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 1.0

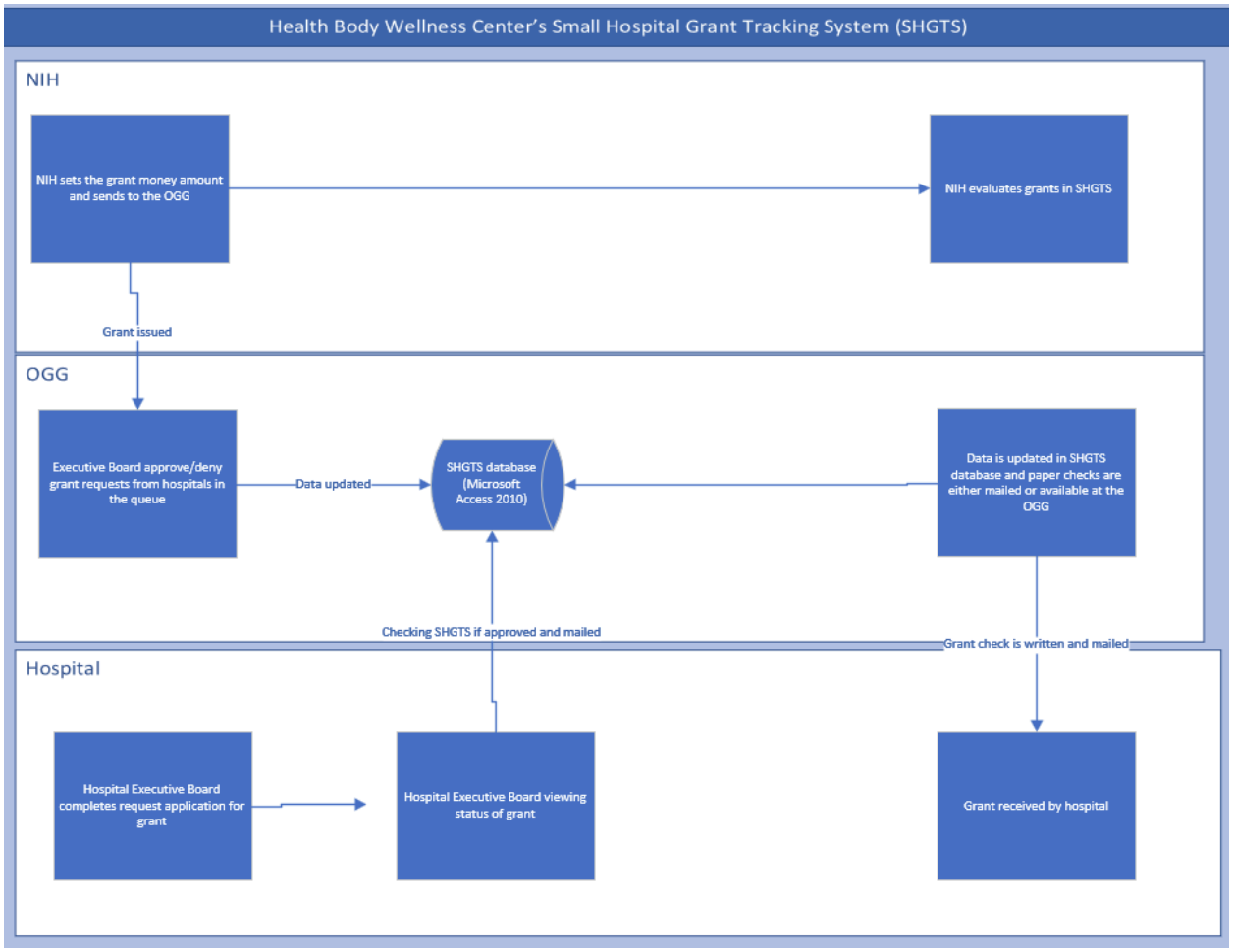
Updated 7/22/2023

Table of Contents

1. Introduction

2. Current Systems

The current system at HBWC uses the Small Hospital Grant Tracking System (SHGTS) which runs on Microsoft Access 2010 as its primary database running on a Windows 2008 Server R2; both have reached the end of life and are no longer supported. The SHGTS is used to grant money from the Office of Grants Giveaway (OGG) to small hospitals. The National Institute of Health (NIH) sets the amount of money distributed to the OGG. Once evaluated by the NIH the grant money is available to the OGG to approve or deny requests from small hospitals by the Executive Board. Once approved, the database is updated in the SHGTS and a paper check is mailed to the hospital or made available at the OGG. The issue with the SHGTS is that Access 2010 is not suitable for multiple users. This delays the rate at which HBWC can serve up new grants, causing small hospitals to miss out on necessary funding. Depending on the number of grants ready for distribution, HBWC may be forced to create a queue, causing hospitals to wait. This wait can become too long, causing hospitals to miss their deadlines and lose the grants. HBWC is also using QuickBooks to manage the employee payroll, HBWC HR provides paper checks to employees at the end of each pay period. The issue with using paper checks is that it is inefficient and it is better to streamline payroll and grant processes. It is recommended that HBWC moves to a digital form of payment that has direct deposit and automatically takes care of taxes, and provides accurate calculations for payments. The current systems are shown in the diagram below.



3. Goals, Objectives, and Rationale for New or Significantly Modified System

3.1 Project Purpose

The purpose of the project is the modernization of HBWC systems. This involves upgrading systems to be up to date with the latest security patches, making systems more efficient, and allowing for systems to scale to future workloads. To do this HBWC will need to upgrade and streamline their web services, allow for data to be securely and easily accessible by authorized personnel, and ensure that HBWC can scale towards future goals without the limitations of current technologies. The new system(s) will be focused in the cloud moving off of Microsoft Access 2010 to Microsoft SQL and moving off of Windows 2008 Server and to a cloud-based Microsoft Azure server for computing. The retirement of the outdated systems will begin once I.T and Executive Board after new systems are set up, tested, and validated.

3.2 System Goals and Objectives

In the case study and security assessment report, HBWC Executive Board highlights that there is a need to upgrade major systems and business processes across the company so that it meets federal security regulations and provides robust and efficient services to partners. The goal is to modernize HBWC

systems to better support small hospitals via grants by upgrading hardware and software to support multiple concurrent connections running on supported servers. HBWC wants to streamline payroll and payment processing by using Workday, an enterprise tool for handling finances and benefits. To better under the feasibility and work needed to be done HBWC has hired a security consulting firm Endothon Security Consulting to provide a security assessment report (SAR) to assess the security of HBWC's systems, network, Office of Grants Giveaway (OGG) processes, Small Hospital Grant Tracking System (SHGTS), and cryptographic controls. Currently, there are critical systems identified in the SAR which are payroll and the SHGTS. The payroll system currently runs on QuickBooks and payments are provided via paper checks. The SHGTS runs on outdated hardware Microsoft Windows 2008 Server R2 and software Microsoft Access 2010 as its database which have reached end-of-life (EOL) and are no longer supported. The overall objective is to provide a more efficient and secure web service to serve grants to small hospitals via SHGTS and automate payment processing using direct deposit and this can be done by moving to a cloud-based system such as Microsoft Azure for computing and updated software to comply with federal regulations as well as scale systems and services on demand.

3.3 Proposed System

The system that will be proposed will be focused on using Microsoft Azure a cloud provider to provide sufficient and needed upgrades to HBWC system(s). The Small Hospital Grant Tracking System (SHGTS) will be the first system that needs to be upgraded using Microsoft Azure. The system will need to replace an existing database using Microsoft Access 2010 with a Microsoft SQL Server 2022 database. The infrastructure that the SHGTS runs on is currently a Windows 2008 Server R2 and will be replaced with a cloud-based Microsoft Windows Server 2022 running Microsoft Azure's data center. The payroll system is running on QuickBooks and will be replaced with Workday, an enterprise payment/benefit processing system. Additionally, once the production environment is set up for the SHGTS it is important to also set up a disaster recovery site that will act as a hot site that will be an active replica of the production environment in the event the production environment is down. With the help of Microsoft contractors working with HBWC I.T, the shift towards Azure will streamline services that will aid in the future growth of the company as well as to ensure regulatory requirements are in compliance with industry standards (Privacy & HIPAA).

3.3.1 System Scope

The scope of the project will be focused on moving off of the Windows 2008 Server to Windows 2022 Server, migrating off of Microsoft Access 2010 to Microsoft SQL Server 2022 through Microsoft Azure, and upgrading the payroll system to Workday from QuickBooks. The payroll system will be upgraded to Workday allowing for HR and the Executive Board to process employee pay via their timecard submission, once approved a direct deposit will be sent to the employee. In addition, once a grant has been approved, Workday will automatically deposit funds to small hospitals. With the upgrade to modern systems, a web portal will be developed by HBWC that will allow small hospitals to submit applications for approval by the Executive Board.

3.3.2 Processes Supported

The processes supported will be the new infrastructure setup and configuration in Microsoft Azure, setup of Microsoft SQL Server 2022 in Windows 2022 Server, set up of Workday to automate payroll and payment processing, and creation of a hot site that will be used as disaster recovery in the event production is not available. Once set up and creation of infrastructure and software(s) technical processes such as setting up a secure web portal for hospital application submissions will be created.

3.3.3 High-Level Functional Requirements

General/Base Functionality

- Purchase license/contract with Microsoft Azure to provide SaaS services. Azure will be used in the cloud to set up Microsoft Windows 2022 Server and Microsoft SQL Server 2022. The SHGTS will make use of both Windows 2022 Server and Microsoft SQL Server 2022 to improve system performance. Additionally, an equivalent hot site used for disaster recovery will be set up in the event the main site (production) is down.
- Purchase a license/contract with Workday and set up will replace QuickBooks as the primary payroll and benefits system. This will allow for direct deposit to be set up for small hospitals and employees at HBWC.

Security Requirements

- Remote access to the Workday system will require authorized personnel to use a virtual private network (VPN) to ensure traffic between clients and the Workday system is encrypted (using TLS 1.3) to keep Personal Identifiable Information (PII) and Protected Health Information (PHI) from being exposed to the internet.
- Data encryption will be set up on both Microsoft SQL Server 2022 and Windows 2022 Server and access should only be given to authorized personnel
- Databases from the older system (Microsoft Access 2010) will be backed up and archived in the event it is needed for audits or data migration does not capture all data.

Reporting Requirements

- Grant access to small hospital applications to view the status of their applications and other recorded information that is relevant to the hospital
- Allow for approved Executive Board members to administer the SHGTS system so that they can approve or deny applications as they are inputted into the SHGTS.

Usability Requirements

- Allow for the ability to have multiple concurrent connections to the SHGTS so that Executive Board members can read/write and Small Hospital Applications can read simultaneously.

Audit Requirements

- Audit reports are generated and viewed by the Executive Board and Administrators. If unauthorized access is granted the report is flagged and alerts the administrator assigned in the system.

4. Factors Influencing Technical Design

4.1 Relevant Standards

The relevant standards that HBWC must adhere to in their technical design of the current system are as follows:

1. The SHGTS and Workday systems must generate logs tracking who is on the system and flag suspicious activity on the system. When suspicious activity is detected administrators will be alerted to provide incident response and handling. This will proper incident procedures are conducted by having the system alert when an activity that is not warranted as safe is being

conducted. Also to meet guidelines set in the Computer Security Incident Guide (NIST SP 800-61) a guide that provides organizations incident handling skills to identify, analyze, contain, eradicate, and recover from security incidents.

2. The NIH are to comply with the Federal Information Security Modernization Act (FISMA 2014) requiring that NIH sends annual reports of major incidents such as threats, vulnerabilities, and impacts, risk assessments from HBWC, total number of incidents, description of individuals affected, major incidents involving breaches of PII and PHI.

3. The SAR report states that HBWC and NIH are to meet Health and Human Services (HHS) requirements to meet FISMA compliance. The standard to follow as a framework would be the Guide for Developing the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (NIST SP 800-37) to develop policies and procedures to align with federal government guidelines. The Risk Management Framework goes over the seven-step process where systems are prepared by establishing context and priorities, categorizing information systems and information processed, stored, and transmitted, selecting baseline security controls, implementing security controls, assessing third-party controls and verifying controls are properly in place, authorizing systems to grant or deny authorized parties, and finally monitor security controls in the systems continuously.

4. HBWC using Microsoft Azure services in a SaaS-model format requires that NIST SP 800-145 (A NIST Definition of Cloud Computing) be followed as a standard for cloud computing. The upgrades associated with the project require that Microsoft SQL Server 2022 and Windows 2022 Server can scale when the company needs more computing power or storage. The development and hosting of web applications such as a web portal can be easily and efficiently managed and updated. Additionally, a disaster recovery site will be needed to act as a secondary site when the main site (production) is no longer available providing failover services via the SaaS-based model offered by Microsoft Azure.

5. The SAR report categorizes risks by rating each risk the strategy employed and followed can be found in the Risk Management Guide for Information Technology Systems (NIST SP 800-30). Using a Risk Exposure Matrix Endothon Security Consulting created a Risk Exposure Ratings table rating each risk by likelihood from high to moderate to low. By using Microsoft Azure to provide high-level security we can assume that major risks will likely be removed and since the current system implemented has been rated high risk using Microsoft Azure will remove existing risks as the systems are now managed via Azure however, HBWC I.T needs to understand any new risks from moving to a cloud provider.

Finally, HBWC I.T and the Executive Board must understand that the development of any new systems needs to have policies and procedures well established and follow national standards. The upgrade will involve the compliance of NIST SP 800-64 (Security Considerations in the System Development Life Cycle) where administrators will understand the budgetary and technical requirements needed to perform current and future upgrades; this requires that an SDLC (System Development Life Cycle) document be maintained and regularly updated. This will help the identification and mitigation of security vulnerabilities, awareness of potential engineering challenges, and provide facilitation of informed

decision-making throughout the project making use of comprehensive risk management on time. Following all applicable regulations and standards will allow HBWC to be effective in its information security of newly developed systems so that the company can maximize returns on investments made throughout the project.

4.2 Assumptions

HBWC Executive Board, HR, and IT will need to work closely with Microsoft Azure and Workday contractors to ensure that system upgrades are coordinated and keep the timeline of the project. Understanding the complexities of each system being upgraded is important as the contractors hired are temporarily going to be available. Delays that will be incurred due to initial setup taking longer than expected could have drastic consequences on the company's reputation. The existing environment and new project should have minimal downtime as they can be stood up while the existing environment is made available for existing users. The migration of data to a new database will need to be validated by both IT and contractors from Microsoft Azure. Any data loss will not be tolerated as backups should be made in the event all data is not transferred to Workday or Microsoft Azure.

4.3 Dependencies

The dependencies are caused by project cost, time, and project scope. For example, the upgrades of both payroll and the SHGTS systems require a fixed timeline to be set to avoid delays in new grants or payments being processed. If the timeline cannot be met it's important to understand where the gaps are and work on a new critical path. External dependencies such as the contractors from Workday and Microsoft Azure will be needed to provide expertise in the initial setup of both systems if not available or resources provided by the vendors cannot satisfy the project timeline. Then it's important for HBWC Executives to have alternative plans. The dependencies on leads in each department Executive, HR, and IT in HBWC will be needed to provide tasks and scheduling for each team member involved as well as acting as a final decision maker for each section of the project. Staff knowledge will need to be present through the upgrade and after it's been set up and completed. This means that HBWC will be dependent on those who were a part of the initial set up of the new system, requiring that documentation be created to write up new policies and procedures.

4.4 Constraints

Project constraints would predominantly be placed on the budget set by the Executive Board. Cloud services are known to be expensive if not set up to provide on-demand services when HBWC needs them. That being said, leaving a virtual machine online when not necessary would increase project cost over time. This could reach over what is expected. Licensing and contracts could mean HBWC Executive Board could face charges beyond what was advertised as any delays or additional time needed by contractors could increase the costs of the project. Staff knowledge beyond the set up could prove to be an issue that is only noticed after the project is set up and running in production. Once a major incident occurs and existing employees are unable to resolve the issue this might force HBWC to pay additional vendor support fees. Any variation of data center or hardware failures or software incompatibility can increase the overall time needed to be spent finalizing the project forcing leadership to extend timelines. The loss of any important staff members during the critical phases of the project can be detrimental to the project's completion or feasibility.

4.5 Design Goals

The goal of the project is to upgrade and modernize the existing HBWC infrastructure, software, and payroll system. This will require a complete upgrade of the SHGTS system's database and server, set up a web portal for small hospitals to view the status of their applications, and moving off of the existing QuickBooks payroll system to a more enterprise payroll system such as Workday. Once upgrades are complete HBWC should be able to scale on demand allowing for systems to be efficient and responsive. The design is highlighted below.

SHGTS and Web Portal

- Granting system will have an approval and deny system that will automatically be stored in the Microsoft SQL Server 2022
- Hospitals will be able to view the status of their application via a web portal that pulls data from the SHGTS database
- HBWC Executive in the OGG will be able to receive notifications when new grant money is available
- Grant money that is not used will be returned to the OGG and if no hospitals are available to receive a grant will be sent back to the NIH
- Once approval status is set an automatic direct deposit will be set out to small hospitals removing the need for hospitals to wait for paper checks in the mail.

Workday

- HBWC Executive Board and HR will be able to automatically send out direct deposits to employees as well as W2 tax forms for taxes.
- Timecard submissions will all be managed in Workday allowing employees to submit their timecards and for HR to validate hours and approve the submission.
- Administrators of the system will need to access the Workday system via an encrypted VPN tunnel utilizing TLS 1.3 to ensure PII and PHI are not leaked.
- Hospitals will be automatically sent funds via Workday direct deposit once their application is approved.
- Benefits for existing and new employees can be set in Workday allowing for easier onboarding and management of employees by the Executive Board.

5. Proposed System

5.1 High-Level Operational Requirements and Characteristics

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
HBWC Executive Administrator	Able to manage, edit, configure SHGTS data and status of approval	Employee	HBWC	LAN, WAN, External	10	10

Hospital Members	Able to apply for a grant via web portal and view status	Employee	Small Hospital in Local Area	External	20	20
NIH Administrator	Able to send funds to HBWC Administrator to send to SHGTS system	Federal	NIH Headquarters	External	5	5
HBWC I.T	Upgrading systems to use Microsoft Azure SaaS services (Windows 2022 Server and Microsoft SQL Server 2022)	Employee	HBWC	LAN, WAN, External	20	20
HBWC HR	Upgrading payroll systems moving from QuickBooks to Workday	Employee	HBWC	LAN, WAN, External	10	10
Vendor Contractor	Providing expertise and critical skills in the set up of new Azure and Workday systems.	Contractor	Microsoft/Workday	External	10	10

5.1.2 Nonfunctional Requirements

ID	Requirements
NFR-001	HBWC I.T will need expertise and knowledge transfer from Microsoft Azure contractors. Once the project is complete HBWC will need I.T employees to become the experts.
NFR-002	HR and the Executive Board will require training in how to use Workday as the payroll administrators will need policies and procedures properly documented before going live.
NFR-003	The newly designed web portal will need to be reviewed by the Executive Board before being made available to ensure it meets HBWC's mission statement.
NFR-004	Security training will be needed for HBWC employees. HBWC employees will need to go through security awareness training, technical security training, security management training, and compliance training to prepare for new system architecture.
NFR-005	Payment processing will need to be automatic using Workday as QuickBooks requires manual payments to be sent out via OGG or mail. It's important that automatic direct deposit must be set up.

5.2 High-Level Architecture

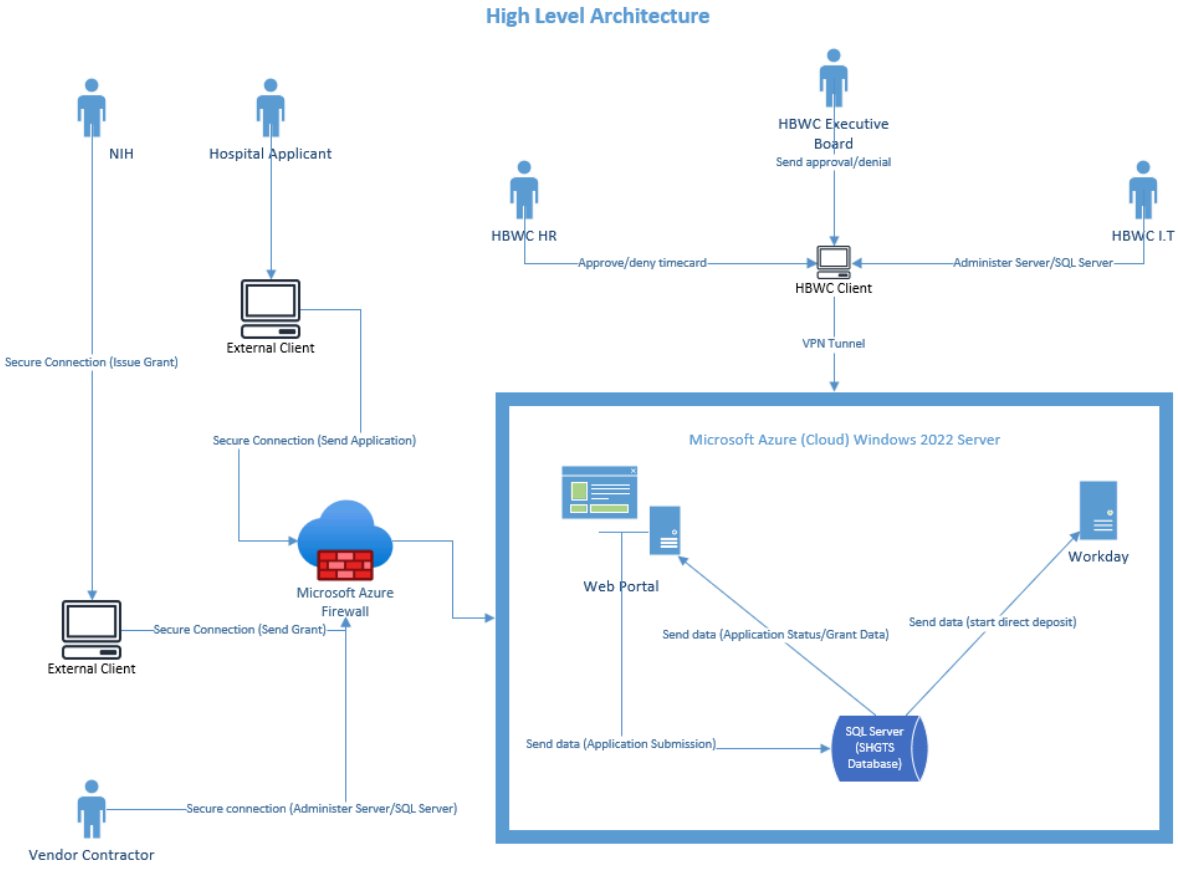


Table 2: Alternatives Considered for the Overall Architecture

Alternative	Description	Pros	Cons	Preferred Alternative ?	Rationale
Apache Web Server	Host web portal on on-prem hardware and set up an HTTPS Web Server using Certificate Authority for SSL certificates.	HBWC would save greatly in resource costs by using an open-source web server. The documentation to set up and get the server up and running would be readily available online.	Security requirements may not be met because the service is open-source as well as the majority of the technical expertise would need to come from HBWC I.T.	No	While setting up the Apache Web Server would be cheaper at any point in time if the HBWC would like to increase the Web Server's capability there would be limitations as to what could be set up. While in a SaaS-based model, you can scale all services as needed such as increasing bandwidth to handle more connections.
Purchase On-prem hardware and upgrade	Purchasing new Server and Database software such as using	HBWC I.T. would have physical access to all machines and virtual	Using open-source technology requires full knowledge of	No	While potentially saving the company money in the short term, the skills and expertise needed to self-manage a system would require HBWC heavily invest in its I.T.

security systems	open-source open systems such as CentOS or paid version such as RedHat Enterprise and using MySQL Server.	access to all software(s)/databases. This would allow HBWC to have full ownership of its entire architecture.	keeping it secure as well. HBWC would need experts in this realm. If going with a paid operating system such as RHEL (Red Hat Enterprise Linux) then HBWC would need a solid knowledge base there as well. Additionally, a data center with a UPS, Switches, Firewalls, and an HVAC system would need to be set up. This might require HBWC to hire outside vendors, defeating the costing saving benefits.		department along with hiring contractors to help with the initial setup. This could prove to be too costly for the HBWC Executive Board to take on.
Intuit QuickBooks for Payroll	Upgrading the existing QuickBooks payroll system to use Intuit QuickBooks.	This could save HR and Executive Board time by using a familiar dashboard and only having to learn new features.	The costs of using an enterprise payroll system such as Workday would be the cost-benefit as Workday proves more features for less than Intuit Quickbooks such as automation for benefits and taxes.	No	Easily migrating to a familiar system requires there to be less training and cost to training therefore saving money and time however, the monthly charges and lack of advanced features would not make it a better choice than Workday.

5.2.1 Application Architecture

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
ID01	Web Portal	Web Portal for HBWC connecting to SHGTS	Operational and Online	Build	Apache	Scaleable, Secure, and assistance can be given by Microsoft in the event technical know-how is now available by HBWC	Supported only in Azure products, Not open-source documentation is limited, and requires experts to manage the system	Apache
ID02	SHGTS Database (Microsoft SQL Server 2022)	Database for SHGTS application using Microsoft SQL Server 2022	Operational and Online	Buy	MySQL Server	Supports multiple concurrent connections, is scalable, includes support by Microsoft, and is less costly than MySQL Server overtime	Resources expertise in subject matter and short-term costs are higher than MySQL Server	MySQL Server
ID03	Workday (Payroll)	Enterprise Payroll System for HBWC handling grants and employee payment	Analytical and Online	Buy	Intuit QuickBooks	Supports direct deposit, automates benefits and taxes, and provides analytical data for making business decisions. Additionally, helps the Executive Board and HR understand financial needs for future planning.	Requires extensive training for Executive Board and HR and initial costs are higher than using QuickBooks	Intuit QuickBooks

ID04	Windows Server	Microsoft Windows 2022 Server that will host all relevant SaaS applications.	Operational and Online	Buy	CentOS/RHEL	Secured by Azure's robust data center technology, provides quick and efficient policy control, supported by Microsoft and training will be provided by Microsoft	Short-term costly, locked into a single operating system so doesn't provide flexibility, requires a large amount of training if knowledgebase not already available	CentOS/RHEL

5.2.2 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
ID01	HBWC Executive Board	The Executive Board approves/denies grants sending data to the SHGTS database.	Analytical	System of Record	User Data Entry	None	Allowing reviewers to send data to the web portal and SHGTS databases status can be viewed by external clients	None	None
ID02	HBWC Human Resources	Access to Workday allows for accounting information for reporting, record keeping, and approvals of timecards	Transactional and Analytical	System of Record	User Data Entry	None	Decreasing time spent on timecards and grant application processing.	None	None

ID03	HBWC Information Technology	Access to server management and database configuration.	Analytical	System of Record	Interface	None	HBWC I.T will be able to analyze logging metrics, generate reports, and produce predictive charts for future HBWC planning	None	None
ID04	SHGTS Database (Microsoft SQL Server 2022)	Data provided by NIH, OGG, Hospital Application, and Executive Board will be stored in Microsoft SQL Server 2022 Database and showcased in Web Portal	Transactional and Analytical	System of Record	User Data Entry and Interface	None	Provides a central database to pull critical data from to store in applications such as web portals. Can scale to handle more data as the company grows.	None	None
ID05	Web Portal	Web Interface to establish a connection to the SHGTS to showcase the status of grants to small hospitals	Analytical	System of Record	Interface	None	Allows for automated checks of existing applications and their status and once approve in the SHGTS database a deposit is sent to hospitals	None	None
ID06	Workday	System to provide enterprise grade payroll to handle grants and employee payroll	Transactional and Analytical	System of Record	Data Entry and Interface	None	Allows for the ability for HBWC to automate direct depositing, tax record keeping, and provide categorize benefits	None	None

5.2.3 Interface Architecture

5.2.4 Technology Architecture

With the use of Microsoft Azure as a SaaS-based model the architecture will be based on the use of the Azure data center to host the Windows 2022 Server and HBWC will be connecting to the server as an external client allowing for security to be handled in Azure once connected. The second technology is the use of Microsoft SQL Server 2022 to migrate the existing Microsoft Access 2010 database. This will remove limits on multiple applications or users connecting to the database as well as remove limitations such as the 2 GB memory limit, and not being able to scale as new physical storage mechanisms would need to be in place for the database size to increase. A web portal will be built once the database and server are set up to allow for grant approval to be automatically displayed for small hospitals and a new payroll system using Workday will enable HBWC to set up direct deposit to work in tandem with other new systems to deposit grant money to small hospitals and provide employees automated payment versus the existing system QuickBooks which prints out paper checks that are then mailed to employees/hospitals or available at the Office of Grants Giveaway (OGG).

5.2.4.1 Platform

The new system will focus on using Microsoft Azure. The first system needed will be a Windows 2022 Server that will handle all computing power needed for applications. The second system would be the SHGTS database using Microsoft SQL Server 2022 that will handle storage, backups, and data delivery. Microsoft SQL Server 2022 will be migrated off of the existing Microsoft Access 2010 database. The migration to Microsoft SQL Server 2022 from Microsoft Access 2010 is documented on Microsoft's website where an application called Microsoft Access Database Engine 2010 Redistributable has been created to help facilitate a transfer of data between Microsoft Access 2010 to Microsoft SQL Server 2022. The Windows 2022 Server will be replacing the Windows 2008 Server that has reached EOL (End of Life) and the new server will be reaching EOL 2026 with extended support up to 2031. Microsoft SQL Server 2022 will be supported up until 2028 with extended support up to 2033 as well as providing 10 years of backups allowing for HBWC to quickly recover in the event data is lost or corrupted. Workday the new payroll system replaces the existing QuickBooks payroll system to allow for direct depositing, creating tax recording, and enhancing the benefits system. Workday offers advanced features over QuickBooks and in the long term is more cost effective. HBWC I.T will take the lead in setting up the new platform with guidance and funding from the HBWC Executive Board. HBWC HR will take in setting up the new payroll system Workday with the guidance and funding from the HBWC Executive Board.

5.2.4.2 System Hosting

The applications such as the SHGTS, Web Portal, and Workday will be hosted in Azure inside of the Windows 2022 Server using Azure's robust data center to handle large workloads and scale as the environment needs more computing power to handle workloads. Microsoft Azure offers the latest and greatest security and monitoring capabilities allowing HBWC to focus on building great applications that serve its customers. The reporting system in Azure is known for its ability to provide detailed records and assessments on the state of the current environment allowing for monitoring and alerting to be set up by HBWC I.T with ease. Additionally creating suggestions and recommendations on changes to make the systems is another feature Azure provides to its customers. Modernizing HBWC will put them in a stronger position in the market.

5.2.4.3 Connectivity Requirements

The new system will be hosted in a Software as Service (Saas) based model which will be on cloud infrastructure in Microsoft Azure. All networking excluding accessing the environment will be handled via Azure's high-speed data center network. NIH, HBWC, Hospital Applicants, and Contractors would all need to go through either a VPN or through the Azure firewall to access the system. In the event a new role or member needs access the existing or new rule will be set up in Azure to allow for access.

5.2.4.4 Modes of Operation

The modes of operation will consist of **inactive** where when an application is not in use it is preemptively put into hibernation saving the company funds, **active** where the applications that are being used are turned on and made accessible by connecting clients, and **maintenance** where the application is online but is being worked on by HBWC I.T. The server itself will always be active as if it's not available then the application running on the server will also not be available. Backups will be made of the entire system on a nightly basis during this the system can still be used but no new data can be written.

5.2.5 Security and Privacy Architecture

Security and privacy will be predominantly provided by Microsoft Azure as we are using a SaaS-based model where cloud infrastructure is set up running an application where Microsoft Defender for Cloud is used as the centralized security management service. Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) designed to protect applications from various cyber security threats and vulnerabilities. The CNAPP service will provide threat monitoring, recommendations on improvements, identity and access management, compliance management, and information governance, and Azure will be scanning systems on a regular basis to warn HBWC if any new threats are affecting systems HBWC owns. HBWC will ensure that its following mandated federal regulations such as HIPAA along with frameworks such as NIST to meet general system standards to ensure systems and data are secured in new systems working with Microsoft to do so. Microsoft will provide physical security outlined in their Service Level Agreement (SLA) where the data center in which the Windows 2022 Server is running will be managed and monitored by Microsoft. External access for administration or data entry will only be allowed to white-listed groups assigned and created by HBWC I.T. Microsoft's privacy policies are well documented and state any data at rest or in transit will be encrypted and will not be available to the public this is including in virtual machines, databases, and applications hosted in virtual machines. Microsoft will not be inspecting or be able to read data owned by HBWC, Microsoft will not own or claim to own data by HBWC, and will only engage with HBWC post initial set up for support reasons.

5.2.5.1 Authentication

Using Microsoft Azure we will be leveraging Active Directory (AD) to handle group roles and permissions with this single sign-on (SSO) will be used as it's the cloud industry's best practice in cloud-based projects. With the use of AD, the HBWC I.T department will be able to set conditional access policies which will be based on groups, roles, and applications. Administrators of systems will be required to use multi-factor authentication (MFA) which will send a soft token to the admin's cell phone for account escalation. In the event administrator's credentials are stolen the malicious actor will need to also have the generated token which will ensure that administrative accounts are more difficult to access as an administrator will need to know their password and something the administrator has, their phone.

5.2.5.2 Authorization

HBWC and External users will have two different forms of authorization. Using firewall rules and role-based access HBWC I.T and Executive Board can set who has access to what and only give a user access to what they need to complete their role via a least privilege policy. Since the system requires you to be whitelisted in the firewall prior to gaining access and have specific permissions set for your role this will ensure no bad actors have access to critical system(s) or software(s). The authorization has been highlighted below.

Internal

- Employees at HBWC will be required to use a VPN tunnel using the latest traffic encryption (TLS 1.3) to connect to Azure systems.
- Roles are created to administer each system. HBWC I.T will be granted access to the server configuration and database that the SHGTS system is using. HBWC HR will be granted access to Workday as the admins of the system. HBWC Executive will have access to approve and deny requests sent in by hospital applicants.
- Any unauthorized party will be blocked and an alert will be sent to HBWC I.T and HBWC Executive Board

External

- NIH, Hospital Applicants, and Contractors will be required to whitelist in Azure to access the Web Portal to view application status or send grant information.
- NIH will have access to send grants over to the OGG where they will be reviewed by the HBWC Executive Board.
- Hospital Applicants will have access to the Web Portal to view application status (approve/deny).
- Contractors will have access to support and assist HBWC with systems/software however, will only be allowed to work on what was contractually agreed upon.

5.2.5.3 Encryption

HBWC data will need to be fully encrypted which includes databases and connections to systems. Azure's Microsoft Defender for Cloud will ensure applications and data transmitted are encrypted and secured. Microsoft SQL Server 2022 is used as the database for the SHGTS will have Always Encrypted enabled which is a feature that uses column master keys (CMK) and column encryption keys (CEK). The Always Encrypted feature uses NIST FIPS 140-2 as requirements to meet making it an effective solution for data encryption. All Microsoft CMKs encrypt CEKs by using RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP). Internally HBWC will be using a VPN to access Azure systems and external users will need to be whitelisted in the Azure firewall to access the Azure systems. HBWC will review any mandated federal law such as HIPAA and FISMA. For HIPAA compliance states encryption is required in the section of Technical Safeguards in the Security Rule to protect health information and control access to it. While FISMA requires password keys to be changed regularly to ensure data security. Additionally, following NIST SP 800-111 for data at rest and NIST SP 800-52 for data in transit will help contribute to compliance as NIST is a recognized security framework. Since the governing body of the grant system is NIH it is important to be following their lead when it comes to encryption by keeping in line with HIPAA, FISMA, and NIST standards for encryption.

6. Analysis of the Proposed System

6.1 Risks Prioritization and Descriptions

1. **PWC-02**:
    a. **Preferred Alternative**: CentOS/RHEL
    b. **Risk Description:** Outdated server software
    c. **Justification (not to use alternative):** A server running on CentOS due to its open-source nature can easily go out of date and might not have the latest security patches as the open source community would actively need to be working on server software and extensively testing the server software. Based on the time commitment needed an open source operating system would not be a safe choice for HBWC to use. RHEL while enterprise supported may not support application software needed for production service. This will be resolved by the migration of the old server infrastructure. The current SHGTS runs on Microsoft Windows 2008 Server R2. The new server will be on a Microsoft Windows 2022 Server in Microsoft Azure.
2. **PIC-01**:
    a. **Preferred Alternative**: CentOS or RHEL/Apache/MYSQL Server/Intuit QuickBooks
    b. **Risk Description:** No patch management system in place.
    c. **Justification (not to use alternative):** CentOS or RHEL, Apache, MYSQL Server, and Intuit QuickBooks while all offering documentation patching will require HBWC I.T to manually patch systems that would require downtime and employees to work extra hours past regular working hours. This will be resolved by the move to the cloud this will mean patch management on the systems will be handled by Microsoft. The only patch management HBWC will be in charge of is the applications running on the server that were installed by HBWC.
3. **P-Crypt-01**:
    a. **Preferred Alternative**: CentOS or RHEL/Apache/MYSQL Server/Intuit QuickBooks
    b. **Risk Description:** No cryptographic controls in any system at HBWC
    c. **Justification (not to use alternative):** Apache, MYSQL, and Intuit QuickBooks do provide encryption mechanisms for each technology; however, it has to be manually enabled which is not the preferred route for HBWC as it would require expertise on cryptography. With the use of a SaaS-based model Microsoft will be providing fully encrypted tunnels and encrypted databases using Always Encrypted feature in Microsoft SQL Server using AEAD_AES_256_CBC_HMAC_SHA_256 encryption algorithm. All Microsoft CMKs encrypt CEKs by using RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP).
4. **PWC-01**:
    a. **Preferred Alternative**: Apache/MYSQL Server/Intuit QuickBooks
    b. **Risk Description:** Web server not protected by application firewall
    c. **Justification (not to use alternative):** Firewall protection will need to be manually set up if using open-source technologies such as Apache and MYSQL. In Intuit QuickBooks the product does not come with a firewall installed so one would need to be put in front of it to protect from malicious threat actors. Firewall protection will be available at all times via Microsoft Azure's data center network as well as for applications via Microsoft Defender for Cloud.
5. **EDC-01:**
    a. **Preferred Alternative**: None
    b. **Risk Description:** Data center: no physical security

c. **Justification:** HBWC's data center does not meet minimum requirements so it is better to use Microsoft Azure that does meet federal and national standards for physical security. Using Microsoft Azure's data center physical security and protection from the weather will be ensured.

6.2 Risk Analysis

Risk ID	Description	Mitigation/Acceptance	Justification
PWC-02	Outdated server software	Mitigated	Microsoft Windows 2022 Server and Microsoft SQL Server 2022 are adequate technologies to be running enterprise systems as they are on the latest version of each software. It is important that systems are secured, fast, and available. Microsoft Azure can ensure these criteria are met.
PIC-01	No patch management system in place	Mitigated	Using Microsoft Azure we can ensure systems are being patched with the latest security fixes, reporting/logging, and recommendations given to HBWC in the event I.T needs to remediate a threat.
P-Crypt-01	No cryptographic controls in any system at HBWC	Mitigated	Encryption is highly important for an enterprise system. With Microsoft Azure, HBWC I.T can enable Always Encrypt to encrypt databases which uses AEAD_AES_256_CBC_HMAC_SHA_256 algorithm to encrypt data in the database and it meets requirements to NIST FIPS 140-2. All Microsoft CMKs encrypt CEKs by using RSA with Optimal Asymmetric Encryption Padding (RSA-OAEP).
PWC-01	Web server not protected by application firewall	Mitigated	To avoid the expertise needed along with time, funds, and manpower it is better to use Microsoft Azure which provides enterprise-grade firewalls for systems and applications.
EDC-01	Data center: no physical security	Mitigated	Physical security is important and HBWC's data center may not be up to par with federal and national standards. To avoid data loss/corruption, lawsuits, or outages it is important a robust system is set up to handle all weather and physical-related damages such as wear and tear on the system's hardware over time. Microsoft Azure's data center will always keep hardware inside the data center up to date and protected from weather and physical related attacks.

Appendix A: Referenced Documents

Table 9: Referenced Documents

Guide for Conducting Risk Assessments - NIST. (n.d.).

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

S.2521 - 113th congress (2013-2014): Federal Information Security ... Congress . (n.d.).

https://www.congress.gov/bill/113th-congress/senate-bill/2521

Office for Human Research Protections (OHRP). (2021, June 23). Regulations. HHS.gov.

https://www.hhs.gov/ohrp/regulations-and-policy/regulations/index.html

Risk management framework for information systems and organizations - NIST. (n.d.).

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

The NIST definition of cloud computing. NIST. (n.d.-b).

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Risk Management Guide for Information Technology Systems - NIST. (n.d.-a).

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Security Considerations in the System Development Life Cycle - NIST. (n.d.-a).

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-64r2.pdf

Microsoft Access Specifications. Microsoft Support. (n.d.).

https://support.microsoft.com/en-gb/office/access-specifications-0cf3c66f-9cf2-4e32-9568-98c1025bb47c

Windows server 2022 - Microsoft Lifecycle. Microsoft Lifecycle | Microsoft Learn. (n.d.).

https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2022

End of support options - SQL server. End of support options - SQL Server | Microsoft Learn. (n.d.).

https://learn.microsoft.com/en-us/sql/sql-server/end-of-support/sql-server-end-of-support-overview?view=sql-server-ver16

About workday. (n.d.-a).

https://www.workday.com/content/dam/web/se/documents/datasheets/datasheet-about-workday-se.pdf

What is Microsoft Defender for Cloud? - Microsoft defender for cloud. Microsoft Defender for Cloud | Microsoft Learn. (n.d.).

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

Blog. RCDevs Security. (2022, April 7).

https://www.rcdevs.com/why-is-the-software-token-the-best-mfa-method/

Always encrypted cryptography - SQL server. SQL Server | Microsoft Learn. (n.d.).

https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-cryptography?view=sql-server-ver16

Security requirements for cryptographic modules - NIST. (n.d.-d).

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

The Federal Register. Federal Register. (n.d.).

https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312

RSI Security. (2020, February 11). FISMA ENCRYPTION: What you need to know. RSI Security.

https://blog.rsisecurity.com/fisma-requirements-for-encryption/

Guide to Storage Encryption Technologies for End User Devices. NIST. (n.d.-b).

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

Guide to Storage Encryption Technologies for End User Devices. NIST. (n.d.-b).

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. NIST. (n.d.-b). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf