Mississippi Department of Human Services

Legacy Systems Assessment

Deliverable 5. Conceptual System Design

Version 1.1

Submitted by:

Danielle Ewing, Principal
Lauren McTear, Engagement Manager
Jessica Lindley, Project Manager
BerryDunn
2211 Congress Street
Portland, ME 04102-1955
Phone: 207.541.2200
dewing@berrydunn.com
lmctear@berrydunn.com
jlindley@berrydunn.com

Submitted on:

April 29, 2022

Table of Contents

Section **Page**

Version	Delivered Date	Version Notes
0.1	April 6, 2022	Working draft submitted to the Mississippi Department of Human Services (MDHS)
1.0	April 29, 2022	Final draft submitted to MDHS for approval
1.1	May 9, 2022	Updated conceptual system design diagram and the PDF files with the updated diagram

1.0 Conceptual System Design Overview

The purpose of this document is to provide a conceptual system design for the MDHS' future modernized integrated information technology (IT) solution. The conceptual system design is agnostic to the alternatives presented and provides the equipment, performance, functional, and technical requirements needed for a modernized integrated IT solution.

1.1 The MDHS Business and Technical Vision

The MDHS currently uses five legacy IT systems to operate its Supplemental Nutrition Assistance Program (SNAP) (including Disaster SNAP [DSNAP] and SNAP Employment and Training [SNAP E&T]), Temporary Assistance for Needy Families (TANF), TANF Work Program (TWP), Child Support Enforcement (CSE), and the Child Care Payment Program (CCPP), as follows:

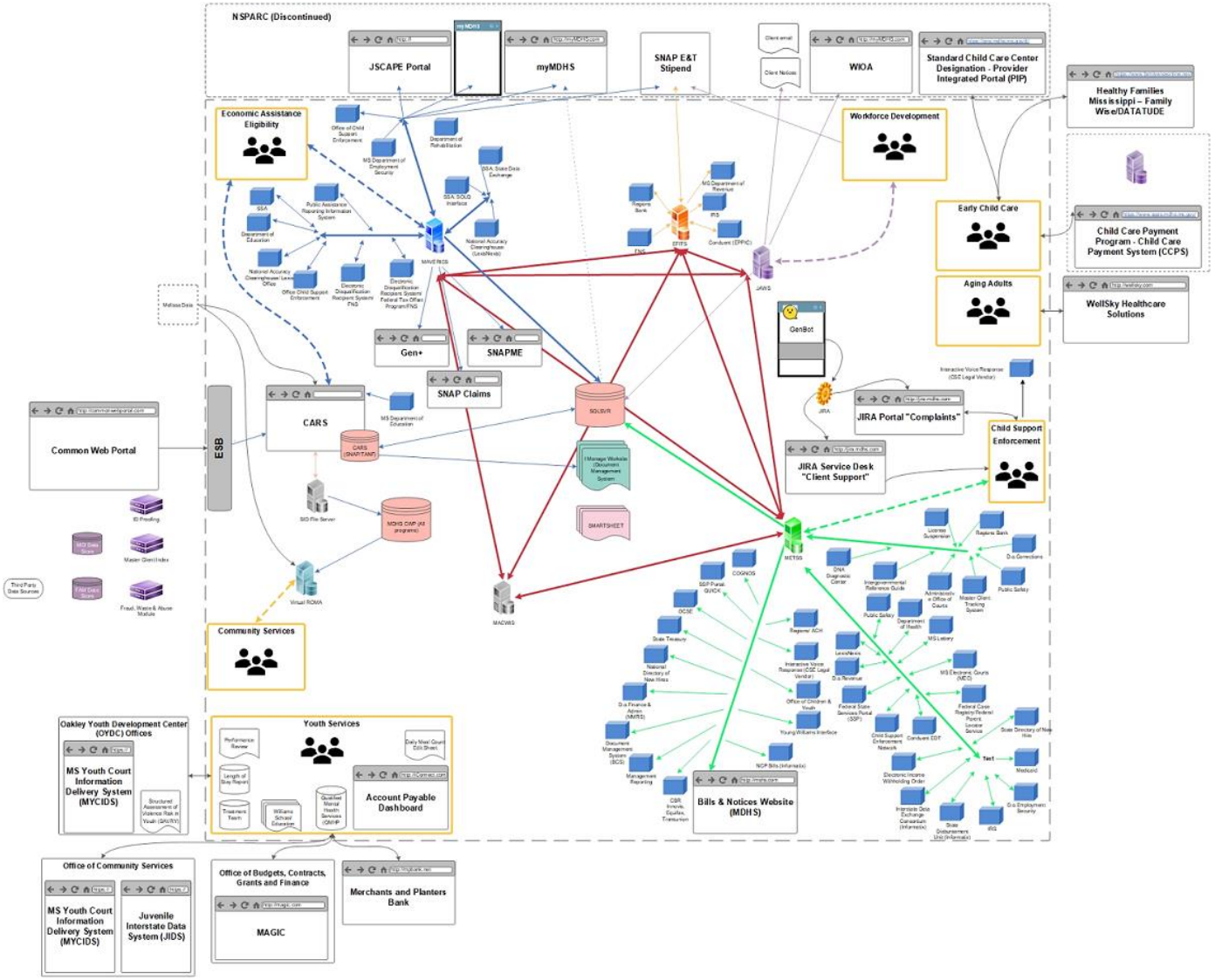
- Mississippi Automated Verification Eligibility Reporting Information Control System (MAVERICS)—manages eligibility determinations for SNAP; subsystems include DSNAP and SNAP E&T.
- Jobs Automated Work System (JAWS)—manages TANF eligibility and TWP case management service for eligible recipients.
- Electronic Financial Interface Tracking System (eFITS)—an interface with the State of Mississippi's (State's) Electronic Benefit Transfer (EBT) contractor systems; eFITS provides deposits to a client's cash benefit card from multiple programs and reconciles the use of benefits.
- Mississippi Enforcement and Tracking of Support System (METSS)—collects and maintains data on all CSE cases and performs automated functions pertaining to CSE activities.
- Child Care Payment System (CCPS)—manages the CCPP within the Division of Early Childhood and Development.

Figure 1 on the following page provides an overview of the current MDHS ecosystem, inclusive of the current MDHS' legacy systems and their components.

The PDF version of Figure 1 is located on page one in the file below.

D5 Design Diagrams-2.pdf

Figure 1: The Current MDHS Ecosystem



Although these legacy IT systems have supported the MDHS' service delivery needs and allowed it to provide critical benefits to clients, the MDHS seeks to implement a modernized, integrated IT solution to help achieve its project vision and goals. The MDHS' vision is for MDHS staff and providers to support the delivery of—and for clients to access—public assistance programs, social services, and other supports in a seamless, efficient, effective, timely, and transparent manner through modernized, integrated IT systems.

The MDHS identified the following modernized, integrated IT solution objectives to meet its vision based on desired IT system improvements, including the requirements, capabilities, features, and/or enhancements not supported by the current legacy IT systems.

1. The MDHS IT systems must be flexible and responsive to the needs of the MDHS and the residents of Mississippi, and they must support regulatory, policy, or procedural changes.
2. The MDHS IT systems should decrease maintenance and operational costs and enable the reuse of components from other program areas within and external to other State agencies.
3. The MDHS IT systems should increase staff satisfaction and decrease staff workload and inefficiencies.
4. The MDHS IT systems should improve the timeliness and accuracy of eligibility determinations and issuance of benefits to the residents of Mississippi.
5. The MDHS IT systems should reduce the potential for fraud, waste, and abuse and improve overall program integrity.

1.2 Current System Limitations

The MDHS has identified several current system limitations that are expected to be addressed by the conceptual system design. Current system limitations include:

1. The current environment is neither scalable nor appropriately load-balanced across servers to meet peak volume demands. This results in performance degradation when peak volume is reached, causing service interruptions and sporadic system resets, and it negatively affects general system performance.
2. Several databases are used within a single environment, including training, quality assurance, and help desk, which contributes to performance issues. In addition, some applications run on a single server, which can further complicate the application delivery process.
3. Antiquated legacy programming languages and the system environment make installation of system maintenance updates (including rollbacks) difficult and time consuming. MAVERICS uses Natural and Common Business-Oriented Language (COBOL) programming languages. JAWS, eFITS, and METSS use Natural only. This creates a challenge acquiring technical resources to support the IT systems, because

individuals with Natural and COBOL experience are scarce, expensive, and often unavailable.

4. The current backup processes use a slow connection with high latency, which results in performance degradation and directly impacts users. While the MDHS does have access to data backups, should a disaster occur, a robust disaster recovery (DR) architecture does not exist. The cloud backup options, also available to the MDHS, use slow and unstable connections. Should a system failure or disaster recovery scenario occur, rebuilding a working environment to recover would be a laborious and time-consuming process. General backups are run as part of a batch process, and full backups—as opposed to incremental backups—are generated nightly. This contributes to further strain on performance and system usability.
5. With data for the legacy IT systems currently residing in silos, data collected is often not complete and differs in quality. Lack of a universal parent record, coupled with manual data entry processes, results in limited protection against duplicate records. Similarly, client demographic data varies based on the interface source and is not received in a consistent manner; therefore, client demographic data cannot be validated on a regular basis across systems.
6. The IT systems lack an effective Master Data Management (MDM) and data governance system, as there is an inability to identify all that is known about a person (client) across the MDHS systems, which can negatively impact the entire benefits coordination process.
7. The current technical architecture does not leverage machine learning platforms and languages, limiting the ability for predictive trend analysis, including the detection and identification of potential fraud, waste, and abuse.
8. Because each legacy IT system uses unique code bases, they are often at various stages of compliance with federal security and programmatic standards across programs, including Internal Revenue Service Publication 1075 (IRS-1075) and National Institute of Standards and Technology Special Publication 800-53 (NIST-800-53) Revision 5 (Rev. 5).

1.3 New System Assumptions and Constraints

1.3.1 Assumptions

Assumptions are premises about the business, policy, technical, and/or other factors in the project environment that, for the sake of the project, are taken as fact. The following assumptions may influence the implementation of a modernized, integrated IT solution:

1. All reuse components might have to be updated or reconfigured as required to access the new cloud-based system.
2. The interoperability of the MyMDHS mobile app will need to be updated and reconfigured to access the new cloud-based system, although the new vendor's solution mobile app may be preferred.
3. The new system will grant clients access to both benefits status and application status.
4. Direct read may not be allowed in the new vendor's system.
5. MDHS will need to decide what programs are protected entities for health information privacy and protection, and confidentiality.
6. Interactive Voice Response (IVR) may need to be reconfigured to accommodate access to the new cloud-based system.
7. The current call center system may need to be reconfigured to have access to the new cloud-based system.
8. The new worker portal will act as the front door to the new cloud-based system to streamline access and provide other prioritizing and routing tools.
9. Rule-based routing will be provided by cloud-based vendor system for document routing.
10. Single Sign-On (SSO) will need to be enhanced to support the new cloud-based system.
11. The new cloud-based system will need access to all the systems logs in the MDHS landscape for the vendor to produce aggregated logs (e.g., system logs, user logs).
12. The new system vendor will enable rule-based, role-based access.
13. The new system vendor will provide and support real-time, near real-time, and asynchronous data exchanges.
14. The new system vendor will support external web services as required by the State.
15. The new system vendor will provide and support performance monitoring and capacity planning tools for monitoring the new cloud-based systems.
16. The system integrator will be responsible for providing the tools, support services, and Maintenance and Operations (M&O) for the following:

a. Services registry for cataloging all web services (e.g., application programming interfaces [APIs], micro-services, etc.)

b. Workflow automation and related services

c. Rules-engine/rules-repository services

d. Performance monitoring/capacity planning for the MDHS' existing systems

e. Records management and record retention services

17. IRS-1075 will be the baselined compliance requirement for the new system environment.

18. There are other MDHS applications that depend upon the current legacy system applications, which will need to be evaluated case-by-case by MDHS and the new system vendor. The system integrator will have the responsibility to accommodate legacy application system integrator tasks.

19. The MDHS envisions real-time data exchange as the preferred exchange method. The ability to provide real-time exchanges with data partners is dependent on the technical capabilities of each partner. MDHS may need to perform a case-by-case evaluation with all data partners to determine if real-time data exchange could be supported for both inbound and outbound data.

20. The current MDHS systems run on RedHat Fuse®, which may need to be reconfigured for the new cloud-based system.

21. Legacy databases for all applications are replicated live to a structured query language (SQL) database.

1.3.2 Constraints

Constraints are known facts over which there is limited or no control. Constraints can affect the scope, direction, planning, and implementation of a project. The constraints listed below apply to the conceptual system design and are higher-level, but they are documented in more detail within the MDHS Requirements Traceability Matrix (RTM).

1. The new system architecture must comply with State and federal security and privacy requirements for public, community, and private clouds, including compliance with the State Enterprise Security Policy (ESP), State Off-Site and Cloud Hosting, Food and Nutrition Services (FNS), Office of Child Support Enforcement (OCSE), IRS 1075, and Social Security Administration (SSA).

2. The new system must use SSO, integrating with the MDHS' Azure SSO.

3. The new system must enforce minimum password requirements compliant with MDHS security policies.

4. The new system must automatically sign off users (e.g., clients and service providers) after a certain amount of time of inactivity, configurable by the MDHS as specified by the MDHS security policy.
5. The new system must have the ability to automate purging/archiving and retention of cases and case data, based on the MDHS, State, and federal purging/archiving rules and retention policy, including, but not limited to:
    a. Inactive records
    b. Closed cases
    c. Client health information
    d. Any other types or classes of data as defined/authorized by relevant regulation or agency policy
6. The new system vendor must support conversion of historical data into the new system and create conversion data staging tables to load active and historical data from multiple systems as directed by the MDHS and/or the system integrator.
7. The new system must be interoperable with tools managed by the system integrator, including any MDM tools.
8. The new system must integrate with the existing document solution (Worksite) to support tracking and efficiently scanning of documents and preparing them for further processing. This may include the ability to attach a scanned document(s) to a case/client record. These could include any documents associated with a client's case and can be received in hard copy via fax and include, but are not limited to: applications, referrals, returned mail, and supporting documentation. Integration with Worksite will be evaluated by the MDHS from a cost benefit analysis perspective.
9. The new system must integrate with the existing content management (iManage). Integration with iManage will be evaluated by the MDHS from a cost benefit analysis perspective.
10. The new system must support the use of electronic signatures and integrate with existing MDHS/State-approved third-party electronic signature tools (e.g., Smartsheet®). The use of additional third-party electronic signature tools will be evaluated by the MDHS from a cost benefit analysis perspective.
11. The new system must use the MDHS Enterprise Service Bus (ESB) for all online and potential batch interfaces.
12. The new system must use the MDHS reference tables to translate code values to facilitate interface processing of inbound and outbound data with external systems.
13. The new system must have the ability to integrate with, and be managed by, Microsoft (MS) InTune or by any other MDHS' approved Enterprise Mobility Management solution.

14. The new system must provide, or integrate with, MS Office365 or with any other MDHS-approved office automation tools as determined by the MDHS.
15. The new system must use the MDHS' existing email server (MS Office365) to send/receive email, and only send client messages in a secure format by default, logging email failures and virus scan rejections.
16. The new system vendor must use an industry-standard, third-party application performance-monitoring and management solution to monitor operations daily, using automation with real-time alerts, making necessary adjustments to maintain peak operation efficiency.
17. The new system must meet and comply with all current State and federal security and privacy policies.
18. MDHS is in the process of migrating all systems to the State private cloud.

1.4 Identification of Reuse Components

The MDHS has identified several technical assets, business assets, and resources that the department will use to support the future MDHS modernized, integrated IT solution. The reused functionality contributes to cost avoidance as MDHS has already invested in the items and may not need to fund Design, Development, and Implementation (DDI), M&O, or other expenses related to the costs—except for minor changes to accommodate the new system components. The existing assets and resources are already maintained and operated by the State or its agents (as listed in Table 1 below) will provide reused functionality in the new system and will not need to be re-procured or modified by the incoming vendor.

Table 1 on the follow page provides a non-exhaustive, high-level summary of the major components and technical assets within the current MDHS ecosystem. The MDHS will evaluate each reuse component from a cost benefit analysis perspective to determine whether reuse or a vendor-based solution is preferred.

Table 1: Summary of MDHS Reuse Components

Reuse Component	Description/Overview	Reuse Review
Common Web Portal (CWP) and MyMDHS Application	The MDHS modernized, integrated IT solution is expected to integrate with the MDHS' current and future iterations of the Common Web Portal and the MyMDHS application.	As confirmed by the MDHS, House Bill 1090 mandates the use of the modules CWP, FAM, and MPI. The MDHS is open to review the mobile app provided by the new system vendor and decide based on the functionality and ease of use of the vendor-provided mobile app.
Databases and Data Warehouses	Many existing databases, and some COGNOS-based data warehouses and reporting platforms, will not be replaced.	The incoming vendor will provide data services for its own solution but will need to integrate with those that exist currently in the State's domain. Integration of data services may be a function of the system integrator.
Disaster Recovery (DR)	The MDHS is in the process of migrating all systems to the State private cloud, which allows high availability (HA). Storage is currently managed by EMC Storage Solutions.	While the MDHS does employ redundancy in some hardware servers, areas for improvement exist. There is currently no duplicate data center for DR. There is no HA redundancy in the production server. The new system vendor must provide hot DR site and business continuity support, as required by the MDHS.
SNAP Notice Replacement Project	A project designed to improve SNAP notices is currently underway. The incoming vendor is expected to enhance the existing Communications Generation Tool, enhance existing notices, and incorporate the notices from the SNAP Notices Improvement project. The vendor will be able to use either the report description files and/or the design documentation from the SNAP Notices Replacement Project immediately.	The new system vendor is expected to enhance the existing notices and incorporate the notices from the SNAP Notices Improvement project into the platform.

Reuse Component	Description/Overview	Reuse Review
Call Center, IVR and Chat Bot Functionality	Customer service functions such as mailroom, call center, and IVR or conversational user interface (Chat Bot) will not be replaced. The MDHS has a standing call center resource with an IVR. Chat Bot services are already in use and will be integrated with the new solution where necessary. When necessary, the modernized, integrated IT solution will integrate with, and collaborate to, support existing artificial intelligence Chat Bot functionality.	The new system vendor will be expected to integrate, as necessary, with the MDHS call center and IVR including additional configuration changes. The MDHS is open to review the Chat Bot functionality provided by the new system vendor.
Existing Targeted Reporting	The MDHS has existing specialized reporting needs that will not be replaced. This is predominantly in CSE to support the current CSE vendor, with data extracts from State systems incorporated into the CSE vendor ecosystem.	The MDHS has mandated State and federal reporting that happens at prescribed frequency. The new system vendor must provide the data required to support these mandated reports at the prescribed frequency. Report definitions can be reused/converted for the new system. The State could require the vendor to provide an extract that is identical to what is provided today. The new system vendor may have to interface and support the existing CSE vendor or provide continuity with the current CSE vendor, while leaving an opening for alternative approaches depending upon the status of the current CSE vendor contract.
Address Verification Services	The existing address verification system provides services that are regulatory and compliant and have the MDHS' desired functionality. The vendor will be able to interface with this service instead of passing it on, potentially increasing the cost for subscription service(s).	The MDHS modernized, integrated IT solution is expected to integrate with and use existing address verification services. The MDHS stated a unique aspect of address verification services being that the Melissa Personator® is in use to verify, correct, and append all client addresses, and it associates the individual with their respective address. The MDHS is open to working with the new system vendor to determine if a new-vendor solution addresses the MDHS' address verification service needs.

Reuse Component	Description/Overview	Reuse Review
SSO	The MDHS already has SSO capability. These services are already capable of being integrated using existing standards.	The new system vendor is expected to integrate with and use the State's Azure SSO system.
Fraud and Abuse Module (FAM)	The State has an FAM that is in development, not yet currently functional in the production environment. MDHS plans to utilize the module in the future. The vendor is expected to integrate with and enhance FAM functionality.	State House Bill 1090 mandates the use of the State FAM. The MDHS is open to review the FAM functionality provided by the new system vendor. The existing FAM may need enhancements to the existing functionality.
ESB	The MDHS has an ESB that ties into some of the services intended for reuse.	The new system vendor is expected to integrate with the MDHS ESB. The MDHS may need to upgrade their services and connectors to connect to the new system vendor.
Master Person Index (MPI)	MPI is currently not implemented. CWP, FAM, and MPI come with a House Bill 1090 bulk pack that is mandated to the MDHS. The State might have an enterprise-level MPI in place for use in the new solution.	State House Bill 1090 mandates the use of the State MPI module. As MPI is not fully implemented, the MDHS is open to review the MPI module functionality provided by the new system vendor. The MDHS is looking for an industry-recognized third-party solution for MDM to help with its growing needs. The MPI could serve to bridge the vendor's MDM and existing data requests the MPI can provide. The MPI can also serve as a springboard for data conversion that is necessary for an MDM.
Testing Environments	The modernized, integrated IT solution must integrate, where applicable and necessary, with the State development and testing environments.	The new system vendor must provide testing and training environments and must integrate with existing MDHS environments as required.

2.0 Description of Alternatives

Alternative 4: COTS/MOTS Solution, and Alternative 6: Enterprise-Wide System Framework were identified in the previously conducted alternatives analysis and cost benefit analysis reports as functionally, technically, and operationally feasible solutions to achieve the MDHS' system modernization goals. The alternatives are provided for context. Regardless of which alternative is selected by the MDHS, the information provided in this document applies to either alternative. The conceptual system design serves as a high-level abstract of the system interactions and functionalities that align with the MDHS requirements. It should be noted that the components outlined in this document may not be available with any single COTS/MOTS system or an enterprise vendor.

2.1 Alternative 4: COTS/MOTS Solution

This alternative involves the procurement and configuration of a COTS/MOTS SNAP, TANF, CCPP, and CSE replacement system to meet the MDHS' needs. The alternatives analysis evaluated the fit of a COTS/MOTS system used by a peer state for similar needs against requirements identified by the MDHS' stakeholders and determined that strong alignment could potentially exist. Leveraging information and lessons learned from a COTS/MOTS system already in use by a peer state and then configuring and customizing it to meet State-specific needs could help meet the MDHS' objectives while offering the opportunity to avoid pitfalls experienced elsewhere. From a technical perspective, this approach provides an opportunity to replicate a proven and stable architecture with configuration and customization points available to align the solution to the MDHS' requirements.

2.2 Alternative 6: Enterprise-Wide System Framework

An enterprise-wide system framework is defined as an approach that uses common technologies or integrated platforms as the foundation for all of a state's human services programs, thus avoiding the use of multiple human services IT systems—each developed and maintained separately. Although in general this concept extends beyond eligibility and enrollment to include other program administration and management functions (e.g., case management, enforcement, assessment, care planning, and service tracking), for the purposes of this project, Alternative 6: Enterprise-Wide System Framework is defined as an integrated framework supporting state programs such as SNAP, TANF, CCPP, CSE, Medicaid, Long-Term Care, and Low-Income Home Energy Assistance Program (LIHEAP). Of particular interest to the MDHS is that the approach emphasizes containerized modularity through a Service-Oriented Architecture (SOA). In practice, an enterprise-wide system framework could leverage a combination of SOA approaches, potentially including COTS/MOTS solutions, state-transfer components, and/or applications that are refactored for the cloud.

3.0 System Performance Requirements

Optimized system performance is a critical component of any future system used by the MDHS. Currently, the MDHS system is not optimized for scale and experiences performance degradation due to several reasons, including user load, backup processing, and general database usage. Substandard performance results in system timeouts and lag times, negatively impacting user satisfaction and production. Please reference Section 1.2 for additional details of the current MDHS system's limitations.

The future system must be operationalized around performance, ensuring that system availability, response time (e.g., system responsiveness to user keystrokes), DR time (including the expected recovery point), and system maintenance windows are acceptable to the MDHS. In addition, the contract with the new system vendor will include service-level agreements (SLAs) related to DR and other key system performance measures. SLAs might relate to system availability (e.g., 24/7 availability – 99.99% uptime) and system response time (e.g., 95% of record search responses are < 4 seconds).

The MDHS will work with the new system vendor on the appropriate SLAs at the time of procurement to identify the specific metrics around performance. Examples of typical performance requirements may include:

1. The system must be backed up on a consistent schedule, compliant with defined SLAs, and with no impact on system availability or system performance.
2. The system's responsiveness (e.g., system responsiveness to user keystrokes) must be compliant with defined SLAs.
3. The system's DR plan must be identified and approved by the MDHS, with DR thresholds outlined in defined SLAs.
4. System maintenance requirements must be identified and approved by the MDHS and monitored in accordance with defined SLAs. It is expected that maintenance operations will be modularized, allowing non-impacted system components to remain functional during maintenance windows.
5. The system vendor must use an industry-standard, third-party application performance monitoring and management solution to monitor operations daily, using automation with real-time alerts and making necessary adjustments to maintain peak operation efficiency.
6. The system must provide SLA monitoring and reporting utilizing out-of-the-box (OOTB) platform and portal platform reporting/monitoring capabilities.
7. The system must provide information on performance metrics identified.

8. The system vendor must support and provide system capacity planning and review as required. It is expected that the system will have sufficient storage space and a proactive storage strategy to allow a growing number of clients, cases, and affiliated attachments and progress notes without vendor intervention.

4.0 System Operating Environment

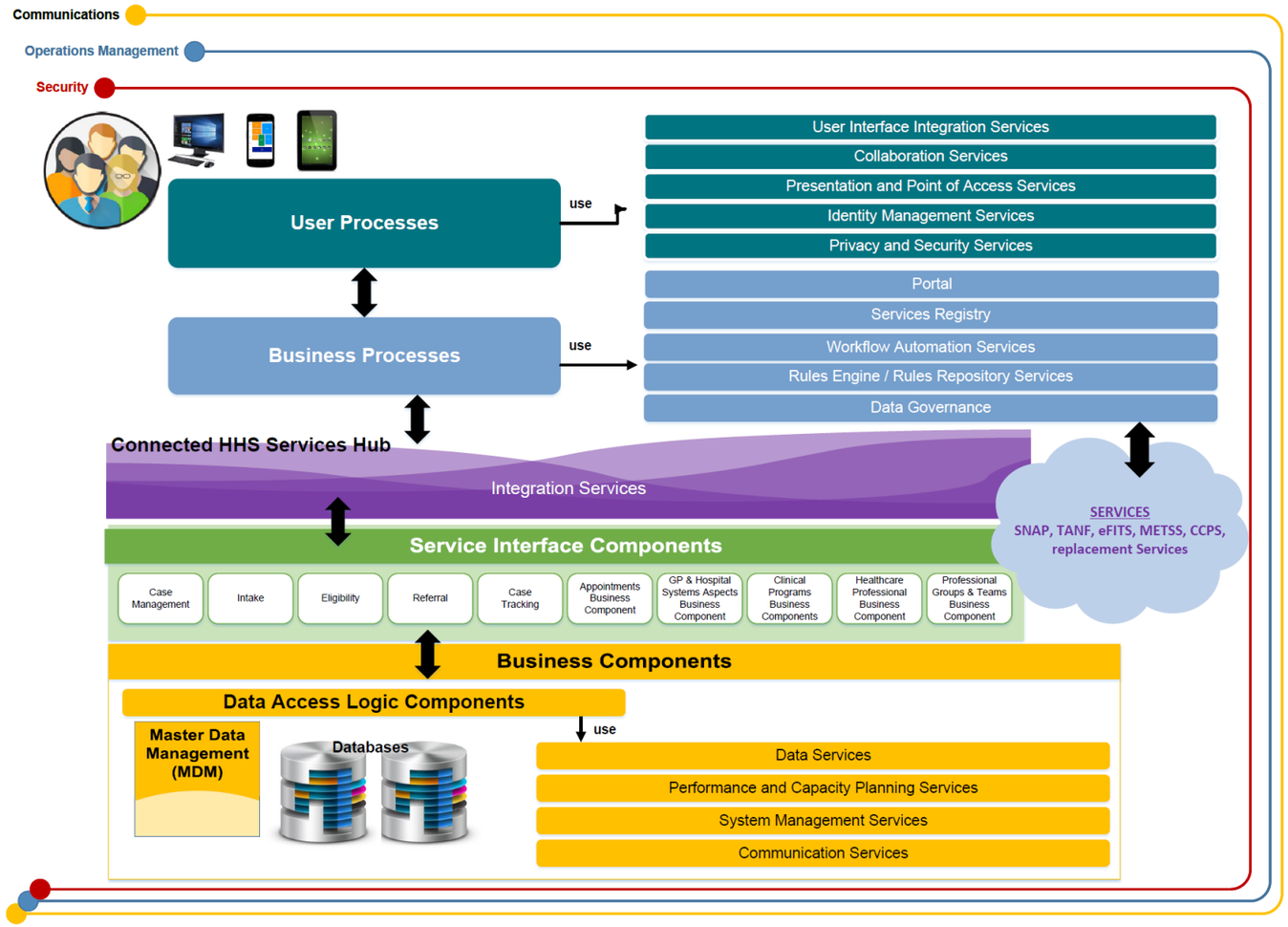
The MDHS identified the following high-level modernized, integrated IT system operating environment needs based on the MDHS' current system limitations, as listed in Section 1.2 and the MDHS Legacy System Assessment Project supporting documents (e.g., Legacy Systems Assessment Report, Feasibility and Alternatives Analysis Report, and Cost Benefit Analysis Report). System operating environment requirements are also listed in the MDHS RTM. The system operating environment for the MDHS' modernized, integrated IT solution must:

- Use a single integrated human services system using a cloud-native architecture with the ability to add modules for additional systems
- Have integrated reporting, analytics, and machine learning
- Employ a containerized, open-system platform agnostic vendor
- Employ elastic resource allocation to allow applications to dynamically respond to workload fluctuations
- Improve overall system performance
- Use real-time data exchange and accommodate a mix of real-time, asynchronous near real-time, and batch processing
- Reduce M&O costs
- Provide robust DR architecture

Figure 2 on the following page presents a high-level conceptual system design of the MDHS operating environment for a modernized, integrated IT solution.

The PDF version of Figure 2 is on page four in the file below.

Figure 2: Conceptual System Design: Operating Environment



The preferred approach for the system operating environment is to use both an enterprise system integrator vendor and an Independent Verification and Validation (IV&V) vendor. The enterprise system integrator will need to manage integration of new systems and existing systems. Federal Regulation 45 CFR 307.15(b) (10) requires an entity independent of the State Title IV-D Agency and of the Child Support Enforcement Services (CSES) project management structure to review all technical and managerial aspects of the project. The IV&V vendor can help:

- Review activities/results for each development step
- Inspect final products for compliance and functionality
- Proactively identify risks
- Provide the MDHS Project Management Office (PMO) with objective visibility into the progress of the project
- Increase the probability of project success by reducing errors in delivered products

5.0 Conceptual System Design Diagrams

The conceptual system design serves as a high-level abstract of the system interactions and functionalities that align with the MDHS requirements. Please reference Section 2.0 for more details regarding requirements and functionalities.

Figure 3 on the following page provides the current MDHS' ecosystem—inclusive of the current MDHS' legacy IT systems and their components—and identifies (at a high level) the systems to be replaced by a modernized, integrated IT solution.

Figure 4 on the pages that follow provides a conceptual system diagram of the high-level architecture for a MDHS modernized, integrated IT system.

The PDF version of Figure 3 is on page two and Figure 4 is on page four in the file below.

Figure 3: Current MDHS Ecosystem with Replacement Components

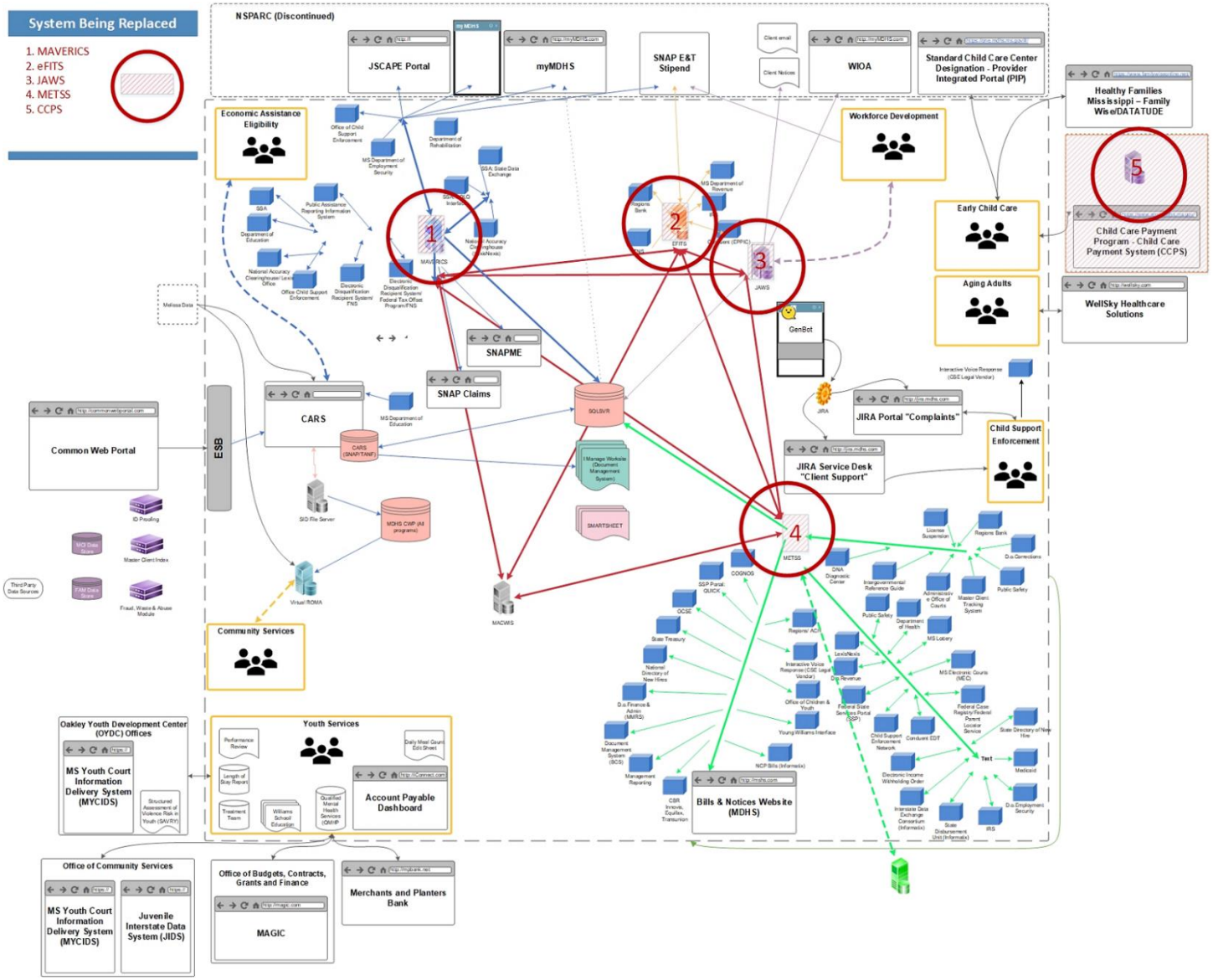
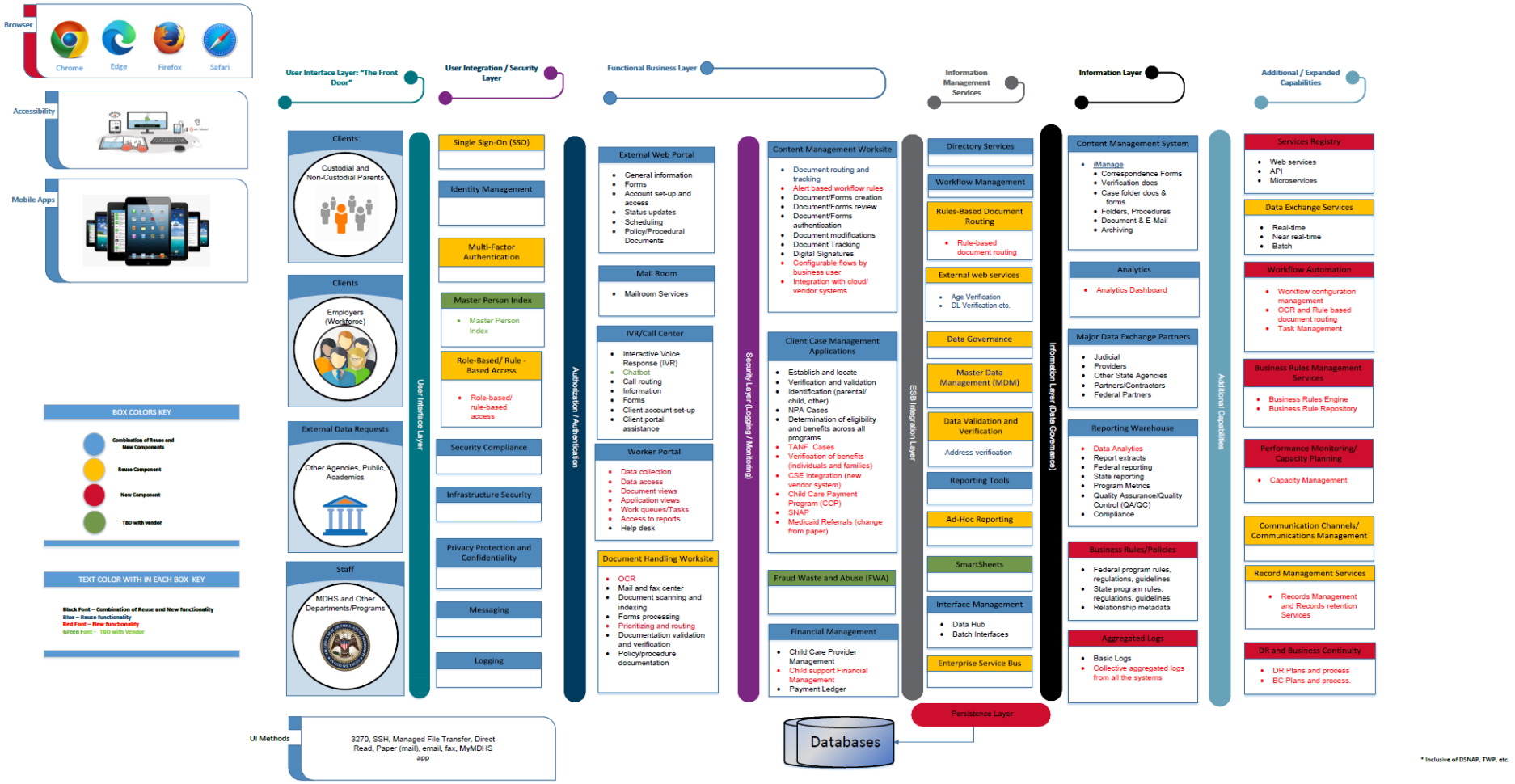


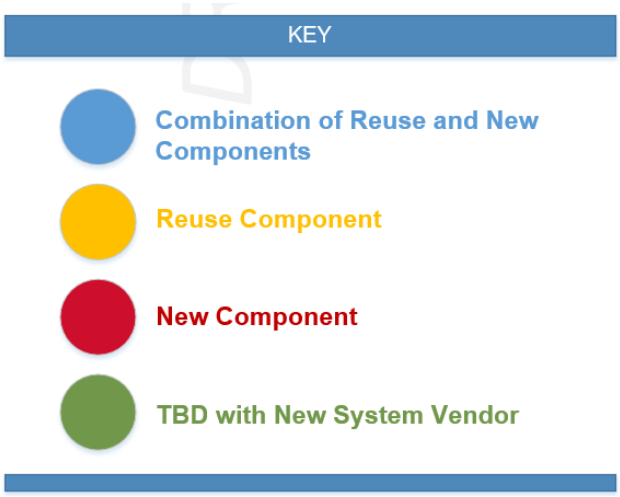
Figure 4: Conceptual System Diagram (High-Level Architecture) for Modernized, Integrated IT Solution



6.0 Conceptual System Design Description

The conceptual system design diagram in Figure 4 on the previous page outlines the supported components within each system layer. The narrative in the following sections provides a high-level description of the key components of the MDHS conceptual system design. The key in Figure 5 links components in the conceptual systems diagram (Figure 4) and the narrative description of each component.

Figure 5: Conceptual System Component Key



6.1 User Interface Layer: "The Front Door"

The MDHS workers are currently limited in their ability to access the application due to legacy 3270 emulation technology, screen scraping, and other updated technology. With technology for user access devices constantly evolving, a more modern solution must be used in future environments. The MDHS users interact with the applications using the following methods:

- 3270 – Emulation technology
- SSH – Screen scraping technology using emulation
- Managed File Transfer – Secure File Transfer Protocol (SFTP)
- Direct Read – Access the legacy systems directly for data read and transfer
- Paper (mail) – Paper forms that are scanned and sent to a team for data entry into the system
- Email – Emails that are sent to a team for data entry into the system
- Fax – Faxes are scanned again and to a team for data entry into the system

- MyMDHS – MDHS Mobile app

The future User Interface Layer, which serves as the “front door” into the modules leveraged by the MDHS, must include support for the most common web browsers across various operating systems. The User Interface Layer must leverage a responsive design—allowing access on desktop computers, laptop computers, tablets, and smartphones—and support federal accessibility standards. Utilizing a modern infrastructure reduces accessibility barriers and allows the system to be used across all user types utilizing different hardware and devices, operating systems, and browsers.

6.2 User Integration/Security Layer

The User Integration/Security Layer of the conceptual system design is designed to manage user authentication and the management of activities between the various types of User Interfaces and the Functional Business Layer. These services provide rule-based, role-based security of access to the system, route users to the appropriate business functions based on role, and independently manage access to different business functions such as client management, application management, or document management. Some of the business reuse components and existing functionality of these services are already in place for the MDHS.

The User Integration/Security Layer provides the security required across systems, such as user authentication, multi-factor authentication (MFA), security compliance, and logging services. This layer focuses on the tools required to protect the business, the role of security in the needs of the business, how to implement proper security function through management and protocols, roles and responsibilities, authorizations, and authentications, as well as when the protection should be provided.

When an operating system used by these devices needs to be updated or a new device and associated technology are required, the user interface changes are accommodated in the User Integration Layer and not in the business application, thus reducing the amount of application code changes required. This approach will facilitate the future needs of the MDHS clients, custodial and non-custodial parents, workforce employers, and State staff, and send notifications as required. User Interface Integration/Security Services requirements are covered in more detail in the MDHS RTM.

6.2.1 Single Sign-On (SSO)

The MDHS already has SSO capability using Azure SSO. The vendor is expected to integrate with these services. These services are already capable of being integrated using existing standards. There is potential that a vendor might include costs in bid prices to replicate and enrich SSO data from the MDHS.

6.2.2 Identity Management (ID)

The Identity Management (ID) component of the conceptual system design is the organizational process that helps ensure individuals have the appropriate access to technology resources. ID management works together with identity and access management (IAM) systems. IAM involves identifying, authenticating, and authorizing a person to access systems, networks, applications, or other resources associating user rights and restrictions with established identities.

In the new system, the identity management tools can be run as applications on a dedicated network appliance or server. The MDHS will need to work with the new system vendor to define and identify the policies for which devices and users are allowed on the network as well as what each user is allowed to do based on their device, location, role-based access, and other factors.

6.2.3 Multi-Factor Authentication (MFA)

Implementing a robust MFA solution instantly secures data and IT resources against identity theft, account spoofing, and phishing. MFA is an electronic authentication method in which a user is primarily granted access to assets of an organization after presenting two or more evidence pieces to an authentication mechanism: knowledge, possession, and inheritance. Each piece of evidence must come from a different category: something they know, something they have, or something they are. To distinctly identify users, MFA uses the following factors to make it more difficult for an unauthorized person to access organizational assets:

- **Knowledge factor (KNOW):** This is something only the legitimate user knows, like a password or a PIN. It is the first security layer.
- **Possession factor (HAVE):** Authentication is performed with something the user possesses, like a mobile phone. For example, this could be code generated via an authenticator app on the phone or communicated to the user through an automated call.
- **Inheritance factor (ARE):** This factor uniquely identifies the user, and it is easily the safest form of authentication. Here, the user's identity is verified using biometrics such as facial or voice recognition or their fingerprint.

Figure 6 illustrates the key components the MDHS needs for a robust MFA.

Figure 6: MFA Key Components

6.2.4 Master Person Index (MPI)

The MDHS expects all program areas leverage an MPI to accurately identify clients across modules and across departments. The MPI will recognize when common data is changed and then share the updates via data exchanges with all applicable systems. This will help to better ensure staff are using the most current known information when working with client records within the system. The MPI will leverage robust algorithms to match records and identifiers from various sources. An MPI would provide unique client identification to not only optimize data sharing across programs, but also help protect against fraud, proactively identifying potential matching clients based on collected data attributes. Data changes made to the MPI are immediately available across program areas.

6.2.5 Role-Based/Rule-Based Access

The MDHS anticipates using role-based access/rule-based access control for controlling the authentication process and authorization of its users. For example, the MDHS rule-based access control would allow the MDHS to control a user's access to areas, devices, or databases according to a predetermined set of rules as defined in the MDHS access permissions and regardless of a person's role within the organization. Role-based access control will allow the MDHS to control a user's access to the MDHS' organizational resources (or assets) and regulate access based on the user's organizational role(s). In a modernized, integrated IT solution the permissions in role-based access control are defined as pairs of assets (the specific system resources) and actions permitted on those resources (the specific operations). These

permissions are not granted directly to individual users; instead, they are assigned to roles that denote job functions, which are then mapped to individual users. A user can be easily reassigned from one role to another.

6.2.6 Security Compliance

The MDHS anticipates that organizational security compliance will be improved in the new system, including the monitoring and assessment of systems, devices, and networks to help ensure they are compliant with regulatory requirements, as well as State and federal security standards.

6.2.7 Infrastructure Security

Infrastructure security, which includes critical infrastructure security, is necessary to help prevent damage to technology assets and data from attacks and disasters. It is also necessary to minimize the amount of damage from such attacks or disasters. Infrastructure security includes the following three types of controls:

- **Access control:** The prevention of unauthorized users and devices from accessing the network.
- **Application security control:** Security measures placed on hardware and software to lock down potential vulnerabilities.
- **Firewall control:** Gatekeeping devices that can allow or help prevent specific traffic from entering or leaving the network.

6.2.8 Privacy Protection and Confidentiality

The new system architecture will comply with state and federal security and privacy requirements for public, community, and private clouds, including State MDHS ESP, State Off-Site and Cloud Hosting, FNS, OCSE, IRS 1075, and SSA.

The new system vendor will need to work with the MDHS to determine the programs are protected entities for health information privacy and protection and confidentiality controls to protect against the unauthorized use of information.

6.2.9 Messaging

The new system vendor will employ diagnostic tools to alert respective teams of any system-related issues or suspicious events.

6.2.10 Logging

The new system vendor will employ a method of tracking and storing all system access data, including failures, to help ensure application availability and to assess the impact of state transformations on performance.

6.3 Authorization/Authentication Layer

The Authentication Layer of the conceptual system design will verify the user's identity. The authorization layer will provide users permission to access information. In the new system, every user must first prove that their identities are genuine before the MDHS administrators grant access to the requested resources. Authentication will work through:

- Passwords – Usernames and passwords are the most common authentication factors. If a user enters the correct data, the system assumes the identity is valid and grants access.
- One-time pins – Grant access for only one session or transaction.
- Authentication apps – Generate security codes via an outside party that grants access.
- Biometrics – A user presents a fingerprint or eye scan to gain access to the system.

Authorization and Authentication Layer requirements are covered in more detail in the MDHS RTM.

6.4 Security Layer (Logging/Monitoring)

The Security Layer of the conceptual design focuses on the tools required to protect the business, role of security in the needs of the business, how to implement proper security function through management and protocols, roles and responsibilities, authorizations, and authentications, and when the protection should be provided. The MDHS seeks layered security as an option for the Security Layer. Layered security refers to security of the systems that use multiple components to protect operations on multiple levels or layers. Security Layer requirements are covered in more detail in the MDHS RTM.

6.5 Functional Business Layer

The Functional Business Layer encompasses the processes and tasks related to the everyday management of clients and client-affiliated records and contains both existing legacy systems and new modules introduced by the chosen vendor.

Functional Business Layer requirements are covered in more detail in the MDHS RTM.

6.5.1 External Web Portal

An external public-facing Client Portal will provide initial, secure access to the MDHS information. It is expected that clients with web portal credentials will have access to the following functionality:

- General information about programs and services
- Forms and applications
- Account management tools
- Status updates
- Scheduling tools
- Policy/procedural documents

6.5.2 Mail Room

Mailroom functions will not be replaced, although the current mail room functionality used by the MDHS can be modernized with automated:

- Classification and identification of routing of critical information and time-sensitive documents
- Routing
- Eliminating manual data entry where possible

6.5.3 Interactive Voice Response (IVR)/Call Center

The User Interface Layer will also provide AI tools tightly coupled with the appropriate modules. Chat Bot services are already in use and will be integrated with the new solution where applicable, unless the chosen vendor uses Chat Bot functionality that exceeds that of which is currently in place within the MDHS systems.

MDHS has a standing call center resource with an IVR that should be integrated with the new solution. It is possible that IVR functionality could be replaced with an included or recommended solution by the new system vendor, should that solution exceed that of which is currently in place. Example call center functionality includes:

- Call tracking and automated routing
- Accessibility to client and call history information
- Accessibility to forms and applications
- Client management

- Client portal assistance tools

6.5.4 Worker Portal

The worker portal used by the MDHS staff will be modernized and updated with a graphical user interface designed to streamline the following functions:

- Data collection
- Data access, including access to a single, unified client record
- Document views
- Application views
- Work queues/tasks
- Access to reports
- Help Desk

6.5.5 Document Handling (Worksite)

Document and content management is currently managed using the existing Worksite solution. Worksite manages the collection, routing, indexing, and retrieval of documents, forms, and correspondence. It is possible that Worksite could be replaced with an included or recommended solution by the new system vendor. Document storage remains critical for the future system, although the MDHS is willing to evaluate solutions from the new system vendor. Required functionality includes:

- Optical Character Recognition ([OCR] added to new capabilities)
- Mail and fax center functionality
- Document scanning and indexing
- Forms processing
- Prioritizing and routing
- Documentation validation and verification
- Policy/procedure documentation

6.5.6 Content Management (iManage)

The MDHS currently uses the content management system iManage. It is expected that this will remain a critical component of a future system. The MDHS expects the new system vendor to

integrate with the MDHS iManage for document management and tracking. Functionality offered within iManage includes:

- Configurable document routing and tracking
- Alert-based workflow rules
- Document/forms creation
- Document/forms review
- Document/forms authentication
- Document tracking
- Digital Signatures (Smartsheet®)

6.5.7 Client Case Management Applications

A critical piece of the Functional Business Layer is the functionality related to client case management. Processes and functionality supported include client management functionality and determination of eligibility and verification of benefits across all programs (for both individuals and families).

6.5.8 Fraud, Waste, and Abuse (FWA)

The MDHS is developing an internal, automated FAM within its eligibility system through Softheon Inc. FAM is a joint platform that is integrated into the Department of Medicaid and the MDHS to verify identities and identify FWA. The MDHS will evaluate the use of FAM in the new system from a cost benefit analysis perspective to determine whether reuse or a vendor-based solution is preferred.

6.5.9 Financial Management

Financial Management functions for child care provider management are depicted as a separate business function since this function is provided as a separate business module. Child care provider management functions and payment ledger functions will remain as reuse components, interfacing with the new system, while financial management functions for child support will be provided by the new system.

6.6 ESB Integration Layer

The ESB Layer decouples systems from one another and enables them to interact without any dependency on or knowledge of one another or other systems on the bus. The ESB layer helps to replace point-to-point integration, which becomes brittle over time, resulting in custom integration code being spread among applications without any central monitoring or troubleshooting. ESB Layer requirements are covered in more detail in the MDHS RTM.

6.7 Information Management Services

The Information Management Services layer of the conceptual system design includes services that govern and manage the MDHS' data. It is expected that the Information Management Services will automate data flow using configurable workflow automation and rules-based document routing to help ensure that data flows to the appropriate resources, improving data quality and consistency. It is within the Information Management Services layer that the verification and validation of data entered into the MDHS applications and databases is managed. MDM tools will be leveraged to provide de-duplication of records and a single client source across the MDHS programs.

Interfaces with external systems are also managed within the Information Management Services layer for all transaction types, including real time, near real time, or batch processing. Interfaces will leverage automation with the MDHS ESB. Information Management Services requirements are covered in more detail in the MDHS RTM.

6.7.1 Directory Services

The new system will store and maintain information such as usernames, passwords, user preferences, and device information.

6.7.2 Workflow Management

Workflow Management is currently maintained through iManage. This includes the flow of tasks, documents, and information across work-related activities performed independently in accordance with the MDHS business rules.

6.7.3 Rules-Based Document Routing

The MDHS is seeking rules-based workflow document routing functionality to help the routing of OCR documents and related document-based tasks to respective workers.

6.7.4 External Web Services

Currently the MDHS uses the following external web services in real time to validate client information. The MDHS expects to integrate with more service partners for real-time data access to validate and verify client and provided related data.

- Client age verification
- Client driver's license verification

6.7.5 Data Governance

Increased data sharing and use across the MDHS programs, other State agencies, and external partners will require establishment of an effective and agreed-upon data governance framework. The MDHS should consider initiating a formal data governance team to define, implement, and oversee a framework that governs the use, accessibility, and security of all system data coming from heterogeneous systems to help ensure data quality, security, and accuracy.

The MDHS expects any chosen solution to adhere to and include a data governance model ensuring that the data architecture and data management policies result in high-quality data and MDM across records, entities, and objects. As part of the data governance model, the system will assign unique high-level client index identifiers to each client while protecting against duplication. In addition, usability functionality that aids data governance is expected, including the ability to merge identified duplicate records, and intuitive searching to help navigate users to the appropriate clients.

6.7.6 Master Data Management (MDM)

The MDHS expects any chosen system to adhere to the MDHS data governance model, ensuring the data architecture and data management policies result in high data quality and MDM across records, entities, and objects. The system must initially load and apply all updates to high-level client index data from all client data sources to an MDM tool and synchronize data changes with all contributing systems per the program rules of each system.

The State might have an enterprise-level MPI in place for use in the new solution, with preference to one utilizing open-source standards. The MPI could serve to bridge the vendor's MDM and existing data requests the MPI can provide. The MPI can also serve as a springboard for data conversion that is necessary for an MDM. If the MPI is used by the vendor to support existing service requests that do not need MDM-level scope, the MDM can push data to the MPI, and the MPI can serve existing connections. This could save the vendor, and the MDHS, some effort replacing MPI interfaces with MDM interfaces. For some data requests, MPI will not suffice, and these applications will need to be enhanced to request data from the MDM. It is also expected that the MPI will share data with the Mississippi Division of Medicaid.

6.7.7 Data Validation and Verification

The MDHS seeks to optimize data validation and verification throughout the system. This includes in-line data validation as data is entered by workers, validation on inbound and outbound data exchange data, and address verification. Melissa Personator® is currently in use by the MDHS to verify, correct, and append all client addresses. Melissa Personator® accurately associates individuals in their respective address as required by the MDHS. The new system must be able to interface with this service or provide equivalent validation functionality.

6.7.8 Reporting Tools

Reporting tools provide both on-demand (i.e., ad hoc) and other analytical reports from the MDHS system either via a Reporting Data Warehouse or directly via the system's Transactional Database(s). The MDHS has existing specialized reporting needs that will not be replaced. This is predominantly in the MDHS CSE program to support the current CSE program vendor with data extracts from State systems that are incorporated into the CSE vendor ecosystem. The new system vendor may have to interface and support the existing CSE vendor or provide continuity with the current CSE vendor, while leaving an opening for alternative approaches depending upon the status of the current CSE vendor contract.

It is expected that the reports that are currently generated and distributed using the iManage solution will be replicated within the new system.

6.7.9 Ad Hoc Reporting

Currently, reports are designed against the MDHS data sources using Cognos, and results are offered to users through the iManage application. Users do not have access to the data to customize reports as needed without going through a report request. The MDHS expects the new system to use a versatile data reporting solution to provide streamlined access to data and outputs, without the need for vendor intervention.

6.7.10 Smartsheet®

The MDHS uses Smartsheet®, an off-the-shelf work management tool, for public-facing and provider-facing portals and often for electronic signatures. While it is possible that an incoming vendor may offer similar functionality that negates the need for Smartsheet®, similar functionality will be managed within the Information Management Services layer.

6.7.11 Interface Management

Currently the MDHS replicates data to a centralized SQL server database, which acts as the main data hub. All interfaces, including batch interfaces, originate from the SQL database. The MDHS seeks a solution where data is consolidated from all the systems through ESB and shared with interface partners as required.

6.7.12 Enterprise Service Bus (ESB)

The MDHS uses an ESB that ties in with some of the services intended for reuse. The enterprise system integrator would integrate the MDHS ESB currently in place and integrate with the existing MDHS' systems. The new system vendor will facilitate data exchange with the new cloud systems. The ESB in place is expected to provide connectivity to services in the MDHS ecosystem that the vendor system will connect to for data exchange.

6.8 Persistence Layer

The Persistence Layer of enterprise applications serves as an intermediary between the business functions of the application and the data it stores in a relational database. This layer maps the business functions to the underlying database for storage. Persistence Layer requirements are covered in more detail in the MDHS RTM.

6.9 Information Layer

The Information Layer contains many sources of data used by MDHS users. It consists of the Transactional Database, the MDHS Document Management System, federally mandated requirements for child support such as the Query Interstate Cases of Kids (QUICK) application and Federal Case Registry, the MDHS Reporting Warehouse, the Judicial E-filing Library, and state and federal agency databases and other major data partners. This information layer should be enhanced with a Business Rules Repository to simplify the maintenance and management of business rules by State staff. A separate rules engine to access, manage, and maintain the business rules and policies may be required to help ensure consistency across the applications. The need for the aggregated logs must be addressed with access to collective aggregated logs from all the systems for systems analytics. Information Layer requirements are covered in more detail in the MDHS RTM.

6.9.1 Content Management System

The current content management system used by the MDHS is iManage, a third-party document management system (formerly owned by Hewlett Packard) that stores reports from jobs run in legacy systems, manages correspondence forms, care files, applications, attachments, and more. The system is heavily used by the MDHS and delivers reports to a user's inbox, manages alerts, and leverages dashboard functionality. The new system must provide equivalent content management functionality or integrate with iManage.

6.9.2 Analytics

Currently IBM® Cognos is used to provide basic data analytics capabilities across the MDHS programs. The MDHS is currently transitioning from Cognos to the MS Power BI analytics solution. It is expected that the new system will integrate with the MDHS' chosen analytics solution or offer equivalent functionality while adhering to the MDHS' data governance policies to provide accurate, unduplicated reports across populations and programs. The new system should provide powerful aggregation and visualization capabilities used by workers across distinct roles.

The analytics solution must aggregate data from multiple data sources to support reporting, data cleanup, data mining, pattern recognition, and machine learning (including interoperability with machine learning languages/platforms such as Python, AzureML, AWS, Snowflake, etc.).

- **Analytics Dashboard:** Visual dashboards derived from the MDHS analytics solution are necessary components to monitor, track, and display key performance indicators (KPIs), metrics, and important measures. The new system must provide secure, role-based access to dashboards, allow users to optimize their caseloads and efficiency, and provide better insight into data trends across all the MDHS programs.

6.9.3 Major Data Exchange Partners

The MDHS legacy databases for all applications are replicated live to an SQL database for all data exchange and reporting needs. Some of the interfaces utilize a direct read into the system. In addition, some of the inbound interfaces already use some real-time interfaces for receiving and processing external data (e.g., driver's license information, age verification). All secure data exchange with the new cloud-based system will occur in real-time, near real-time, and in asynchronous and batch modes with preference to real-time data exchange. The MDHS would like to include other inbound interfaces as part of the real-time interface model.

6.9.4 Reporting Warehouse

Currently Cognos is the main tool used by the MDHS for analytics, including State and federal reporting. The new system must aggregate data in accordance with the MDHS data governance policies and MDM model to manage data analytics, State and federal reporting, quality assurance/quality control, compliance reporting, and other program metrics.

6.9.5 Business Rules/Policies

The MDHS currently has business rules, program rules, and regulations hardcoded into various legacy applications. The MDHS seeks to have all these rules and regulations consolidated in a Business Rules Management System (BRMS). The BRMS should include:

1. State program rules, regulations, guidelines
2. Federal program rules, regulations, guidelines
3. Relationship metadata

6.9.6 Aggregated Logs

Currently the MDHS logs are scattered across systems. The MDHS expects the new system vendor to import logs from many sources across the MDHS organizational infrastructure, collect and aggregate into a central location, and provide reporting and analytics.

6.10 Additional Capabilities

The following additional system capabilities are recommended for a modernized, integrated system. The additional capabilities align with the MDHS' objectives for desired IT system

improvements, including the requirements, capabilities, features, and/or enhancements not supported by the current legacy IT systems, and are documented in the MDHS RTM.

6.10.1 Services Registry

The new MDHS system requires a service registry for the storage of data structures for application-level communication and to serve as a central location where app developers can register all SOA services, micro-services, or APIs that are available for use

6.10.2 Data Exchange Services

The new MDHS system requires a data exchange where the process of sharing and exchanging data is structured under a source schema and transformed into a target schema, so that the target data is an accurate representation of the source data. The data exchange services in the new system should allow data to be shared between different computer programs, in real time with instant requests and a response in the same transaction. In the new MDHS system, the request and response may be different transactions, and middleware software may need to be used to track the requests and responses. Typically, the request and response are not synchronous, and the asynchronous processing of requests occurs in a batch.

6.10.3 Workflow Automation

The new MDHS system requires workflow automation to improve the flow of tasks, documents, and information across work-related activities in accordance with MDHS' predefined business rules. Using the rules-based workflow, the processes will need to be configured with minimal changes to the processes and with changes to the rules.

- **Workflow Configuration Management:** The MDHS will manage the definition and configuration of workflow automation rules, allowing for rapid modification as business processes and policies evolve. The MDHS workflows should be automated whenever possible for numerous reasons, including faster operations and increased efficiency and accuracy. Other improvements include the following:
    - Workflows create increased task efficiency, allowing employees to work on other non-automated tasks
    - Due to increased productivity, cost savings can be achieved
    - Workflow automation creates processes that are more transparent, giving an organization a top-down view of its workflows
    - Communication improvement with employees can be achieved with increased visibility
    - Automation of customer services provides better customer service

    - Processes can be improved because of an increased and mapped-out visibility of workflows
    - Task redundancies can be easily identified and removed in a workflow
    - Provides better overall product as human error is minimized

- **OCR and Rules-Based Document Routing:** Currently the MDHS uses paper and fax applications submitted by clients who may not have access to online resources. These applications are scanned and uploaded to Worksite for processing along with a cover sheet and stored as PDF. Fax applications received are also scanned again to create a PDF file and upload to Worksite. The MDHS seeks to automate this process of paper and fax applications through OCR and create the application in the system and assign the task to a worker based on predefined rules to review, edit, and complete the submission.
- **Rules-Based Document Routing:** The MDHS seeks workflow document routing to assist in the routing of OCR documents and related tasks to respective workers. Rules-based document routing also helps to:
    - Create workflow definitions and recurring workflows
    - Track and audit assigned tasks
    - Identify tasks that are past-due
    - Identify workloads of different individuals and their performance
    - Standardized document and task handling through business process automation
- **Task Management:** The MDHS seeks to use the workflow automation to better manage the rules-based, role-based task management functionality, allowing workers to easily keep track of both the automatically generated and manually generated tasks for which they are responsible. Task lists will be dynamic and interactive, accompanied securely by external alerts through common methodologies including SMS text and email. Users should be able to monitor and manage task statuses with clear visibility into overdue or high-priority tasks via automated alerts or customized dashboards.

6.10.4 Business Rules Management Service (BRMS)

A BRMS is a technology system used to capture any business decision logic as a business rule, which is then cataloged, stored, and automated across applications. Instead of embedding rules as code within multiple applications across the systems, with a BRMS, the rules are externalized and managed away from application code. The MDHS seeks to have a BRMS with the following components:

- **Business Rules Engine (BRE):** A BRE is a software tool that executes one or more cataloged business rules of a business process in a runtime production environment.

The decisions are made according to predefined rules and conditions loaded into the BRE.

- **Business Rules Repository (BRR):** The BRR is a repository for the MDHS business rules and other decision-making artifacts. It is similar to a database or source code management system since it uses those technologies to manage Decision Management artifacts. Some of the BRR capabilities include:
    - Sharing of ownership of business rules in general--BRR assists in the sharing and collaboration which significantly reduces the time for rule creation and rules management.
    - A built-in database allows for storage capabilities along with logic backup
    - Visual user interface for ease in the creations and maintenance of rules
    - Versioning and tracking for traceability or for convenient “roll-back”
    - Access to the repositories based on roles and responsibilities and configured with authentication
    - Search options for help in finding a rule as rules repositories grow
    - Analysis of business rules to detect potential anomalies such as gaps, overlaps, or any kind of inconsistencies and executing business rules against predefined test cases and highlights discrepancies between the expected outcome and the actual result
    - Ability to add meta-information for finding business rules based on criteria that may be independent of the content of the rule
    - Ability to catalog business logic
    - Adherence to a predefined and approved promotion process for all the business rules through all the lower and higher environments

6.10.5 Performance Monitoring/Capacity Planning

The MDHS will define requirements for performance monitoring and capacity planning for the new system. The MDHS will also require that the new system vendor provide a process to regularly collect and analyze performance information, including performance indicators and performance goals.

- **Capacity Management:** The MDHS will also require that the new system vendor provide capacity management, including:
    - Establishing and maintaining a capacity management plan to meet current and future workloads
    - Ensuring performance goals are met on time and within budget
    - Monitoring capacity continuously to support the service-level management process
    - Diagnosing and resolving incidents
    - Analyzing capacity variances and taking proactive measures to improve performance when cost-effective

6.10.6 Communication Channels/Communications Management

The new system vendor is expected to enhance the existing Communications Generation Tool and to enhance existing notices. The new system vendor is required to provide monitoring tools to monitor the communication channels to alert respective teams of any system-related issues or suspicious events. The new system vendor will be able to use either the report description files and/or the design documentation from the SNAP Notices Replacement Project immediately.

6.10.7 Record Management/Record Retention Services

The MDHS seeks a Records Management and Records Retention service that would automate the data retention and archival as per the State and federal requirements and based on the MDHS' retention policies. The MDHS requires that the new system retain the entire history file of a closed case in an accessible automated manner, based on federal and/or State requirements, after case closure, or until resolved under any auditable action. Further, if any litigation, claim, negotiation, or other action has started prior to the expiration of the retention period, then the records must be maintained in accordance with each program area's record retention rules.

6.10.8 Disaster Recovery (DR) and Business Continuity (BC)

The MDHS will define requirements for BC and DR for the new system. The MDHS will also require that the new system vendor provide a BC and DR Plan as a deliverable. The plan might include:

- Maintaining essential business processes in the event of natural disasters, hardware or software failures, human error, or other contingencies that could disrupt business operations
- Recovering business functions, human resources, and technology infrastructure associated with the new cloud-based system
- Participating in the alternative site readiness along with DR exercise on the MDHS-approved frequency
- Providing the MDHS-approved Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Developing threat considerations (natural, technical, human, etc.) with impact assessments, including:
    - Strategies for recovering key assets, such as facilities, hardware, software, data, and customer service, and key personnel responsible for the recovery plans and related procedures
    - Cloud system data backup, retention, and restoration processes
    - Testing procedures for the BC and DR Plan
    - Procedures and policies to adopt in the event of an unplanned disruption of business operations, such as loss of utility service, building evacuations, or a disaster such as a fire, flood, earthquake, etc.
    - Required hardware, software, data, and communications components to provide alternative site operations for production and development
    - Process for duplicating the cloud-based system at the alternative site, specifying the retention period for all application and operating components
    - Steps required for troubleshooting, replacing, reconfiguring, and restoring the cloud-based system
    - Processes utilized to verify the health and accuracy of cloud-based system backups
    - Conditions that trigger the MDHS to use the alternative site
    - Procedures for testing the alternative site

7.0 System Configuration Recommendations

The MDHS is considering using the existing ESB solution to support a modernized, integrated system. Ideally, this would be implemented as a two-step process that requires the review of the current ESB architecture and upgrade as a first step, followed by integration to include other applications. BerryDunn recommends the MDHS begin with an enterprise systems integrator that is vendor-agnostic and brings in the tools, skillsets, and staff to lead and manage Enterprise Application Integration (EAI).

An enterprise systems integrator can help standardize the MDHS business processes and prepare the agency for a digital transformation. Enterprise systems integrators have expertise in assessing all IT systems and applications, providing infrastructure expertise, and creating a roadmap for upgrading and integrating them. As part of this process, the MDHS should consider establishing a formal intake process to evaluate applications, database, and infrastructure configuration items as they are integrated into the environment through the ESB.

The MDHS might consider providing oversight resource(s), such as an Architecture Review Board (ARB), that reviews the current MDHS landscape, helps develop a system architecture roadmap, and recommends a technology stack in alignment with the MDHS' goals, strategies, objectives and broader technology plan. An ARB can help ensure cross-project collaboration, coordination, consistency, and outcomes that support the MDHS.

Additional activities an ARB might perform include, but are not limited to:

- Review and make recommendations related to technology decisions on an ongoing and timely basis
- Evaluate conformance with the MDHS future system vision
- Evaluate conformance with agreed upon technology and architectural standards
- Disseminate architectural standards and technology roadmaps
- Assess and review new technologies
- Assess and identify technologies for retirement and replacement

Benefits of an ARB include:

- Mitigation of risks and potential negative impacts to the business by using due diligence and more informed technology decision-making processes
- Improved efficiency and cost control through reuse and consolidation of technology and by using more informed decision-making processes
- Optimization of technology investments and resources
- Management of complexity in the MDHS enterprise by establishing enterprise architecture and technology compliance

Risks of not having an ARB include:

- Maintaining old technology in the absence of a governance body that assesses and reviews technologies for replacement or retirement
- Duplication of efforts and reduction in the quality of applications
- Incremental, fragmented implementation of technologies that might not align with the existing system architecture or recommended technologies
- Non-compliance with an overarching enterprise architecture for complex projects
- Lack of adherence to industry best practices for technology stacks and architecture

Other considerations include:

- Incremental systems integration without a dedicated enterprise systems integrator could result in multiple vendors owning the role of system integrator, leading to conflicts and impacts to the MDHS' modernization goals
- Lack of a dedicated enterprise systems integrator might result in conflicts between various solution vendors and create project delays
- Lack of a dedicated enterprise systems integrator might result in an underestimation of necessary infrastructure changes, i.e., should the MDHS focus solely on prioritized projects, then the broader vision may be missed, which in turn could lead to siloed planning and scoping of the project, limited ability to identify risks or impacts to the overall MDHS' roadmap, and higher risk of not meeting the desired project roadmap outcomes and milestones
- Incremental implementation might increase costs and MDHS' resource commitment if re-work is required as new project initiatives begin, or if the implemented structure is found to not support overall the MDHS' needs
- The risk and burden to the MDHS IT and PMO team to manage multiple vendors and their systems' integration might be increased

Appendix A: Glossary of Acronyms

Table A1 lists and defines acronyms used in this deliverable.

Table A1: Glossary of Acronyms and Terms

Acronym/Term	Definition
Adabas	Adaptable Database System
API	Application Programming Interface
BC	Business Continuity
BRE	Business Rules Engine
BRR	Business Rules Repository
BRMS	Business Rules Management System
CARS	Client Application and Registration System
CCCP	Child Care Certificate Program
CCPP	Child Care Payment Program
CCPS	Child Care Payment System
CCR&R	Child Care Resource and Referral
COBOL	Common Business-Oriented Language
COTS	Commercial Off-the-Shelf
CRS	Case Review System
CSE	Child Support Enforcement
CWP	Common Web Portal
DDI	Design, Development, and Implementation
DOH	Department of Health
DR	Disaster Recovery
DRAAS	Disaster Recovery as-a-Service
DSNAP	Disaster Supplemental Nutrition Assistance Program
EAI	Enterprise Application Integration
ECA	Early Childhood Academy
E&T	Employment and Training
EBT	Electronic Benefit Transfer
EDP	Employability Development Plan
eFITS	Electronic Financial Interface Tracking System

Acronym/Term	Definition
EPPIC	Electronic Payment Processing and Information Control
ESP	Enterprise Security Policy
FNS	Food and Nutrition Service
FS	Feasibility Study
FWA	Fraud, Waste, and Abuse
ID	Identity Management
iOS	iPhone Operating System
IT	Information Technology
ITS	Information Technology Services
IVR	Interactive Voice Response
IV&V	Independent Verification and Validation
IBM®	International Business Machines
JAWS	Jobs Automated Work System
LARS	Child Care Licensing System
LIHEAP	Low-Income Home Energy Assistance Program
M&O	Maintenance and Operations
MAVERICS	Mississippi Application, Verification, Eligibility, Reporting, & Information Control System
MDES	Mississippi Department of Employment Security
MDHS	Mississippi Department of Human Services
MDM	Master Data Management
MECIC	Mississippi Early Childhood Inclusion Center
MEMA	Mississippi Emergency Management Agency
METSS	Mississippi Enforcement and Tracking of Support System
MIS	Management Information Systems
MOTS	Modified Commercial Off-the-Shelf
MPI	Master Person Index
MS	Microsoft
OCR	Optical Character Recognition
OCSE	Office of Child Support Enforcement
OIG	Office of Inspector General

Acronym/Term	Definition
OOTB	Out-Of-The-Box
PMO	Project Management Office
QA	Quality Assurance
QC	Quality Control
RTM	Requirements Traceability Matrix
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SNAP	Supplemental Nutrition Assistance Program
SNAP-ED	Supplemental Nutrition Assistance Program Education
SNAP E&T	Supplemental Nutrition Assistance Program Education & Training
SOA	Service-Oriented Architecture
SQL	Structured Query Language
SSA	Social Security Administration
SSO	Single Sign-On
State	State of Mississippi
TANF	Temporary Assistance for Needy Families
TWP	TANF Work Program
USDA	U.S. Department of Agriculture
WFD	Workforce Development

Appendix B: Glossary of Terms

Table B1 lists and defines the common terms[1] used throughout this report.

Table B1: Glossary of Terms

Term	Definition
Application Programming Interfaces	A connection between computers or between computer programs.
Asynchronous	Transmission of data without the use of an external clock signal.
Authentication	The act of validating that the user is whom they claim to be. This is the first step in any security process. Authentication is visible to and partially changeable by the user.
Authorization	The process of giving the user permission to access a specific resource or function. Authorization is not visible to or changeable by the user.
Batch	When the requests or processes are batched together for processing automatically with minimal human interaction.
Commercial Off-the-Shelf	Products that are packaged or canned (ready-made) hardware or software, which are adapted aftermarket to the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions.
Chat Bot	A software application used to conduct an online chat conversation via text or text-to-speech, in lieu of providing direct contact with a live human agent.
Data Warehouses	Central repositories of integrated data from one or more disparate sources. They store current and historical data in one single place that is used for creating analytical reports for workers throughout the enterprise.
Enterprise Service Bus	A communication system between mutually interacting software applications in an SOA. It represents a software architecture for distributed computing, and is a special variant of the more general client-server model, wherein any application may behave as server or client.
Enterprise System Framework	An information system application that can be configured or customized and consists of several modules and integrates data, information, and business processes in an organization and between organizations.
Independent Verification and Validation	Independent procedures that are used together for checking that a product, service, or system meets requirements and specifications and that it fulfills its intended purpose.
Interactive Voice Response	Technology that allows humans to interact with a computer-operated phone system using voice and dual-tone multi-frequency signaling (DTMF) tones input via a keypad.

[1] https://en.wikipedia.org

Term	Definition
Machine Learning	Part of artificial intelligence that uses algorithms to build a model based on sample data, known as training data, in order to make predictions or decisions.
Master Data Management	Technology-enabled discipline in which business and IT work together to ensure the uniformity, accuracy, stewardship, semantic consistency, and accountability of the enterprise's official shared master data assets.
Master Person Index	A database used by organizations to maintain accurate data across its various departments. Clients are assigned a unique identifier, so they are represented only once across all the organization's systems.
Modifiable Commercial Off-the Shelf	A COTS product whose source code can be modified. The product may be customized by the purchaser, by the vendor, or by another party to meet the requirements of the customer.
Near Real-Time	When the request and response are different transactions and there is a lag between the request and the response. Typically, middleware software is used to track the requests and responses.
Real-Time	When a system responds to the request of information at a speed that is near-instantaneous or has a short delay from when the event occurred. Usually, the request and response are in the same transaction and instantaneous.
Recovery Time Objective	The maximum acceptable delay between the interruption of service and restoration of service. This determines an acceptable length of time for service downtime.
Recovery Point Objective	The maximum acceptable amount of time since the last data recovery point.
Single Sign-On	An authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.
Security	Security is a collection of technical approaches that address issues covering physical, electronic, and procedural protection for information collected.
Service-Oriented Architecture	An architectural style that supports service orientation in software design where services are provided to the other components by application components, through a communication protocol over a network.
System Integrator	A person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems function together.
Workflow Automation	Software developer production of a list of actions to automate a task and interface to the back-end system using internal application programming interfaces (APIs) or dedicated scripting language to assist the user in

Term	Definition
	performing a task, allow access to appropriate tools and methods, and make available suitable information resources.

Appendix C: Sources

Table C1 includes a non-exhaustive list of key documents and other sources of information BerryDunn used for the conceptual system design. Links to source documents are located on the MDHS SharePoint site HERE. Website links are included in the table below.

Table C1: Sources

No.	Document Name	Resource/Reference	Date
1	Architecture Flow Diagram DRAFT	MDHS	08/23/2018
2	CWP Architecture	MDHS	01/13/2021
3	MDHS Architectural Overview	MDHS	09/09/2020
4	MDHS Business Architecture Presentation	MDHS	09/02/2021
5	MDHS Data Analysis – MDHS Ecosystem, v2	MDHS	Unknown
6	OCSE Streamlined Feasibility Study Guide	Streamlined Feasibility Study for Child Support System Modernization	12/15/2020
7	Automated Systems for Child Support Enforcement: A Guide for States	Automated Systems for Child Support Enforcement: A Guide for States	09/19/2017
8	USDA: FNS Handbook 901, Version 2.4, January 2020	FNS 901 Handbook	01/01/2020
9	MDHS Legacy IT Systems Assessment Project, Deliverable 2. Legacy IT Systems Assessment Report and RTM	MDHS	12/03/2021
10	MDHS Legacy IT Systems Assessment Project, Deliverable 3. Alternatives Analysis Report	MDHS	02/04/2022
11	MDHS SRP Planning Roadmap v12152021	MDHS SRP Planning Roadmap v12152021	12/16/2021

Appendix D: Project Participants and Meetings

Table D1 provides a list of meetings that BerryDunn facilitated with the MDHS stakeholders to gather information for the conceptual system design. In addition to the meetings listed below, BerryDunn participated in weekly project status and Executive Steering Committee meetings, during which the MDHS project leadership and the BerryDunn core project team shared and discussed project information.

Table D1: Project Participants and Meetings

Meeting	Meeting Date	MDHS/Other State Invitees[2]
MDHS System Design Discovery Session 1 (Issues/Constraints and Performance Requirements)	March 11, 2022	Richard Taylor; Cheryl Joiner; Marcus Gentry; Beverly Williams; Eric Coleman; Michael Wise; Kevin Keniston; Jesse Nicholson; Thomas Costa; Johnny Waldrop; Guy Sylvester; Brenda Wilson; Thomas Hederman; Jason Campbell; Jay Harper; Jennifer Allen; Chad Shook; Eleanor Monroe; George Berry; Breanne Anderson; Angela Ware; Sridhar Kota; Cynthia Edwards; Angela Crockett; Shane Cooley; Kristi Kinnel; Laura Mallery; Tina Ruffin; Donald Truett; Melissa Goodson; Mark Allen; Rachelle S. Richardson; Steve Stanford; Chad Allgood; Sandra Griffith; Patrick Black; Nathan Wilson; Bob Anderson; Daniel Gallarno
MDHS System Design Discovery Session 2 (System Operating Environment and System Diagram/Narrative)	March 11, 2022	Richard Taylor; Cheryl Joiner; Marcus Gentry; Beverly Williams; Eric Coleman; Michael Wise; Kevin Keniston; Jesse Nicholson; Thomas Costa; Johnny Waldrop; Guy Sylvester; Brenda Wilson; Thomas Hederman; Jason Campbell; Jay Harper; Jennifer Allen; Chad Shook; Eleanor Monroe; George Berry; Breanne Anderson; Angela Ware; Sridhar Kota; Cynthia Edwards; Angela Crockett; Shane Cooley; Kristi Kinnel; Laura Mallery; Tina Ruffin; Donald Truett; Melissa Goodson; Mark Allen;

[2] Meeting invitees may not have attended the meetings as listed above.

Meeting	Meeting Date	MDHS/Other State Invitees[2]
		Rachelle S. Richardson; Steve Stanford; Chad Allgood; Sandra Griffith; Patrick Black; Nathan Wilson; Bob Anderson; Daniel Gallarno
MDHS System Design Discovery Session 3 (Diagram/Narrative)	March 21, 2022	Richard Taylor; Cheryl Joiner; Marcus Gentry; Beverly Williams; Eric Coleman; Breanne Anderson; Michael Wise; Kevin Keniston; Jesse Nicholson; Thomas Costa; Johnny Waldrop; Guy Sylvester; Brenda Wilson; Thomas Hederman; Jason Campbell; Jay Harper; Jennifer Allen; Chad Shook; Eleanor Monroe; George Berry; Angela Ware; Sridhar Kota; Cynthia Edwards; Angela Crockett; Shane Cooley; Kristi Kinnel; Laura Mallery; Tina Ruffin; Donald Truett; Melissa Goodson; Carol Girod; Mark Allen; Rachelle S. Richardson; Steve Stanford; Chad Allgood; Sandra Griffith; Patrick Black; Nathan Wilson; Bob Anderson; Daniel Gallarno; Jeanette Rhodes; Latitia Kennedy; Marilyn Williams; Kristine Jefferson; Rick Dawkins; Sherry M Jackson