security team.

Virtual LANs (VLANs)

VLANs will be used to further segment the network based on the type of services. A security and systems management VLAN will be established where critical security services such as firewall management, identity and access management services, and the security information and event management system reside.

Remote Access

The DW/DSS solution will require remote access to the systems from remote locations and will require secure access through the Internet. The final HIPAA Security Rule requires that ePHI transmitted over open networks must be encrypted. The network security design of the DW/DSS solution will provide encryption for all data in transit over open or untrusted networks.

There are three types of remote access to the DW/DSS infrastructure, to include Virtual Private Network (VPN), IPSec Tunnel, and HTTPS or Secure Socket Layer (SSL).

Deloitte will use an SSL VPN solution combined with two factor authentication for users that will need to remotely access the DW/DSS systems directly over the Internet. Cisco VPN Concentrator will be used for the SSL VPN solution and will be deployed to work in conjunction with RSA SecurID (hard tokens) in order to provide two-factor authentication.

Deloitte will use IPSec tunneling for direct database access. IBM will configure 2 IPSec tunnels, between the primary hosted data center location and the DR hosted data center location and the second between the primary data center location and BMS. Cisco routers/firewalls will be used and configured to meet FIPS 140-2 compliancy. The IPSec tunnel would be used to transfer data between BMS's MMIS systems to the primary data transfer servers.

Access to the i-Portal will require using HTTPS in order to provide SSL encryption. This would be configured in the Web Access Management product as part of the IAM solution for the DW/DSS. This would encrypt all traffic between the user's browser and the DW/DSS i-Portal. The SSL connection would be terminated on the LTMs that load balance the DW/DSS i-Portal Web Servers.

Vulnerability Management

The DW/DSS Vulnerability Management approach will consist of seven major activities:

- System hardening for servers and network devices
- Real-time intrusion prevention and detection
- Anti-malware/Anti-Virus Protection
- Proactive vulnerability patching based upon vendor security patches
- Vulnerability scanning prior to production deployment for new devices and servers
- Periodic vulnerability scanning performed by the Rapid7 scanning software and potentially other scanning tools
- Annual penetration testing (performed by 3rd party)

Network Monitoring

Deloitte will leverage IBM's hosted solution enterprise monitoring solution. IBM's monitoring solution will monitor the availability and performance of the network, servers, and applications. All alerts from these products will be forwarded to an Enterprise Event Console for incidents to be opened according to incident response and management procedures. The handling of security breaches will adhere to the HITECH breach notification law.

Application Security

Access control is the most important aspect of securing the database as it determines who is authorized to access ePHI. This section describes the different areas how Deloitte will deploy controls for access control for the DW/DSS solution to address mandatory requirements in the RFP and Federal and State regulatory requirements.

Identity and Access Management (IAM)

Deloitte build an IAM framework using the Oracle suite of IAM products in order to create and manage accounts and identities and manage role based access for the DW/DSS solution.

User Provisioning

Oracle Identity Manager (IM) will be used for the user provisioning solution. The user provisioning solution will be used to request, create and manage users of the DW/DSS solution, assign access privileges through roles, provide password self-service capability, and provide account reconciliation and attestation (re-certification) workflows.

Identity Proofing and Validation

The identity proofing and validation process will be designed based on requirements gathered during the Requirements phase of the project and designed during the design phase. This process must take place before a user is granted access to DW/DSS resources.

Identity and Account Creation

The user provisioning solution will be used to request, create and manage identities and accounts for the DW/DSS solution. All of the identity and account life cycle workflows (i.e., create, modify, suspend, restore, etc.) will be designed based on requirements established during the requirements phase of the project.

Password Management

The user provisioning solution will provide password management capability for the DW/DSS solution. The user provisioning solution will synchronize the user's password for i-Portal, database, DSS application, and network access and enforce the DW/DSS password policy across all resources managed by the user provisioning solution. The user provisioning solution will also provide users with the ability to change their own password or to use challenge/response questions in order to reset forgotten passwords.

Reconciliation

The user provisioning solution will provide the ability to determine if accounts were created natively in managed resources rather than through the user provisioning solution, which would be a violation of the access control policy that will be established. The user provisioning solution provides a centralized tool to create and manage access to DW/DSS resources according to the access control policy and reconciliation workflows provide the ability to disable or delete any accounts that violated the access control policy.

Account Attestation (Recertification)

Periodic review of user access privileges is a key component to managing the principle of least privilege access to DW/DSS resources. DW/DSS users will need to be recertified on a defined interval (e.g., every six months by either the user's supervisor and/or the information owner.) The account attestation workflows will be designed during the design phase of the project based on approved requirements. The diagram that follows outlines the Provisioning proposed provisioning solution.

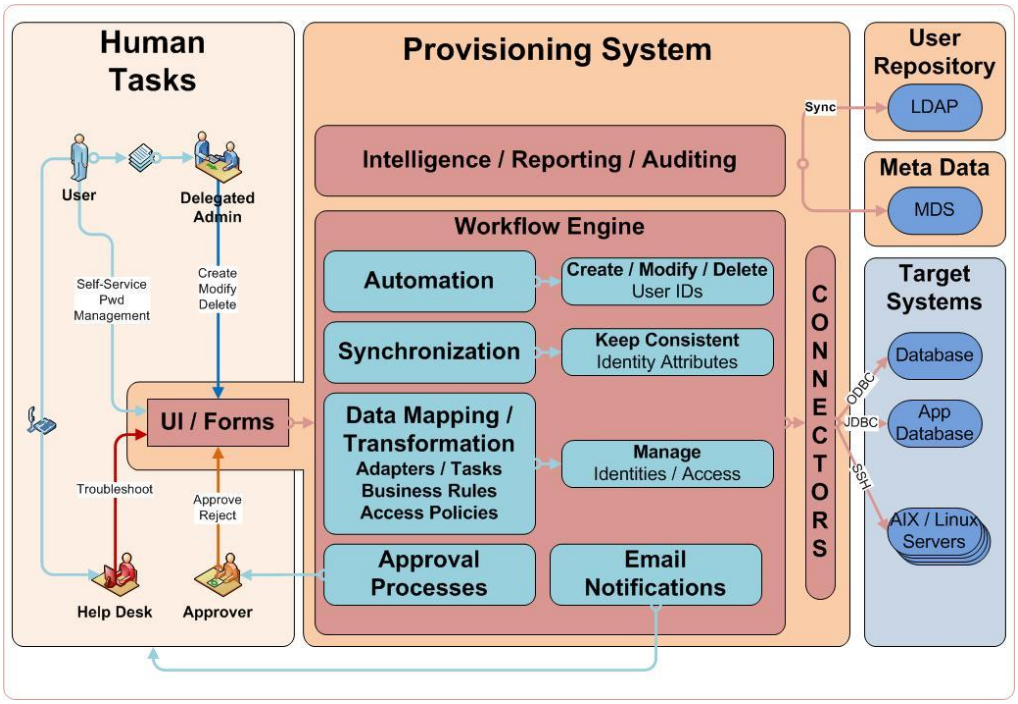


Figure 11-12. Proposed Provisioning Solution.

Web Access Management

Oracle Access Manager (OAM) and Oracle Adaptive Access Manager (OAAM) or the State's Web Access Management solution will be used to provide single sign-on (SSO) capability to the Portal and other Web-based applications in the DW/DSS solution as well as providing additional identity verification capability to combat identity fraud.

Directory Services

Oracle Internet directory will be used in conjunction with OAM to provide authentication for both the DW/DSS i-Portal and the DW Oracle database. A multi-master LDAP topology will be used for both local high availability and geographical failover to the DR site. LDAP data will be replicated in near real-time in order to meet defined requirements.

Role Management

The assignment of roles will be managed in the User provisioning solution (OIM). Roles will be assigned to each user in OIM that will dictate which group memberships in OID and which database roles will be assigned. Role engineering will need to take place during the design phase of the project to determine which roles need to be developed that map to OID groups and database roles to form the role based access control model for the DW/DSS solution.

Physical Security

Deloitte with its IBM hosting teaming partner will designate a Physical Security Officer and Facility Manager for the DW/DSS facilities. The responsibilities of the Physical Security Officer and Facility Manager will include:

- Supervise the assignment of security credentials and security access for access to the DW/DSS Data Centers
- Periodically review physical security policies and processes to see if updates are necessary
- Oversight of the security guards that monitor the facility as well as the equipment (i.e., cameras, etc.) used
- Reviewing the physical access logs regularly
- Preparing an incident report for the ISO in the event of a real or suspected violation of the Physical Access Policy
- Perform audits to confirm policy is being implemented. The frequency of the audits will be annually at a minimum

Facility Structural Security

The proposed hosting facilities are located in Phoenix AZ and Sterling VA - and in - with the following addresses:

Phoenix, AZ (DR Location) IBM – AOD Operations 811 South 16th St. Phoenix, AZ 85034	Sterling, VA (Primary Location) IBM – AOD Operations 22860 International Drive Sterling, VA 20166

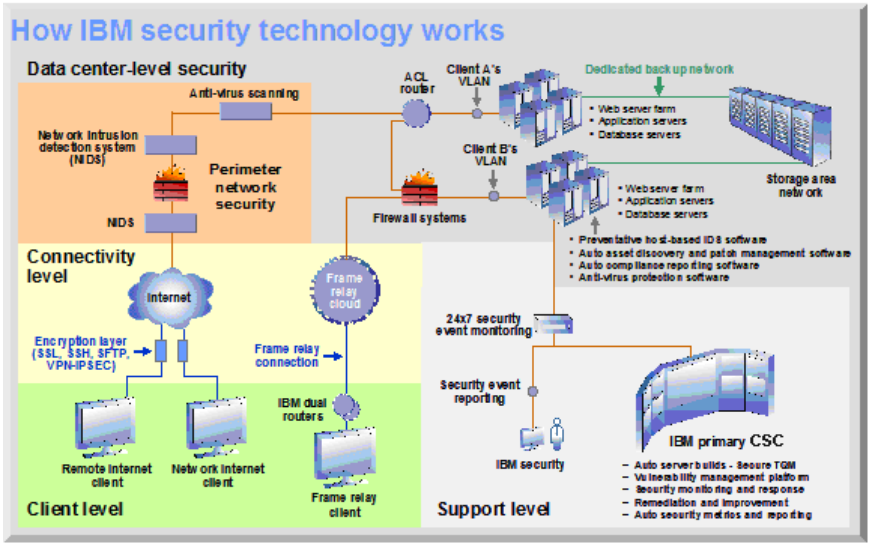
Physical access to IBM facilities is protected by badge access. Badge access to the facilities is only granted to IBM personnel and authorized contractors. All IBM critical infrastructure including servers, security infrastructure, and networking equipment is housed in IBM's facilities. These are protected by steel cages, double door entry ways, hallway cameras, and authorized personnel are restricted through the use of badge access and are required to show government-issued identification to receive that badge at the security desk (e.g. driver license).

Employees are screened prior to being hired. They are given a security badge (the badges have pre-defined access rights) to enter into secured areas of the building to perform their work functions. Upon termination, the facility is notified of their termination and all right and privileges are revoked. IBM limits access to the building by a single card-key controlled entrance adjacent to the security station. Security features include:

- Entrants use the biometric hand scanners for data center access.
- Electronic Card Key Access
- “Man Trap” with Biometric Palm Scan and Individual Personal Access Code
- 24 x 7 on-premise security officers
- Facilities command station
- Continuous closed circuit video surveillance through Stationary and 360° Cameras (interior and exterior)
- Security breach alarms
- The Data Center is staffed on a 24 x 7 basis, as well as a 24 x 7 Security Guard at the security desk. Aside from regular staff movement around the Data Center, the Security Guard conducts hourly rounds of the facility.

- Cabinets have dual power sources, as does all server equipment.
- IBM permits clients to visit the data center, but they must first, register at the security station and are then escorted during their entire visit. Visitors must wear a “visitor” badge and be escorted at all times. Before a visitor enters into the facility, an employee must submit the proper paperwork to Security identifying the visitor and expected arrival and departure times. All visitor tours must be facilitated by a tour coordinator. At no time are they allowed in the data center without an escort. The double doors are alarmed according to standard Data Center procedures.
- Facility Director/Manager performs regular internal audits on employee, vendor and visitor access. Every year, a third party audit firm conducts a site visit and reviews current processes/procedures and performs tests to verify that security policies are followed. These third party audits have not identified any material issues over the past two years.

IBM’s unified security framework is illustrated in the diagram below.



WV_DW_DSS-068

Figure 11-13. How IBM Security Technology Works.

Business Continuity

In support of BMS’s overarching Business Continuity Plan, Deloitte is proposing a disaster recover solution that provides a complete replicate of the DW/DSS production platform in a highly secure Tier 3 data center environment. This environment will provide a fully functional, fault tolerant site in case of a primary site failure or there is a severe reduction of service.

Business Continuity Plan

Deloitte will develop a business continuity plan for the sustainability of the DW/DSS solution during the DDI phase, which will encompasses the necessary technical solution components that will be required for BMS to maintain operations in case of a disaster or access to the primary data center where it becomes

inaccessible. The plan will address the processes, procedures, and technical aspects that are necessary to failover of the DR data center and begin the recovery of the primary site. We will use our proven Business Continuity Management (BCM) approach that follows many significant published standards and frameworks including NIST SP800-34, NFPA 1600, BS 25999, BSI/DRI and other industry and technical standards. We combine our BCM approach with our extensive State Government experience to provide BMS with a robust Redundancy, Business Continuity and Disaster Recovery (BC/DR) plan.

Effective recovery planning depends upon finding the right balance between risk of an outage, the cost to maintaining the continuity and recovery program, and recovery cost. We apply this risk managed principle at each stage of the DW/DSS project to provide a recovery plan that takes advantage of the technology provided within our solution. We will apply our established BCM approach to manage redundancy, backup and disaster recovery. To realize our BCM approach, we will leverage an integrated set of tools and techniques. Our approach creates a recover plan specifically tailored for DW/DSS and will include detailed work steps, presentations, databases, automated forms, checklists, and other supporting materials to meet DW/DSS requirements. Deloitte will focus on identifying and mitigating risks to allow BMS to continue operation. We will achieve this objective by:

- Conducting a broad analysis of the current state of preparedness, risks to continuity of operations, and business impact from major unplanned disruptions
- Developing governance and operating model, an emergency response, crisis management and continuity strategies as well as documentation of procedures
- Implementing recovery and resilience technologies, recovery processes, and testing and exercising programs
- Providing for ongoing measurement (qualitative and quantitative) and enhancement of the BCM program over time to sustain continued effectiveness of the program

The key activities we will conduct to build and maintain a recovery plan is shown in the table below.

Phase	Benefit to WVBSS Project
Project Management/Program Governance	Provides structured oversight for the engagement including a detailed project plan with milestones, roles and responsibilities, communications plans and status reporting mechanisms to identify report, assign and resolve challenges along the way.
Analyze	Determines the requirements for the resiliency and recovery of the processes and technology associated with this project. The focus is on understanding what is already in place (current state), a general and specific threat assessment to reduce the overall risks and a business impact analysis to determine the assets that need to be recovered and the timeframes under which it must be done.
Develop	Designs the strategies, resiliency and recovery procedures and assess the completeness and accuracy of the plans. The develop phase will focus on the definition of process to manage recurring back-up and recovery of each layer of the technology stack including documentation; storage and management of media; initiation and execution of restoration procedures; and the execution of actual failover and return procedures in the event of a declared disaster.
Implement	Allows for the execution of the plans both from a resiliency and recovery standpoint by supporting the purchasing and configuration of resources, the training of plan participants and the testing of the integrated recovery capabilities.
Continuous Improvement/Quality Assurance	Supports the maintenance of the program by defining timelines for review, triggers for updates and methods for having a periodic independent review of the content of the program. This phase will also define the annual process and procedures to test the business continuity and disaster recovery plan against one or more the State's prescribed scenarios (natural and man-made disaster, power failure, denial of service, H/W or S/W failure, performance degradation), and revisions to the plan based on the test experience.

Our BC/DR approach will also examine strategies for interfaces and system components based on the requirements analysis. Our focus will be to provide a timely recovery of network communications, storage and servers based on the recovery time objective (RTO) and recovery point objectives (RPO) for each application and dataset as supported by the business impact analysis. The resiliency of the DW/DSS processes is more than just the recovery of information technology. It requires a broader examination of and plan for the entire grouping of assets required to support the underlying functional requirements. To do this, we must examine how a disaster would unfold and then devise a plan for reacting from the on-set to the resumption of normal operations. The plan will address both Deloitte's responsibilities as well as those of BMS, its vendors and its end users.

To address recovery planning, our plan is structured around three types of responses that provide coverage from the time of the event to the time when normal operations return across the spectrum of disaster related events. The overall plan and responses will be revised on at least a semi-annual basis to reflect changes in the BC/DR capability and the results of testing.

- **Emergency Response.** Addresses the human safety and immediate response requirements after a disaster event affects the ability of the DW/DSS to provide these specific services. As covered above each response will address a number of different scenarios.
- **Crisis Management Response.** Addresses management's decision making processes, roles and responsibilities, communications both internally and externally and procedures for overseeing any crisis whether the event is technology centric, reputational or natural.
- **Disaster Recovery Response.** Addresses the recovery of a system failure, whether the failure is based on a network issue, storage unit or hardware failure, application or software problem or even a data corruption event. The plan includes identification of systems needed to be part of the recovery, (e.g., production only vs. training and other supporting systems). The recovery method for each system must also be identified, which can range from hot standby (minimal, if any, downtime, but more costly) to system rebuild/recovery (greater downtime, but lower cost).

The resulting plan and responses will be submitted for review (both originally and following each revision) by BMS. In addition, the plans will be developed to satisfy the requirements for Federal certification. Electronic and printed copies of the disaster recovery plan will be held at each of the primary and recovery hosting facilities, the local project office and in the care of the nearest Deloitte office as well as any locations the State may designate. In addition the plan will be published in the metadata repository. The plans will be available at these locations at any time for State auditors. To meet the requirements in the RFP, the operations plan for BC/DR will be composed of six major sections:

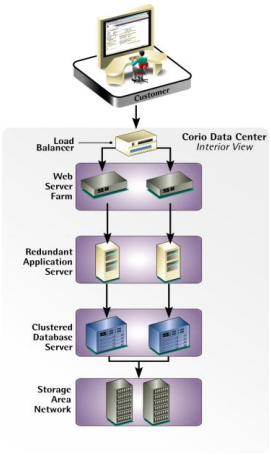
- **Concept of Operations.** In which we will describe the system (software, hardware, solution architecture, vendor maintenance agreements, dependent BMS systems and infrastructure, key BMS contacts and communications/escalation procedures) to be maintained in the event of a declared disaster. The concept of operations focuses specifically on the failover capability of the disaster recovery environment, the RPO and RTO for which the system is designed, and the hierarchy of services designated for restoration.
- **User Communities.** Major user groups, key user contact information, required system functionality, specific security and system access concerns to be maintained in the event of a declared disaster.
- **Planning Principles.** Used in developing the BC/DR plan including back-up methods employed; the alternate site (location, physical and logical infrastructure available, physical and logical controls and

security in place, and an inventory of the hardware and software that are available for use in the event of a declared disaster).

- **Notification Phase Activities.** To be executed in the event of a disaster including business impact analysis, damage assessment procedures, outage notification procedures and communication methods, plan notification procedures and plan activation procedures as well as key roles and responsibilities and success/escalation plans to be followed in the event one or more key responders are unavailable. Notification activities are designed according to the disaster declared – failure of hardware or software, loss of facility, natural or force majeure incident. In each case the business impact analysis, restoration planning and communication escalation as well as hierarchy of services for restoration will change to reflect the severity of the incident.
- **Recovery Phase Activities.** Including critical path activities and recovery plans for specific disaster scenarios (e.g., loss of primary site, loss of hardware, loss of data. loss of application or database software).
- **Disaster Recovery Planning and Testing Activities.** Including annual plan updates/refreshes, annual plan testing including key roles and responsibilities, test scenarios, and anticipated test results in terms of restoration time frames and restoration quality/completeness.

Failover/Fallback

Deloitte takes an active-stand-by approach to failover for the DW/DSS systems. The second hardware and software stack is integrated into the system in such a way that in the event of a failure in any component, the second stack will become active.



Flexible High Availability

- Load balancing at the Web tier – replicated Web servers with configured load director
- Redundant application server with failover capabilities
- Clustered database servers (RAC)
- Storage Area Networks (SAN)

Failover Simulation and Real Time Monitoring

- Fully tested High Availability capabilities to provide SLA compliance
- In event of a hardware or component failure, our applications management center is alerted via automated morning agents, to provide quick response by IBM application on demand personnel

WV_DW_DSS-066

Figure 11-14. High Availability Architecture.

Backup

Deloitte has full redundancy within the hosting site and fail-over to a secondary site. The physical servers are connected to diverse switches via “dual homing” which provides a higher level of availability. The storage RAID protected which means the failure of a single disk drive will not render your system unusable. Single site service levels are 99.5 percent for non-clustered applications, and 99.9 percent for dual sites. IBM supports the server clustering technologies (IBM PowerHA Cluster Manager and Oracle Real Application Clusters (RAC) for server clusters) to provide higher availability (HA) for critical applications. In a two-node,

active-standby cluster, the standby node of the cluster is active but idle, periodically checking to make sure the active node of the cluster is still active.

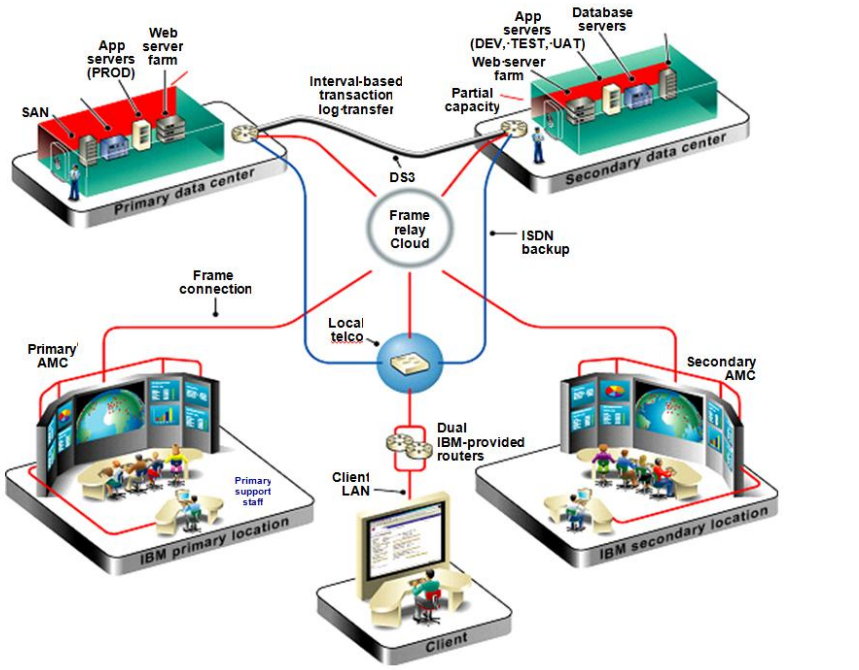


Figure 11-15. Disaster Recovery Architecture.

The disaster recovery service, business data and transactions are transmitted between the primary and secondary data centers continuously throughout the day via a private connection, shown in Figure 11-15. Both the primary and secondary data centers are fully staffed with the skilled personnel required to execute a disaster recovery plan, including fully redundant command-and-control centers from which critical application processes are monitored and controlled. The disaster recovery option also provides all of the secondary and critical network connections to confirm that the secondary data center is accessible during a recovery situation. The secondary infrastructure and the fail over, IBM provides a 99.9 percent availability guarantee for the DW/DSS production environment.