**ASSIST Online Indicator Database**

**Solution Technical Architecture**

**Final Version**

**June 30, 2017**

[Document History 1](#_Toc459786866)

[1. Overview 2](#_Toc459786867)

[1.1. Executive Summary 2](#_Toc459786868)

[2. Hosting / Cloud Platform Solution 3](#_Toc459786869)

[2.1. Microsoft azure 3](#_Toc459786870)

[2.2. Platform as a Service (PaaS) 3](#_Toc459786871)

[2.3. Reliability and support 3](#_Toc459786872)

[2.4. Scalability 3](#_Toc459786873)

[2.5. Global Presence 4](#_Toc459786874)

[2.6. Cost control 4](#_Toc459786875)

[2.7. Automatic Software Updates 4](#_Toc459786876)

[3. Security 5](#_Toc459786877)

[3.1. Azure Active Directory 5](#_Toc459786878)

[3.2. Authentication and Authorization 5](#_Toc459786879)

[4. Application Architecture 6](#_Toc459786880)

[4.1. Web Application / Data Services 7](#_Toc459786881)

[4.2. Mobile Application 7](#_Toc459786882)

[4.3. Database 7](#_Toc459786883)

[5. Source Control 8](#_Toc459786884)

[5.1. Visual Studio Team Services (Team Foundation Services – online) 8](#_Toc459786885)

[6. Compliance 9](#_Toc459786886)

[6.1. Health Insurance Portability and Accountability Act (HIPAA) 9](#_Toc459786887)

[6.2. ASSIST Vulnerability Scanning 9](#_Toc459786888)

[6.3. ASSIST Continuous Monitoring Strategy 9](#_Toc459786889)

[7. Risks Assessment of Hosting With Microsoft Azure PAAS 10](#_Toc459786890)

# Document History

| **Version** | **Date** | **Author** | **Description** |
| --- | --- | --- | --- |
| 1.0 | 8/24/2016 | T. Arseneau | Initial version. |
| 2.0 | 2/1/2017 | T. Arseneau | Updated with internal architecture diagrams. |
| 3.0 | 6/30/2017 | T. Arseneau | Final version. |

# Overview

URC-CHS implements the USAID Applying Science to Strengthen and Improve Systems (ASSIST) Project in over 20 lower- and middle-income countries around the world. The goal of the project is to improve the quality and outcomes of health care and other services by enabling host country health care providers and managers to apply the science of improvement. Fundamental to this science is using real time data to make decisions about what changes are and are not effective in improving health care and other services.

ASSIST tracks data from thousands of health care facilities in dozens of countries around the world. From each facility or site, ASSIST collects anywhere from a few to dozens of indicators, which are usually percentage indicators calculated from defined numerators and denominators. For example: the percentage of women eligible for a service (denominator) who receive that service (numerator). ASSIST collects these data at varying frequencies, including daily, weekly, and monthly.

The new ASSIST Indicator web and mobile application solutions will provide the ASSIST project staff a way to manage, collect, and analyze the quality and outcomes of health care and other services for all ASSIST project activities throughout the world. The solutions and underlying architecture need to provide optimal functionality in a variety of challenging environments, including low bandwidth and no connectivity geographic areas.

## Executive Summary

The new ASSIST Online Indicator Database application will be hosted by Microsoft Azure Cloud Services. The web application will be developed and deployed to Azure’s Platform as a Service (PaaS) framework, and the database will be developed and deployed an Azure SQL Database.

The application will be developed and integrated as a Microsoft Visual Studio project, utilizing Microsoft Team Foundation Server for all source control management. The application will follow best practice application architecture guidelines, and will be designed to separate the solution layers into multiple tiers for presentation, business logic, and data management.

The mobile application will be developed with Microsoft Xamarin for core components, and versions will be deployed for both iOS and an Android operating systems.

Security and Identity services will be developed integrating Azure Active Directory with the URC on-premise Active Directory domain. Authorization for usage of functions within the application will be role based and managed within the application using system administration functions.

Multi-language support will be achieved by the web application using core Microsoft .Net localization technology and design principles for all static application text. Additional language support will be developed within the application and database for data specific language needs.

Health Information and Privacy laws, including HIPAA, will be strictly followed and designed for within the application to insure compliance.

The application will follow guidelines defined by OMB/FedRAMP specific to policies and procedures, security, and disaster recovery requirements for Cloud Service Providers.

# Hosting / Cloud Platform Solution

## Microsoft azure

Microsoft Azure is the market leading cloud and hosting provider, providing cloud services to more than 66 percent of Fortune 500 companies. Microsoft is the cloud provider of choice for hundreds of corporations and organizations, including GE, NBC News, Goodyear, Xerox, Ford, and 3M to name a few.

Azure provides a wide range of hosting and services as a cloud development and operational platform. Although there are other potential choices for cloud solutions, Azure’s combination of administrative support, resource and performance monitoring and reporting, and wide range of products/solutions (virtual machines, cloud services, data services, etc) provide ease of deployment and maintenance.

## Platform as a Service (PaaS)

The legacy architecture for deploying web applications would typically include one to many web servers hosting the web application, with one to many database servers providing the database services and data storage. This architecture requires dedicated resources, both in physical servers and in IT staff resources, to handle the ongoing performance monitoring, maintenance, and procurement of software and operating system updates, and potential scaling tasks when more server processing power or bandwidth is required.

Azure’s Infrastructure as a Service (IaaS) framework provides the ability to host virtual servers in a manner that mimics the traditional legacy architecture. This solution path, however, would still require maintenance of operating system and supporting software and application services. Azure’s Platform as a Service (PaaS) offerings go a stage further and includes the operating system, middleware, and application services as an abstract architectural layer provided and services by Azure.

The ASSIST web and mobile applications will be deployed as Azure PaaS App Services. This solution will provide the best fit for the ASSIST project from a cost, staffing, and scalability perspective.

## Reliability and support

Microsoft provides Service Level Agreements which make commitments for uptime and connectivity. For App Services the SLA guarantees applications running in a customer subscription to be available 99.95% of the time. For Mobile Services and for Database Services the SLA guarantee is 99.9%.

Microsoft offers a variety Azure Support plans which include unlimited 24x7 technical support.

## Scalability

The new ASSIST Online Indicator Tracking application will need to be designed and deployed to allow for the planned increase of users from about 250 users during the initial months to up to 4000 users once all staff and global users are added. In addition, the system will also allow for other organizations to be added to the application which could exponentially increase scale. Microsoft Azure provides a management portal that allows for the scaling of CPU, database, memory, and disk space.

## Global Presence

In addition, Azure provides a worldwide network of over 100 Microsoft-managed datacenters across 26 regions which provide greater flexibility for applications which require global reach and scale (such as the ASSIST application). Deploying of an Azure Application or SQL Database allows for the designation at the client’s discretion of which data centers are utilized, thereby providing very customized, targeted implementations aimed at minimizing response and latency issues.

## Cost control

Azure’s Cloud Services and PaaS framework is an ideal solution for controlling costs related to purchasing and hosting web application and database servers, licensing and maintaining operating system and middleware software, and the cost of IT staff necessary for the ongoing maintenance of those servers. The Microsoft Azure PaaS cost model is pay as you go – the costs incurred will only be for transactions/bandwidth/storage actually utilized within the applications.

## Automatic Software Updates

Microsoft will handle all operating system and security updates required by the Azure servers – URC IT staff will not need to monitor, apply, test, and install software patches related to the server operating system, the middleware, or any other software packages installed as a part of the server infrastructure.

# Security

## Azure Active Directory

In order to implement the integration of the new application with URC’s Active Directory, this project will deploy using Azure Active Directory (Azure AD). Azure AD is Microsoft’s multi-tenant cloud based directory and identity management service. It includes a suite of identity management capabilities including multi-factor authentication, application usage monitoring, rich auditing, and security monitoring and alerting. Azure AD can easily be integrated with the existing URC Active Directory.

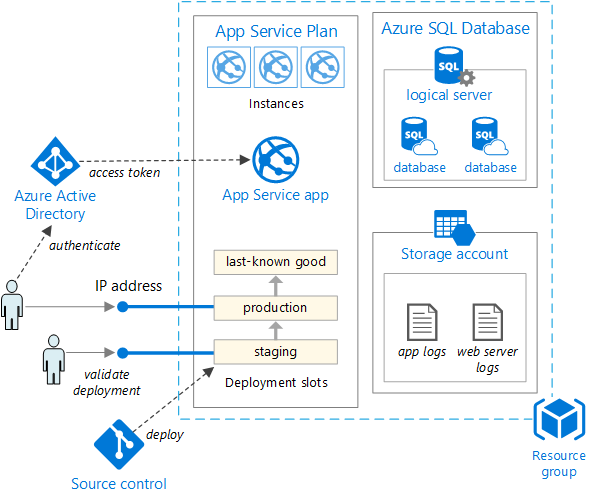
The ASSIST application will use a hybrid security model, interfacing and leveraging URC’s on premise Active Directory for all URC employees, and providing native user management within the application for non-URC users. For access to the application, all users will need to have an ASSIST user table entry, which will include one or more role assignments which will define application access rules. For URC employees, an Active Directory entry will also need be detected to reflect the users are defined by URC as active and valid to access the application.

## Authentication and Authorization

Basic authentication (the ability to sign on to the application) will be implemented using a custom user/password policy defined for the ASSIST application for all external users. Full password encryption will be implemented both within the application and database. For URC employees, the URC On Premise Active Directory will be integrated with Azure Active Directory to provide a single source of URC user information and passwords.

Basic authorization (the determination of what individual users can see and do within the application) will be managed and controlled within the application, implementing custom controls based on organization and role definitions administered by the ASSIST System Administrator(s). An initial set of ASSIST roles will be defined, and each screen will vary in access rules based on a user’s ASSIST role.

# Application Architecture



The ASSIST web application and database solution will utilize many products provided in the Azure Platform as a Service offerings.

## Web Application / Data Services

The ASSIST application will be developed on the Azure App Services platform. Azure App Services provide a means to scale automatically on a load balanced platform, is secured with Active Directory, and provides complete disaster recovery services such as back-up and restore. The App Service framework provides a platform to develop applications that can easily scale within the Azure Cloud.

The application will be deployed using the Microsoft Visual Studio integrated development environment (IDE) and will consist of a solution with multiple projects for each App Service defined. HTML5 standards as defined at <http://www.w3.org> will be adhered to in an effort to provide conformance to those standards as well as improve interoperability.

Following Azure and industry best practices, the ASSIST application will be created as multiple App Service apps – a web application, and a web API. This design will allow for running each in separate App Service plans, which in turn will allow for scaling each independently. The Web API application will serve as the data service for both the web application and for the mobile application.  
  
The business requirements and screen details for the web application are defined and documented in the ASSIST Online Indicator Database Business Requirements document.

## Mobile Application

The ASSIST mobile application will be developed for both iOS and Android devices utilizing Microsoft Xamarin. The Xamarin development platform provides a robust development feature environment and allows for the sharing of common code modules (single source) across multiple mobile operating systems. The mobile application will also deploy with Microsoft HockeyApp, which provides tools to monitor and troubleshoot mobile application testing and usage. The ASSIST mobile application will target a phone form factor only.

URC will need to set up and maintain an Apple App Store account and a Google Play account for application distribution.

The business requirements and screen details for the mobile application are defined and documented in the ASSIST Online Indicator Database Mobile Application - Business Requirements document.

## Database

The ASSIST Database will be deployed as an Azure SQL Database. This infrastructure will provide a highly available, scalable and secure database solution that requires no physical administration by URC IT staff. Utilizing the same service plan scheme that App Services use, scaling and sizing for the database can be managed within Azure’s account dashboard.

In addition, Azure’s Geo Location selection will enable URC to select the exact data centers around the world to get data as close to end users around the world as possible. This distribution will help manage and address network latency issues.

Other benefits of Azure SQL Database include threat detection and alerts, automatic tuning, and multi-tenant support. Also, the same tools and software that are common on the market for managing and developing Microsoft SQL Server databases, objects, and scripts, can also be used for managing and developing Azure SQL Databases.

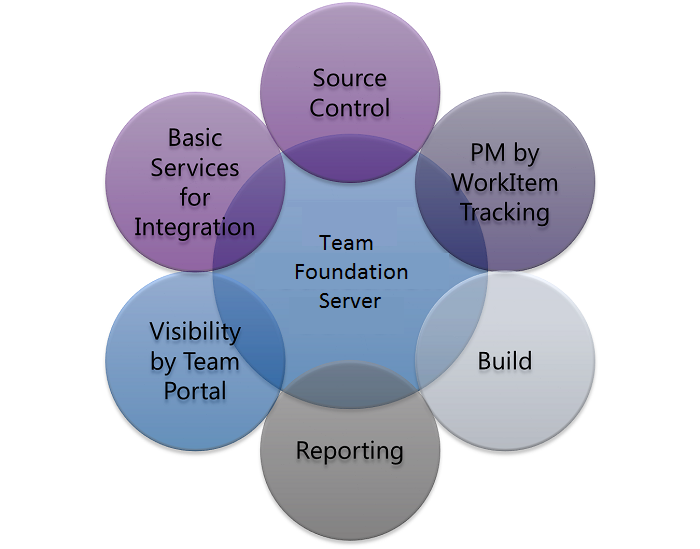
# Source Control

Source control and code management is a critical element in the development and support of software applications. It can be especially critical on projects where multiple developers may update the same code, and when there are multiple environments which may or may not be the same version of the software. In addition, a source version control should be implemented as a complete and comprehensive audit and logging tool to insure only intentional, tested, and approved software changes are deployed to a production environment.

## Visual Studio Team Services (Team Foundation Services – online)

The ASSIST web application will be managed utilizing Microsoft Visual Studio Team Services, which is the online version of Microsoft Team Foundation Services (TFS). In addition to providing a robust source code management environment, TFS provides other key functionality such as change and requirement reporting and management, project management, and automated deployment capabilities.

TFS has a seamless integration with Visual Studio, which will be the integrated development environment (IDE) for the complete lifecycle of the ASSIST application.



# Compliance

The ASSIST application and cloud hosting deployment will follow the guidelines and best practices outlined by the Federal Risk and Authorization Management Program (FedRAMP) for Cloud Service Providers as authorized by the Office of defined by the Office of Management and Budget. Other guidelines include requirements and directives referenced in OMB publications, including the following documents:

Federal Cloud Computing Strategy   
[www.whitehouse.gov/sites/default/files/omb/assets/egov\_docs/federal-cloud-computing-strategy.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf)  
  
The People’s Code – Federal Source Code Policy  
<https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf>  
  
FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide Version 1.0  
<https://www.fedramp.gov/files/2015/01/FedRAMP-JAB-P-ATO-Vulnerability-Scan-Requirements-Guide-v1-0.pdf>  
  
Continuous Monitoring Strategy & Guide, Version 2.0   
[www.fedramp.gov/files/2015/03/FedRAMP-Continuous-Monitoring-Strategy-Guide-v2.0-3.docx](http://www.fedramp.gov/files/2015/03/FedRAMP-Continuous-Monitoring-Strategy-Guide-v2.0-3.docx)  
  
Summary of the HIPAA Security Rule  
<http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/>

HIPAA FAQs for Professionals  
<http://www.hhs.gov/hipaa/for-professionals/faq>

## Health Insurance Portability and Accountability Act (HIPAA)

The HIPAA Privacy Rule establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information. The ASSIST application will not be designed to allow for the collection of any individual’s specific health information. However, there will be functionality to allow for the upload of supporting documentation for observation data collection as file attachments. Any attachment uploaded to ASSIST will not be visible to any other users until a HIPAA review is completed on the attachment manually by a system administrator or other designated URC reviewer.

## ASSIST Continuous Monitoring Strategy

Azure provides various tools to assist with continuous monitoring. Diagnostics are highly configurable and will be defined for the ASSIST App Services to monitor key performance metrics. Rules based on the defined metrics will be configured to trigger alert messaging when values reach the configured metric levels.

Additionally, third party add-ons such as AppDynamics will be evaluated for the ASSIST production environment to determine if further, more configurable monitoring is necessary post implementation of the ASSIST application.

# Risks Assessment of Hosting With Microsoft Azure PAAS

The advantages of cloud PaaS hosting, including decreased costs, reliability, and less IT management needs, easily outweigh the drawbacks. There are, however, some risks and disadvantages associated with PaaS cloud hosting. The following are the main risks of deploying a solution to the Azure PAAS platform:

1. Deploying to Microsoft Azure makes it harder to predict costs and puts URC at the mercy of Azure pricing in the future.   
     
   A typical dedicated server hosting environment would have clearly defined monthly server costs. It will be initially difficult to predict what the pay-as-you-go model of Azure’s PaaS architecture will result in terms of monthly hosting costs. It is however safe bet to be lower, perhaps much lower, than a typical legacy server hosting arrangement. There are other major cloud hosting providers, such as Amazon and Google, which should continue to create an environment of competitive pricing.
2. The reliability of the ASSIST application will only be as good as the underlying Microsoft Azure PaaS infrastructure and software, which URC will not have control or maintenance capability in the case of any outage.   
     
   The fact that URC will have to maintain physical servers, operating system software, and other middleware components is a benefit, but can also be an issue when outages occur. This risk will be mitigated by the contractual expectations set by the Service Level Agreements Azure provides for their PaaS products.
3. Deploying to the PaaS services of Microsoft Azure requires some design and implementation considerations that are specific to Microsoft Azure, and therefore creates a dependency on the Azure PaaS platform.   
     
   Although it is true there are application specific design considerations for Azure PaaS, the structure of an Azure Web App as compared to a standard native web application hosted on a dedicated server is still quite similar, with will have only a few platform specific differences that can be managed with good design and development principles.
4. Deploying to Microsoft Azure creates a dependency on Microsoft stack IT professionals for ongoing support.   
     
   Microsoft has always been and will likely continue to be a major technology stack for both computer application development and implementation. This risk is mitigated by Microsoft’s large market share and presence in the current and projected IT industry software development and implementation market.
5. Customer who deploy applications to PaaS cloud hosting providers only have control and management capabilities of their applications, services, and data, and not on the backend infrastructure and the operating system and supporting software.  
     
   This point is both a benefit and a risk of PaaS cloud hosting. Although control is conceded in managing the infrastructure components, in almost every instance such changes are for maintaining the stability of the hosted environment, and would not have any functional or business value to the actual applications and data deployed. Therefore, if a reliable hosting provider is selected, the risk of this lack of control is mitigated by the service levels and support of the hosting provider.