*For instructions on using this template, please see Notes to Author/Template Instructions on page 11.*

**Healthy Body Wellness Center (HBWC)**

# High-Level Technical Design

**Version X.X**

**Table of Contents**

[High-Level Technical Design 1](#_Toc525646265)

[1. Introduction *(Not required for performance assessment)* 4](#_Toc525646266)

[2. Current Systems 4](#_Toc525646267)

[3. Goals, Objectives, and Rationale for New or Significantly Modified System 4](#_Toc525646269)

[3.1 Project Purpose 4](#_Toc525646270)

[3.2 System Goals and Objectives 4](#_Toc525646271)

[3.3 Proposed System 4](#_Toc525646272)

[3.3.1 System Scope 4](#_Toc525646273)

[3.3.2 Processes Supported 4](#_Toc525646274)

[3.3.3 High-Level Functional Requirements 4](#_Toc525646275)

[3.3.4 Summary of Changes 5](#_Toc525646276)

[4. Factors Influencing Technical Design 5](#_Toc525646278)

[4.1 Relevant Standards 5](#_Toc525646279)

[4.2 Assumptions and Dependencies 5](#_Toc525646280)

[4.3 Constraints 5](#_Toc525646281)

[4.4 Design Goals 5](#_Toc525646282)

[5. Proposed System 5](#_Toc525646284)

[5.1 High-Level Operational Requirements and Characteristics 5](#_Toc525646285)

[5.1.1 User Community Description 6](#_Toc525646286)

[5.1.2 Nonfunctional Requirements 6](#_Toc525646287)

[5.2 High-Level Architecture 6](#_Toc525646288)

[5.2.1 Application Architecture 7](#_Toc525646289)

[5.2.2 Information Architecture 8](#_Toc525646290)

[5.2.3 Interface Architecture (*not required for performance assessment)* 8](#_Toc525646291)

[5.2.4 Technology Architecture 8](#_Toc525646292)

[5.2.4.1 Platform 9](#_Toc525646293)

[5.2.4.2 System Hosting 9](#_Toc525646294)

[5.2.4.3 Connectivity Requirements 9](#_Toc525646295)

[5.2.4.4 Modes of Operation 9](#_Toc525646296)

[5.2.5 Security and Privacy Architecture 9](#_Toc525646297)

[5.2.5.1 Authentication 9](#_Toc525646298)

[5.2.5.2 Authorization 9](#_Toc525646299)

[5.2.5.3 Encryption 9](#_Toc525646300)

[6. Analysis of the Proposed System 10](#_Toc525646301)

[6.1 Risks 10](#_Toc525646302)

## Introduction

*Not required for performance assessment.*

## Current Systems

*Healthy Body Wellness Center (HBWC) is a company that promotes health and overall wellbeing by providing grants to local hospitals. These grants are funded through Office Grants Giveaways (OGG) which uses a system called the Small Hospital Grant Tracking System (SHGTS). All grant applications submitted into SHGTS are checked against data collected by the National Institute of Health (NIH). After being reviewed and approved by the Executive Review staff, grants are given to applicants to use for a period of 30 days. If any funds remain unused, they are returned to HBWC's OGG for use by other approved grant applicants. The technology infrastructure that supports the grant system is located in an unsecured area in the basement of HBWC's main office. The environmental controls in this area need to be updated to create a more efficient server room.*

*The grant system, known as the SHGTS, is housed in a Microsoft Access 2010 database that runs on a Microsoft Server 2008 R2 system. This is a single-user system that can only be accessed by one department, company, or grant applicant at a time. Data transmissions from the NIH must be scheduled at specific times of the day to avoid interference with the Executive Review Staff or Grant Applicants. The SHGTS is currently run on a small desktop computer that is connected to HBWC's local area network (LAN), which is in need of a redesign to better secure ACH transmissions from the Accounting Department, allow secure third-party connections for the OGG & NIH, and enable secure employee remote access. HBWC staff can access the database remotely via a VPN connection.*

*The SHGTS database contains grant and applicant information, as well as other private health information, which has been identified as unsecure during a Security Assessment Review conducted by Endothon Security Consulting group. HBWC's web servers have also been identified as unsecure due to the lack of cryptographic controls, auditing, and user accounts that fail to meet the company's security objectives.*

*In addition to the SHGTS, HBWC uses QuickBooks, which is a database employed by the Accounting Department. The QuickBooks system specifically contains information about employee salaries, job titles, and dates of employment for both current and past employees and is not directly connected to the SHGTS.*

## Goals, Objectives, and Rationale for New or Significantly Modified System

### Project Purpose

*The main purpose of this project is to modernize HBWC’s SHGTS in order to make the application process more efficient and improve accessibility for internal staff, external partners, and grant applicants, and update the company's online security protocols. Although some of the data stored on the Microsoft Access 2010 database will be transferred to the cloud, the primary objective is to enhance the system's functionality and security.*

### System Goals and Objectives

*The current SHGTS process contains several impediments that will be outlined below, along with their respective proposed solutions.*

***Current System Issues & Impediments***

1. *Current Server is outdated:* *The current SHGTS database is located on a Microsoft Windows Server 2008 R2 system, which has reached its "end of life" under Microsoft as of January 2020. The system has not received any security updates or patches for over a year. While the current security measures are effective, relying solely on the concept of Security through Obscurity is not a sufficient means to protect the sensitive financial data of both the NIH and the small hospitals that receive grants from HBWC.*
2. *Database is outdated:* *the SHGTS database is outdated as it is set up in Microsoft Access 2010 (which has reached its EOL under Microsoft as of October 2020), which cannot support multiple concurrent database connections, a feature required in modern database systems. However, the SHGTS is regularly accessed by several departments including Executive Review, Accounting, NIH, and small hospital applications.*
3. *Weakened security posture: Endothon Security Consulting's Security Assessment Report identifies various security loopholes, such as shortcomings in user access rights, improper system access, and the lack of effective remote access to the SHGTS system.*

*With this project we aim to address the above system issues using a cloud-based infrastructure via Microsoft Azure, as we want to maintain rapport with our reliable vendor Microsoft. We also want to update the current database to a new Microsoft SQL database, and because we will no longer be dealing with EOL systems and software, the new system receives the latest Microsoft security updates.*

### Proposed System

*The proposed system will concentrate on migrating the SHGTS from onsite to a cloud-based Microsoft Azure infrastructure utilizing a Microsoft SQL database. The new database will hold imported data from the older Microsoft Access 2020 system. For the new cloud-based system it is imperative that we will be implementing updated security procedures related to access policies (principle of least privilege, role-based access control, etc.) and stronger authentication processes using MFA.*

#### System Scope

*The scope of this project will focus on migrating the SHGTS from onsite to a cloud-based Microsoft Azure infrastructure utilizing Microsoft SQL database. This will assist with our modernization initiative and concentrate on:*

***Primary goals:***

* *Cloud migration and integration*
* *Database migration*

***Secondary Goals:***

* *Disaster recovery planning*
* *Secure remote access via VPN*
* *Implementation of suitable access policies and privileges*

#### Processes Supported

*The main objective of this project is to assist and manage the business process related to the implementation and setup of our new cloud-based systems, as well as remote access, security, and logging/reporting. To illustrate, new remote policies will be established such as defining system access rules, monitoring all actions taken in the remote environment, and generating reports on these activities once the remote setup is in place.*

#### High-Level Functional Requirements

***Instructions: Base Functionality:***

*The main priority of this project is to obtain IaaS access from Microsoft Azure for the modernization of HWC's IT infrastructure.*

*Migrate from Access 2010 to Microsoft SQL environment to significantly improve the system's access and streamlining the grant application process.*

***Security Requirements:***

*Access auditing: to identify who needs access to which systems and why to improve remote access initiatives and enhance system security.*

*Secure retired database: After the cloud migration the IT Department will maintain offline backup copies of the old system. This will protect against data loss and provide a fallback environment in case of disaster.*

*Setting up multi-factor authentication will help to secure remote connections to the Microsoft Azure system.*

***Reporting Requirements:***

*Grant view-only access to hospital applicants: Applicant hospitals need to set up new logins to the system to track the status of their applications.*

*Grant access to Executive Team Staff: The Executive Team requires reporting access to run ad hoc reports for review of grant applications.*

*Grant read/write access to NIH: requires read/write access to the database as the application approval process is based on information from NIH.*

*The Security Administrator for HBWC needs to also regularly review access logs to verify that there is no unauthorized or elevated access to the systems.*

***Usability Requirements:***

*Allow remote access is necessary for improving the workflow of applications and partners, as well as HBWC's internal IT Department.*

***Auditing Requirements:***

*A report needs to be prepared once the modernization via this project has been completed. It will certify that the old system has been retired, is secure, and scheduled for secure destruction after one year.*

## Factors Influencing Technical Design

### Relevant Standards

*The Office of Grants Giveaways (OGG) at Healthy Body Wellness Center (HBWC) utilizes data from the National Institute of Health to aid in their decision-making process for the Small Hospital Grant Tracking System. As the National Institute of Health is a federal agency, it is required to adhere to the Federal Information Security Management Act (FISMA), which is a government-established system based on the Risk Management Framework (RMF) of the National Institute of Standards and Technology (NIST). This framework is designed to safeguard operations and information from online threats. Although contractors and grant recipients are not obligated to comply with FISMA, the requirements are based on the NIST RMF framework and are widely considered the minimum-security standards that an organization must follow concerning cybersecurity. As a frequent grant recipient and partner of NIH, HBWC aims to align itself more closely with the FISMA standards.*

*The following requirements of FISMA were summarized in the Endothon Security Consulting SAR as listed below:*

* *Implement security controls.*
* *Methods to ensure that risks and potential for loss are continuously assessed.*
* *Conduct continuous monitoring of system access.*

*The following constraints were identified within the current system by SAR:*

1. *PICA-01: Improper system access for users*
2. *PWC-03: No effective user login for accessing grant information at the web server.*
3. *P-DC01: No data classification controls allowing access to any data within the organization.*
4. *P-SA02: Users not tracked for access or data rights.*

*The above threats outlined by the SAR will be addressed through some secondary features that will be implemented with the new infrastructure and database:*

* *A remote environment via VPN allowing HBWC’s IT Department and employees access based on the principle of least privilege.*
* *A new DRP managed and outlined by Microsoft’s datacenter.*
* *Remote governance and MFA*

*There are other aspects of HBWC’s infrastructure and business processes that need to be reviewed and modernized, the scope of this project will mainly be in accordance with the FISMA and NIST standards mentioned above.*

### Assumptions

*It is expected that by the end of this project, HBWC's OGG and S.H.G.T.S will operate on a modern SQL database and provide a more secure server environment. It should be kept in mind that some other aspects of HBWC's security processes that are dependent on these systems may also require attention while implementing the Microsoft Azure IaaS modernization project.*

### 4.3 Dependencies

*HBWC's IT Department must create new remote management policies, which will incorporate an audit of employee access to the system to identify which systems and information each employee requires access to. Access logging will be implemented for auditing purposes to ensure that no user accounts have improper access/elevated privileges, and a multi-factor authentication policy will be introduced to assist in managing remote security.*

### Constraints

* High speed internet access for efficient cloud services/application performance.
* Additional platform training for HBWC’s IT Department
* A continued partnership with Microsoft may develop future issues if HBWC were to ever switch over to a competing system.
* Hiring and establishing additional roles to support new system. HBWC may need to consider hiring a SQL Database Admin to manage the new SQL database.
  + 1. **Design Goals**

*Endothon Security Consulting SAR identified various areas where HBWC must improve its infrastructure to align with contemporary security designs, policies, and processes. Following a meeting with the HBWC's Board of Directors, the IT Department has determined that the first step in addressing these shortcomings will be to upgrade the infrastructure by carrying out a cloud-based uplift of its server environment and modernizing its database.*

***Infrastructure Changes***

* *The Microsoft Azure platform will be configured with the new Windows Server 2019 environment that can be accessed through the cloud.*
* *Microsoft Access 2010 will be migrated to Microsoft SQL database.*
* *Curation of a remote access policies to monitor and implement proper access to HBWC systems such as SHGTS.*
* *Microsoft Windows Server 2008 R2 will be permanently retired and securely disposed of after 1 year to ensure the new system is fully functional.*
* *Microsoft Access 2010 Database will also be permanently retired after 1 year to ensure new system is fully functionable per proposal. Once verified, a secured backup of the database will be stored securely for potential disaster recovery.*
* *The lack of a physical server at HBWC will address any lack of physical security controls, and assist in hardening the physical security of cloud servers via Microsoft.*

***Policy & Procedures Changes***

* *MFA should be required to access all HBWC systems.*
* *Users will be granted system access and security audits will be conducted regularly.*
* *The DRP and disaster recovery policies will be revised in order to correlate with new Microsoft Azure IaaS.*
* *HBWC will adopt principles of least privilege policies to assist with employee access limitations based on job functions.*
* *Users will require unique login information for access to all systems. Login policies should be enforced, and unique login information should not be shared.*

## Proposed System

### High-Level Operational Requirements and Characteristics

*Use the following sections to describe the operational requirements and technical design of the proposed system.*

#### 5.1.1 User Community Description

**Table 1: User Community Description**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **User Group** | **Description/Expected Use of System** | **Type**  **(Federal Employee, Contractor)** | **Geographic Location** | **Network Profile**  **(LAN, WAN, External)** | **Total Users** | **Concurrent Users** |
| *Executive Staff* | *Approves grant applications and grant reporting* | *Employee* | *HBWC main location* | *LAN, WAN* | *6* | *6* |
| *OGG* | *Grant application tracking and reporting* | *Employee* | *OGG Office* | *LAN, WAN* | *7* | *7* |
| *NIH* | *Reconnaissance and transmission of hospital applicants’ information for grant applications* | *Federal employee* | *NIH Office* | *External* | *11+* | *11+* |

#### Nonfunctional Requirements

|  |  |
| --- | --- |
| **ID** | **Requirements** |
| NFR-01 | Update grant application processing time to coincide with new streamlined process (this processing time will be significantly shorter than previous). |
| NFR-02 | User training for new cloud-based system/ database |
| NFR-03 | IT Department/ DRP team training for backup procedures after cloud migration |
| NFR-04 | Security training for new MFA |
| NFR-05 | Disbursement of user login information to access all systems using an encryption method (HTTPS, SSL, or TLS) via a secured email service. |

### High-Level Architecture

Diagram

Description automatically generated

**Table 2: Alternatives Considered for the Overall Architecture**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Alternative** | **Description** | **Pros** | **Cons** | **Preferred Alternative?** | **Rationale** |
| *Keep server on-site and purchase additional hardware with increased security mechanisms* | *Purchase additional hardware for creation of a new server and network security equipment (physical security controls, firewalls, etc.).* | *Databases would be onsite and HBWC would have full control over servers and databases instead of allocating (transferring risk) to Microsoft.* | *The purchase of all of these additional physical controls and hardware/software, it would result in a higher utility cost.* | *NO* | *Cost prohibitive* |
| *Keeping payroll on-premises using QuickBooks with the continued utilization of paper checks.* | *There is Privacy Act data included in the QuickBooks database which is housed on the current Windows server. The serve lacks proper access governance, allowing data to potentially be shared/accessed outside of the payroll office.* | *Payroll would remain onsite; Payroll Dept would have maximized control over disbursement of grant funding.* | *Not allocating these services (transferring risk) to cloud-based systems or vendors such as Workday or ADP increase risk of data confidentiality.* | *NO* | *Cost probative and associated risk and compliancy issues.* |
| *Set up server locally* | *Host SHGTS server and store all data locally* | *HBWC tech department would have maximized control over all factors pertaining to the new database.* | *IT Department would have additional responsibilities to implement proper security controls according to FISMA and NIST standards (typical responsibility of a SOC Dept).* | *NO* | *Current personnel would not be qualified to implement such an environment, thus additional personal would be required.* |

#### Application Architecture

*Instructions: Using the table below, describe the application components in the architecture diagram above. If you considered alternatives around a particular application component, discuss them in this subsection.*

**Table 3: Description of Application Components**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Diagram ID** | **Application Component** | **Description**  **(Business Process Supported, Purpose of Component)** | **Type**  **(Identify both (1) Operational or Analytical and (2) Batch or Online)** | **Strategy**  **(Build, Buy, Reuse, Rewrite)** | **Alternatives** | **Pros** | **Cons** | **Preferred Alternative** |
| *ID 01* | *Remote access to new Microsoft Azure Web Portal* | *Implement secured VPN connection utilizing IPsec to Microsoft Azure* | *Operational & online* | *Build* | *Utilize a secured web browser like Microsoft Edge (would maintain vendor product consistency and compatibility)* | *Utilizing a web browser would not require us to build a secure VPN.* | *Reduced security* | *Building a VPN using IPsec is the preferred method in this project.* |
| *ID 02* | *NIH VPN connection* | *Secured file transfer (SFTP) from NIH to SHGTS database* | *Operational & batch* | *reuse* | *none* | *Already in place we just migrate it to updated server.* | *none* | *None- this method is the only approved method for NIH.* |
| *ID 03* | *SHGTS application portal* | *Establishing a new grant application portal* | *Operational & batch* | *Build & reuse* | *Reuse system, but migrate current SHGTS to new Windows 19 web server* | *Faster accessibility to SHGTS* | *Utilizing Windows 2019, a lesser outdated server compared to the original server.* | *Continue building a new application portal while reusing selective portions of the original (that will remain effective).* |

#### Information Architecture

**Table 4: Description of Information Components**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Diagram ID** | **Conceptual Information (Entity)** | **Description** | **Type of Data Store (Transactional or Analytical)** | **System of Record?**  **(Does this system or another system serve as system or record for information?)** | **Data Acquisition Approach**  **(e.g., User Data Entry, Interface)** | **Alternatives** | **Pros** | **Cons** | **Preferred Alternative** |
| *ID 04* | *SHGTS* | *Receives and stores all data regarding grant applications and hospital applicants from NIH, Executive Review Team, and Accounting Dept.* | *Transactional & analytical* | *System of record* | *User data entry & interface* | *none* | *New server and database will be able to store more information* | *none* | *none* |
| *ID 05* | *NIH data transfer to SHGTS* | *NIH will transfer data (SFTP) to HBWC’s database* | *Analytical* | *System of record* | *Interface* | *None* | *Securely transfer data* | *None* | *None* |
| *ID 06* | *HBWC Accounting Dept* | *Accounting Dept will access SHGTS database to run reports, update ACH statuses, and record verifications.* | *Analytical and transactional* | *System of record*  *Record for information* | *User data entry* | *None* | *Improvement of workflow for accounting dept.* | *None* | *none* |

#### Interface Architecture

*Not required for performance assessment.*

#### 5.2.4 Technology Architecture

*The Microsoft Azure environment is a cloud-based platform providing support for a diverse range of OS, programming languages, tools, databases, frameworks, and devices. Microsoft Azure's architecture relies on numerous data centers that house a variety of servers and hardware. These resources enable clients to develop customized technology solutions that align with their specific business requirements. By leveraging this technology environment, Microsoft can provide the Azure platform, which HBWC plans to use to establish a client-server relationship in their S.H.G.T.S system.*

*The second aspect of the proposed technological architecture is the migration of Microsoft Access 2010 to Microsoft SQL database.* *Microsoft Access 2010 is designed for individual and small business use and has a maximum database size of 2 GB. SQL databases are intended for medium to large-sized businesses they require specialized training to migrate outside of the organization, and they are designed to scale up as the organization grows without compromising system performance.*

##### Platform

*Windows Server 2019 operating system (OS)*

##### System Hosting

*Microsoft Azure (IaaS)*

##### 5.2.4.3 Connectivity Requirements

*internet*

##### 5.2.4.4 Modes of Operation

*HBWC’s IT Department is proposing a 6-moth duration of parallel operation and testing for the new environment. The original system will be kept viable as a backup system, and accessible to the IT Department as a failover precaution in the event of a disaster.*

#### Security and Privacy Architecture

*Microsoft Azure will be responsible for HBWC’s security services as the IaaS. The Azure Security Center will assess and monitor recommendations to the IT Department and will also continuously assess the Microsoft Azure environment security posture.*

***Physical security controls***

*Per Microsoft Azure SLA, physical access to their data centers must be arranged with prior notification, prior authorization, and other strict access policies.*

***Remote access security***

*Connections between the NIH and SHGTS must be maintained via the Azure VPN allowing secured site-to-site connections (e.g., VPN Gateway site-to-site VPN). The traffic will be transferred over the internet, but SSTP will be utilized as the Azure VPN is a secured option for HBWC’s remote security. This will allow geographic expansion and potentially increase additional employment opportunities.*

*Microsoft Azure Privacy policies are based on the principles of least privilege, restricting access to customer data, virtual machines, etc. to specific job functions. Microsoft explicitly states that it does not inspect or alter any applications or data that is deployed to Azure and does not claim data ownership.*

##### Authentication

*Microsoft Azure utilized the identity access control system SSO. HBWC’s IT Department will use Azure AD will allow users to setup account information such as company email addresses to access the new system.* *The use of Microsoft Azure, including Azure Active Directory, will assist the IT Department in refining access privileges based on a user's role within the company and the business needs to access important systems remotely. One notable capability of Azure AD is the use of conditional access policies, which can be tailored based on a variety of factors, including group membership, location, etc.*

*HBWC will also utilize an MFA system which will require at least 2 authenticating factors in order for the system to grant authorization for user access. HBWC’s project will propose the “something you know” and “something you have” authenticator method, such as knowing one’s login information and possessing a mobile security passcode via an app like “Microsoft Authenticator” or “Duo Mobile”. To gain entry into the system, the user needs to follow a multi-step authentication process. Initially, the user needs to visit the web portal and provide their login credentials, which include a username and password. After entering these details, the user will receive an access code on their mobile device, which serves as a second authentication factor. Finally, the user will have to input this access code into the system to gain access.*

##### Authorization

*Authorization and access to the SHGTS portal and database will be implemented utilizing the role-based access control” method.*

***Internal employees***

* *Executive review staff: access will be restricted to elevated permissions area of SHGTS portal in order to allow the running of reports and grant application approval.*
* *Accounting department: similar to executive review staff access, they will have access to an elevated permissions area of SHGTS. Portal. This access will allow them to run reports and verify grant application approval statuses.*
* *IT Department: Authorized personnel in this department will have different levels of access. System Administrators' access will depend on their specific job functions and roles.*

***External organizations/applicants***

* *Grant applicants/hospitals: minimal access to the database that will be restricted to applying for grants, checking application status, and reporting.*
* *NIH: This department will have direct access to the database consisting of a secure connection and batch data processing.*

##### Encryption

*The use of an Azure site-to-site VPN connect should be configured using IPsec/IKE connection policies. A collaborative meeting should be conducted between NIH and HBWC’s IT Department to confirm that desired encryption standards are met for each respected organization. NIH is a government agency and will greatly assist in the compliance of FISMA and NIST standards for encryption.*

## Analysis of the Proposed System

*Use the following section to analyze the proposed system by prioritizing risks from the DREAD analysis.*

### Risks Prioritization and Descriptions

1. *PWC-01: Web server not protected by application firewall.*
2. *PWC-02:* *Outdated server software*
3. *P-CM01 No configuration management controls.*
4. *P-PM01:* *No patch management controls.*
5. *P-SA02: No user activity tracking controls or process*

### 6.2 Risk Analysis

*The below information directly correlates with the risks identified in section 6.1 Risks Prioritization and Descriptions.*

1. *Transferred; Because the new system will be through Microsoft Azure, web security services will be provided to protect the server and databases.*
2. *Mitigated; A new operating system will be deployed into Microsoft Azure.*
3. *Mitigated; A new operating system will be deployed into Microsoft Azure with multiple configuration tools/services.*
4. *Mitigated; A new operating system will be deployed into Microsoft Azure with an updated patch system. (Azure patch management)*
5. *Mitigated; A new operating system will be deployed into Microsoft Azure with services such as Azure Monitor to track user activity across the system via activity logs, etc.*

**Appendix A: Referenced Documents**

***(Optional: Not required for performance assessment)***

*Instructions: Summarize the relationship of this document to other relevant documents. Provide identifying information for all documents used to arrive at and/or referenced within this document (e.g., related and/or companion documents, prerequisite documents, relevant technical documentation, etc.).*

**Table 9: Referenced Documents**

|  |  |  |
| --- | --- | --- |
| **Document Name** | **Document Location and/or URL** | **Issuance Date** |
| *<Document Name>* | *<Document Location and/or URL>* | *<MM/DD/YYYY>* |
| *<Document Name>* | *<Document Location and/or URL>* | *<MM/DD/YYYY>* |
| *<Document Name>* | *<Document Location and/or URL>* | *<MM/DD/YYYY>* |

**Appendix B: Notes to the Author/Template Instructions**

*This document is a template for creating a high-level technical design for a given investment or project. The final document should be delivered in an electronically searchable format. The high-level technical design should stand on its own with all elements explained and acronyms spelled out for reader or reviewers.*

*This template includes instructions, boilerplate text, and fields. The developer should note that:*

* *Each section provides instructions or describes the intent, assumptions, and context for content included in that section. Instructional text appears in blue italicized font throughout this template.*
* *Instructional text in each section should be replaced with information specific to the particular investment.*
* *Some text and tables are provided as boilerplate examples of wording and formats that may be used or modified as appropriate.*

*When using this template, follow these steps:*

1. *Table captions and descriptions are to be placed left aligned, above the table.*
2. *Modify any boilerplate text, as appropriate, to your specific investment.*
3. *Do not delete any headings. If the heading is not applicable to the investment, enter “Not Applicable” under the heading.*
4. *All documents must be compliant with Section 508 requirements.*
5. *Figure captions and descriptions are to be placed left aligned, below the figure. All figures must have an associated tag providing appropriate alternative text for Section 508 compliance.*