Plan of Approach
Section 508 Accessibility Compliance Assessment Tool

Installation and implementation Plan of Approach

<table>
<thead>
<tr>
<th>Version</th>
<th>Author</th>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Preety Kumar</td>
<td>Initial Draft</td>
<td>8-15-2018</td>
</tr>
</tbody>
</table>

Contents

Installation of WorldSpace VA Variant (WSVV) ............................................................... 5

Components ................................................................................................................ 5

WorldSpace Comply™ – Enterprise scanning, monitoring and governance ............... 5
WorldSpace Attest™ – Automated testing toolkit ..................................................... 5
WorldSpace Assure™ – Guided Manual Testing ..................................................... 6

System Requirements Review and Approval ........................................................... 6

Installation Considerations ....................................................................................... 7

Perform Content Inventory ................................................................................... 8

Target Data Categorization and Prioritization ....................................................... 8

Catalog ............................................................................................................. 8

Prioritization ...................................................................................................... 9

Categorization ................................................................................................... 9

Reporting Requirements Kickoff Meeting ............................................................. 9

Stakeholder Interviews ......................................................................................... 9

Data Design and Sample Reports ........................................................................ 9

Stakeholder validation .......................................................................................... 9

Iteration .............................................................................................................. 10

Confirm detailed reporting requirements ............................................................ 10

System sizing .................................................................................................. 10

Server Validation .............................................................................................. 11

Installation .............................................................................................................. 11

Installation System Requirements – Internal ...................................................... 11

WorldSpace Comply ............................................................................................... 11
Customer Pre-Installation Requirements ........................................................ 12
Application Server 1 / Core server (Non-Docker) ........................................... 14
Application Server 2 / Analysis server (Non-Docker) ...................................... 14
Database server (Non-Docker) ....................................................................... 15
Installation Methodology for On Premise WorldSpace Comply and Assure
  Internal Servers ............................................................................................ 27
Installation Methodology for Attest .................................................................. 28
Configuration Requirements .............................................................................. 29
Configuration ..................................................................................................... 29
  Comply and Assure reporting configuration ..................................................... 29
  Custom Rules .................................................................................................. 29
  Attest Extension ............................................................................................... 29
  Users ............................................................................................................... 30
Business Process Integration Implementation .................................................... 30
Testing Approach ............................................................................................... 31
  Testing Methodology ....................................................................................... 31
  Automated Testing Approach for Web Applications ......................................... 31
Overall Work Plan/Schedule Tasks ................................................................. 36
Training Plan ..................................................................................................... 41
This document, the Plan of Approach for installation and integration of the Accessibility Compliance Assessment Tool in VA, identifies the methods to be used to conduct installation and configuration of the product as well as the integration of the tool into the business process of the VA.

The Plan also presents an initial detailed schedule for installation and implementation of WSVV that identifies discrete steps/events for the overall work effort and identifies the duration, location, participants (Government and Contractor), along with roles and responsibilities of each, and dependencies.

This plan describes how the automated testing of a web application will be conducted including all steps that will need to be taken by the tool administrator, tools operator, and test requestor from the time a request is received until the time that the audit results are available to the requestor. It also outlines how Deque will meet the requirement of how, at a minimum, ninety-five per cent (95%) of audits will be completed within 15 business days of submission by stakeholder and approval for auditing by government PM.

This is an initial draft of the Plan of Approach. The final plan shall include names, phone numbers, email addresses, and alternates for all participants in the plan.

Following Government PM, Mary Lou Mendez’s, approval of the plan, Deque will implement the plan and begin conducting installation, configuration, and process integration of the WSVV and training courses.

Once the Plan of Approach is finalized, Deque will provide advance written notification to the COR of any deviation from the approved plan, noting the specific deviation, the rationale for the deviation, and impact if deviation is not approved. We will then look for approval of the deviation from the Government PM.

This document outlines how Deque will fulfill the above requirements for the Plan of Approach required in the Contract No. 36C10B18C2746 Award Date: 8-8-2018.
Installation of WorldSpace VA Variant (WSVV)

The WorldSpace VA Variant (WSVV) will be implemented and scaled to accommodate VA’s HTML sites/applications, SharePoint, PDF, Native mobile, eLearning content, documents and software. Our products integrate seamlessly with agile and traditional waterfall methodologies. WSVV uses a common ruleset that can be customized, locked down, and can clearly delineate conformance and best practices. Deque is providing an unlimited perpetual usage of WSVV which includes unlimited WorldSpace Attest™ (API, Integrations and Browser Extensions), WorldSpace Assure™, and WorldSpace Comply™.

Components

WSVV includes the following components that must be deployed in various different capacities within the VA or in the Deque cloud in support of the services being provided to the VA.

1. WorldSpace Comply™, including the Comply Reporting Engine
2. WorldSpace Attest™ HTML
3. WorldSpace Attest™ iOS
4. WorldSpace Attest™ Android
5. WorldSpace Assure™

WorldSpace Comply™ – Enterprise scanning, monitoring and governance

Deque’s enterprise-level scanning, scripting, monitoring and reporting engine will allow the VA to run tests against production and track the “current state” of 508. WorldSpace Comply™ was the first tool to support WCAG 2.0 and is Section 508 Refresh ready. Our reporting engine is a single federated repository for 508. WorldSpace Comply™ will allow the 508 Program Office to improve operational intelligence, maintain historical data integrity and obtain a 360° perspective on 508 including maintaining a dual baseline to understand the impact of the Refresh.

WorldSpace Attest™ – Automated testing toolkit

WorldSpace Attest™ will let development teams at VA automate accessibility testing and test early and often in development. Web developers can stop defects from being introduced in the first place. WorldSpace Attest™ Browser Extensions can be used by developers to test and fix as they develop using browsers they prefer. It can also integrate accessibility into VA’s regular build test automation so the VA team can perform unit and integration testing for accessibility as developers’ code. This product will make great progress in advancing self-sufficiency for the VA.
WorldSpace Assure™ – Guided Manual Testing

WorldSpace Assure™ allows team members with varying skill levels to run guided manual tests for all technologies in use at the VA. WorldSpace Assure™ will help the VA incorporate accessibility testing as a part of normal QA and user testing process while allowing Subject Matter Experts (SMEs) to perform validation as needed. Again, by using this product in testing, the progress towards fully compliant digital content will be advanced in a much more complete manner.

The aforementioned components consist of many different sub-components, not all of which are going to be listed here. However, there are two specific components that require additional consideration and are therefore listed separately:

1. The WorldSpace Attest extension
   a. IE
   b. Firefox
   c. Chrome
2. The WorldSpace Assure extension
   a. Firefox
   b. Chrome

System Requirements Review and Approval

Several components of WSVV will need to go through the process of certification in the TRM and be submitted for a security review:

4. WorldSpace Reporting Services version 1.x
5. WorldSpace Assure version 1.4.x
6. jq version 1.5.x https://stedolan.github.io/jq/
7. Redis 3.x Server
8. Redis 3.x Sentinel
10. OpenSSL 1.0.2k
11. Python 2.7.5x
12. perl-devel
13. perl-CPAN
14. perl-DBD-Pg
15. Keycloak 3.x
16. Pgxnclient
17. Multicorn
18. foreign-keycloak-wrapper
19. Java Development Kit 8
20. Hbase 1.3.x
21. Chromedriver 2.41+
22. RabbitMQ 3.6.4
23. Supervisord
24. Xvfb with X11 dependencies (xorg-x11-font-utils xorg-x11-fonts* dbus-x11)
25. SonarQube 5.x

After the required reviews are completed and an ATO is issued, Deque will start the process of sizing the properties so that hardware can be requisitioned.

Installation Considerations

Implementation of most of the WorldSpace suite is quite straightforward, however there are some components that require thoughtful planning, due to:

1. The need to be able to categorize and tag all generated data in such a way that reports can be produced that meet the needs of the VA stakeholders,
2. The size and volume of reports and assessments being performed by-and-on-behalf of the VA, and
3. The availability of access to target resources outside the VA network
4. User authentication requirements

Specifically, the WorldSpace Comply and Comply Reporting Engine components require significant planning in order to be able to ensure appropriate capacity in the on-premise and off-premise data centers and to configure the software for data tagging. These planning steps include:
Perform Content Inventory

A content inventory is a prerequisite for sizing WorldSpace farms. The VA Section 508 Program Office will need to provide an inventory (# of pages, size) including the following attributes:

1. **Technology**
   a. Web Apps
   b. HTML Web sites
   c. Mobile apps
   d. Sharepoint
   e. Varied Content
   f. eLearning courses

2. **Location (internal vs. external)**

3. **Security constraints (PIV etc.)**

4. **Organization/sub-organization**

Target Data Categorization and Prioritization

The scope of the testing effort is significant and covers a very large number of properties. Most of these properties are not well known by Deque employees. In order to ensure orderly data collection and categorization of results for reporting, we will need to catalog, prioritize, categorize and size the properties.

Catalog

In order to begin the work of assessing the properties, they must be identified. This involves determining their business name, determining the location of the property, determining the accessibility of that location from public or internal network addresses, determining whether the property is protected by authentication and whether this is PIV authentication or some other authentication, and determining the approximate number of pages and the logic that can be used to determine whether a linked address belongs to this property.

Deque will assist the accessibility program office catalogue all of the properties that are in scope. Deque will maintain a list of these properties (the property catalog) on an ongoing basis as we are notified of changes, decommissions, or additions.
Prioritization

To ensure that reports are being produced for the highest priority properties first, catalogued items must be prioritized. We recommend a three tier priority system. Working with the accessibility program office, Deque will document priorities (as provided by the VA accessibility program office) for every property that will be maintained in the property catalog.

Categorization

Collected data must be tagged with the appropriate metadata in order for the required reports to be produced. This involves taking each catalogued property and associating it with the appropriate organizational metadata that will allow the aggregation into organizational units as well as allow the entities responsible to obtain a report at the detailed level.

The categorization will also include the format and version information (inter alia in order to determine whether automated tooling can be used to assist in the assessment). Deque will work with the accessibility program office to categorize each property, utilizing the following steps:

**Reporting Requirements Kickoff Meeting**

The kickoff meeting will identify all the stakeholders for whom reports will be generated and rough outlines of the type of report access each of these stakeholder groups require.

**Stakeholder Interviews**

The project team will schedule meetings and interviews with representatives from each of the stakeholder groups to document their reporting needs. This will uncover the tags and metadata necessary to produce the required reports.

**Data Design and Sample Reports**

Based on the results of the stakeholder interviews, Deque will produce a data design and some sample reports that show how the data design can be used to produce the required reports.

**Stakeholder validation**

The sample reports will be validated with the stakeholder representatives.
**Iteration**

Multiple iterations of design and validation may be necessary before arriving the implementation plan.

**Confirm detailed reporting requirements**

1. Groupings of WCAG success criteria
2. Handling of Section 508 vs. Section 508 refresh requirements
3. Who will have access to which reports (e.g. by VA Component, or specific application)
4. Who will have access to which level of detail
5. Groupings of media-types - e.g. all MS Office docs reported as a single group?
6. Handling of common components
7. Handling of 3rd party components

The production of reports is a critical deliverable for this project. The reporting server requires a good deal of configuration in order to be able to handle the volume of data and in order to be able to produce the types of reports required by different stakeholders.

**System sizing**

At this point, Deque will have the needed data to size the various WSVV components.

The volume of data generated by the assessment activities is estimated to be between 20 million and 100 million rows of raw data per month. This volume of data is significant enough and the estimated range is wide enough that it is of utmost importance to perform a data sizing activity before estimating the hardware configurations required for all the various instances of Comply, Assure and the reporting server.

Working with the accessibility program office, Deque will randomly select 1% of the properties (or at least 10 properties) from each category and analyze them to determine their size. The resulting data will be used to extrapolate over the remaining properties to estimate their size.

Sizing requires also assessing these properties to estimate the number of accessibility issues that each one contains.

Upon conclusion of the sizing exercise, Deque will provide the government with hardware requirements for the Internal installation. Deque will requisition the required hardware for the SaaS (external) installation.
Server Validation

Once the internal servers are made available to Deque, a server certification will be conducted to ensure that all specifications have been met. Any discrepancies will be noted and communicated to the COR.

Installation

Once the sizing and cataloguing exercises are complete we will produce a plan for the installation of the Comply and Assure instances. This plan will detail the number, hardware configurations and location (on-premises vs in-cloud) of Comply and Assure instances that will be required to handle the volume of data generation. The plan will also propose a timeline (with dependencies for hardware requisitioning for the on-premises installations) for the installation of these instances.

We recommend the VA use one of the Linux Operating Systems approved in the TRM. Open source operating systems are identified in the Enterprise Strategic Plan as a strategic priority for the VA Application Modernization Enterprise Design Pattern.

At this time, this plan will be updated to include the details on the amount of hardware required to satisfy the data storage and reporting needs. It will also include a plan for the installation and configuration of the report server and associated data connectors. It is also likely that the plan will include a period of data generation and report testing designed to validate the results of the reporting and modify the configuration to achieve satisfactory results.

Deque will perform the installation of WSVV components and submit an installation notification after installation is complete.

We will also provide an installation report to the VA PM and COR.

Installation System Requirements – Internal

WorldSpace Comply

Introduction

At this time WorldSpace Comply has been verified to work on RedHat 7.x and CentOS 7.x for Linux.
Customer Pre-Installation Requirements

Server Specifications

Each instance of WorldSpace Comply 6.x requires it be installed on 3 servers: 2 for application components and 1 for database. The sizing exercise must be completed before we can determine the number of instances for the VA internal and external analyses.

Each application server must meet the following **minimum** requirements, assuming a 2-node application and a separate database server.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Application Servers / Database Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>16 cores / 16 cores</td>
</tr>
<tr>
<td>RAM</td>
<td>64 GB / 64 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>400 GB / TBD</td>
</tr>
</tbody>
</table>

Based on results of the sizing exercise, Deque will provide updated system requirements. These requirements are minimum system requirements and based on the volume of scans and audits being performed at the VA, minimum requirements will not be sufficient.

Network Requirements

If the allocated servers have unrestricted traffic between them, then the following required ports and connections should be available. WorldSpace Comply cannot be installed nor function without this access.
Figure 1 - Comply Networking

Note - these are the ports necessary for the WorldSpace Comply application to function. You may require SSH (22) and other ports for administrative purposes. We recommend that no other ports be open inbound or outbound on these servers to ensure appropriate network security. To further enhance your network security, we recommend the servers for WorldSpace Comply should be within their own network segment (VLAN) where viable. It’s advised that your network security team scan the servers from a non-Comply node to ensure the minimal access is in place.

The following tables summarize the purpose of the ports noted in the diagram above. Further details regarding the components and architecture of WorldSpace Comply are available if required. Note the tables are denoted as for Non-Docker or Docker installations.
### Application Server 1 / Core server (Non-Docker)

<table>
<thead>
<tr>
<th>Ports</th>
<th>Inbound from</th>
<th>Outbound to</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/443 (TCP)</td>
<td>User browser</td>
<td>n/a</td>
<td>Web interface for WorldSpace Comply</td>
</tr>
<tr>
<td>6379 (TCP)</td>
<td>Analysis server</td>
<td>n/a</td>
<td>Communication to Redis by Worker services on the Analysis server</td>
</tr>
<tr>
<td>5672/15672 (TCP)</td>
<td>Analysis server</td>
<td>n/a</td>
<td>Communication to RabbitMQ by Result Processor and Worker services on the Core server</td>
</tr>
<tr>
<td>8095 (TCP)</td>
<td>Analysis server</td>
<td>n/a</td>
<td>Components on the Analysis server to talk to the Config service</td>
</tr>
<tr>
<td>8761 (TCP)</td>
<td>Analysis server</td>
<td>n/a</td>
<td>Components on the Analysis server to talk to the Registry service</td>
</tr>
<tr>
<td>27017 (TCP)</td>
<td>Analysis server</td>
<td>n/a</td>
<td>Communication to MongoDB by Result Processor on the Core server</td>
</tr>
<tr>
<td>1433 or 3306 (TCP)</td>
<td>n/a</td>
<td>Database server</td>
<td>Access to access/update data in the MySQL or SQL Server database</td>
</tr>
<tr>
<td>25 (TCP)</td>
<td>n/a</td>
<td>Email/SMTP server</td>
<td>Allows WS Comply to send emails</td>
</tr>
</tbody>
</table>

### Application Server 2 / Analysis server (Non-Docker)

<table>
<thead>
<tr>
<th>Ports</th>
<th>Inbound from</th>
<th>Outbound to</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/443 (TCP)</td>
<td>n/a</td>
<td>Customer sites to be scanned by WS Comply</td>
<td>Allows the WS Comply browsers to access sites for scanning</td>
</tr>
<tr>
<td>6379 (TCP)</td>
<td>n/a</td>
<td>Core server</td>
<td>Communication to Redis by Worker services on the Analysis server</td>
</tr>
<tr>
<td>5672/15672 (TCP)</td>
<td>n/a</td>
<td>Core server</td>
<td>Communication to RabbitMQ by Result Processor and Worker services on the Core server</td>
</tr>
<tr>
<td>8095 (TCP)</td>
<td>n/a</td>
<td>Core server</td>
<td>Components on the Analysis server to talk to the Config service</td>
</tr>
<tr>
<td>8761 (TCP)</td>
<td>n/a</td>
<td>Core server</td>
<td>Components on the Analysis server to talk to the Registry service</td>
</tr>
<tr>
<td>27017 (TCP)</td>
<td>n/a</td>
<td>Core server</td>
<td>Communication to MongoDB by Result Processor on the Core server</td>
</tr>
</tbody>
</table>
Database server (Non-Docker)

<table>
<thead>
<tr>
<th>Ports</th>
<th>Inbound from</th>
<th>Outbound to</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1433 or 3306 (TCP)</td>
<td>Core server</td>
<td>n/a</td>
<td>Access to access/update data in the MySQL or SQL Server database</td>
</tr>
</tbody>
</table>

Comply Software Requirements

For a WorldSpace Comply installation, the following components must be available on the servers and running prior to Deque being able to install the Comply v6 application.

Application Server 1 / Core Server

1. Nginx
2. MongoDB*
3. RabbitMQ*
4. Redis-server*
5. supervisord (Linux only)

Application Server 2 / Analysis Server

1. Chrome (recommended browser) *
2. Xvfb (Linux only)
3. supervisord (Linux only)

Database server

1. MySQL 5.7 or MS SQL Server 2012/2014/2016

Required Software Installation Details

The following are additional details on each of the customer-installed components noted above, that will help understand the purpose and assist with the installation process.

Browser

A browser is required for the Comply application to function. Chrome is the recommended browser.

Chrome

The customer should install a recent version of Chrome:

https://www.google.com/chrome/browser/desktop/index.html?platform=linux
**MongoDB**

MongoDB 3.4.4 for Linux should be installed and running:

1. Create and edit mongodb.repo: `vi /etc/yum.repos.d/mongodb.repo`
2. Add the following lines to the mongodb.repo file:

```
[mongodb]
name=MongoDB Repository
baseurl=http://downloads-distro.mongodb.org/repo/redhat/os/x86_64/
gpgcheck=0
enabled=1
```

3. Save the changes to mongodb.repo and exit the vi editor
4. Update yum to register the mongodb repo: `yum -y update`
5. Install MongoDB: `yum -y install mongodb-org`
6. Modify the MongoDB bind address: `vi /etc/mongod.conf`
   a. Change `bind_ip=127.0.0.1` to `bind_ip=0.0.0.0`
   b. Save the changes to mongod.conf and exit the vi editor
7. Enable the MongoDB service: `systemctl enable mongod`
8. Start the MongoDB service: `systemctl start mongod`
9. Check that the MongoDB service is running: `systemctl status mongod`

Please make note of the port number and server address/FQDN which will be used during the application installation process.

**RabbitMQ**

Before installing RabbitMQ 3.6.9 the dependency Erlang must be installed first:

1. Download the Erlang Zero Dependency package manager file: `wget https://github.com/rabbitmq/erlang-rpm/releases/download/v19.3.6/erlang-19.3.6-1.el7.centos.x86_64.rpm`
2. Install the Erlang packages: `yum install erlang-19.3.6-1.el7.centos.x86_64.rpm`
RabbitMQ 3.6.9 should be installed next:

2. Install the RabbitMQ packages: yum install rabbitmq-server-3.6.9-1.el7.noarch.rpm
3. Enable the RabbitMQ service: systemctl enable rabbitmq-server
4. Start the RabbitMQ service: systemctl start rabbitmq-server
5. Check that the RabbitMQ service is running: systemctl status rabbitmq-server
6. Enable the RabbitMQ management plugins: rabbitmq-plugins enable rabbitmq_management

Supervisord (Linux only)

The version 3.0b2 of the supervisord process management utility can be downloaded and installed as follows:

1. Install the epel-release repo: yum install epel-release
2. Install the Supervisor package: yum install supervisor
3. Enable the Supervisor service: systemctl enable supervisord
4. Start the Supervisor service: systemctl start supervisord
5. Check that the Supervisor service is running: systemctl status supervisord

Nginx

Nginx 1.11.3 can be installed as follows:

1. Install the epel-release repo: yum install epel-release
2. Install the Nginx package: yum install nginx
3. Enable the Nginx service: systemctl enable nginx
4. Start the Nginx service: systemctl start nginx
5. Check that the Nginx service is running: systemctl status nginx
**Redis**

Install the 3.2.4 version of Redis:

1. Install the epel-release repo: `yum install epel-release`
2. Install the Redis package: `yum install redis`
3. Enable the Redis service: `systemctl enable redis`
4. Disable the CONFIG command
   a. Edit `/etc/redis.conf`
   b. Remove the comment symbol from the following line: `# rename-command CONFIG ""`
5. Start the Redis service: `systemctl start redis`
6. Check that the Redis service is running: `systemctl status redis`

**Xvfb (Linux only)**
yum install xorg-x11-server-Xvfb xorg-x11-font-utils xorg-x11-fonts* dbus-x11

**SELinux**
Selinux should be set to disabled on Worldspace Comply servers

**Microsoft SQL Server Integrated Authentication**
Integrated authentication with Microsoft SQL Server not supported

**SSL Certificates**
Regardless of installation and OS used the Comply application will require a SSL certificate certificate trust chain, and associated private key, in the format required by nginx (pem format). This is used to protect both the user sessions when interacting with the application through the GUI; as well as, the end-user’s WorldSpace Attest browser extension’s connection to the Comply server

The certificate should either be from a public certificate authority (CA) or if it is self-signed it has to be accepted by the end users’ browsers

**WorldSpace Assure**
WorldSpace Assure is certified to run on Red Hat Enterprise Server 7.3 (RHEL).

WorldSpace Assure should be installed on a dedicated OS which is not used for other purposes.
**Network Configuration**

<table>
<thead>
<tr>
<th>Port</th>
<th>Direction</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>INCOMING</td>
<td>SSH. For application diagnostics &amp; upgrade.</td>
</tr>
<tr>
<td>25</td>
<td>OUTGOING</td>
<td>SMTP. The application requires a suitable SMTP server for automated emails for account verification and other notifications</td>
</tr>
<tr>
<td>80</td>
<td>INCOMING</td>
<td>HTTP. By default the application will redirects to HTTPS.</td>
</tr>
<tr>
<td>80</td>
<td>OUTGOING</td>
<td>HTTP. For application installation. Can be removed after Worldspace Assure installation.</td>
</tr>
<tr>
<td>443</td>
<td>INCOMING</td>
<td>HTTPS. Application API and UI.</td>
</tr>
<tr>
<td>443</td>
<td>OUTGOING</td>
<td>HTTPS. For application installation. Can be removed after Worldspace Assure installation.</td>
</tr>
</tbody>
</table>

For RHEL installations, the system setting httpd_can_network_connect must be enabled as follows:

```
sudo setsebool httpd_can_network_connect on -P
```

**SSL Certificate**

The application will require a SSL certificate, and associated private key, in the format required by nginx (pem format). This is used to protect both the user sessions when interacting with the application through the GUI, but also protects the web-socket connections to the end-user’s WorldSpace Assure browser extensions.

The certificate should either be from a public certificate authority (CA) or if it is self-signed it has to be accepted by the end users’ browsers.

**User Accounts**

The following Operating System User Accounts will be required for the non-Docker based installation and running of the WorldSpace Assure server:

- Installation account for Deque Systems with `sudo` access
- An `assure` user with home directory `/opt/assure-server`
- PostgreSQL and Redis will run as built-in user accounts if installed via package manager

**End User Accounts**

End users of WorldSpace Assure do not require any operating system accounts. WorldSpace Assure user accounts are stored in Keycloak and automatically cached in the database.
Installed software

The following system dependencies are required by the application and for non-Docker based installation must be installed prior to the WorldSpace Assure installation session. These are already included in the Docker containers if using that option:

- PostgreSQL 9.6 (server, client tools, and contrib libraries)
- Redis 3.x (server and sentinel)
- Node.js 9.11.2 (and npm 6.3.0) or earlier (up to Node.js 6.9.5)
- nginx 1.10 or higher (not 2.x)
- jg (1.5 or higher)
- sqitch with libdbd-pg-perl (available in apt or through Perl’s CPAN)
- pgxnclient (for installing database extensions)

These dependencies are available from the core, EPEL, and Remi package repositories for RHEL 7 (except sqitch). Since Node.js updates frequently, installing binaries directly or through an alternative manager such as nvm may be more practical than using the system package manager. The node executable must be available at, or symlinked to, /usr/bin/node with appropriate permissions for the assure system user.

Two database dependencies are not available through standard package managers:

- multicorn
- foreign-keycloak-wrapper

These can be installed through the PGXNclient application, or again, if using Docker, come preinstalled in the PostgreSQL image.

For the Keycloak server (required if there is no WorldSpace Comply service to utilize) the software requirements are:

- Linux OS
- Java 8 JDK

The suggested installation steps as used by Deque follow also covering installation tools and additional prerequisites.

SELinux

Selinux should be set to disabled on Assure server.

Microsoft SQL Server Integrated Authentication

Integrated authentication with Microsoft SQL Server not supported
Database Accounts

A schema owner (assure_owner) and an application user (assure) will be created in PostgreSQL. The database server must enforce md5 authentication locally for these users; this is configurable in /var/lib/pgsql/9.6/data/pg_hba.conf for RHEL.

At installation time Deque Systems will recommend a process for backing up the PostgreSQL database at regular intervals.

SMTP (email) server

The application sends user password resets and other application information through SMTP/email. An SMTP server needs to be reachable and the WorldSpace Assure application will need to be updated with the server hostname and credentials (if required). Please ensure the SMTP server is configured to allow email to be relayed from the WorldSpace Assure host.

Keycloak

WorldSpace Assure 1.4 uses Keycloak, an open source single sign-on provider, to manage user accounts and authentication.

Deque will install the Keycloak application upon the dedicated server provided by the client, if required due to the lack of an existing WorldSpace Comply Keycloak service.

WorldSpace Assure requires access to the master realm in order to administer the system. First, create a dedicated client for the master realm:

1. Navigate to Configure > Clients > Create in the Keycloak admin console
2. Fill out the form and save:
   - **Client ID**: assure-confidential
   - **Client Protocol**: openid-connect
   - **Access Type**: confidential
   - **Valid Redirect URIs**: The base URL(s) of the application instance with the realm subdomain and a global path placeholder (eg “https://master.wsassure.com/**”)

If a realm and users already exist, they can be used with WorldSpace Assure; otherwise, a new realm must be created and enabled. The realm name is important: Assure uses the first subdomain of a request URL to determine which realm it should match the requesting user against.
The following steps assume a realm intended for use with Assure already exists:

1. Create a dedicated client for this realm with the same settings as the master client above, substituting the realm name for “master” in the redirect URIs.
2. Create a new user account, enable it, and set its password.
3. Give this user admin privileges for the realm by navigating to Users > Edit > Role Mappings, selecting “realm-management” under “Client Roles”, and adding “realm-admin” to the assigned roles.

Pre-Installation Steps

This section covers the critical customer steps to ensure the environment is ready for the installation of the Assure application. If the customer is using Docker these steps can be skipped.

**Note:** these steps were confirmed upon a Deque-managed CentOS environment. Customer environments may require variances on some details and this list should serve as a general guide for the customer’s system administrative teams.

1. Install epel-release (yum install -y epel-release)
2. Install the PostgreSQL 9.6 repository (yum install -y https://download.postgresql.org/pub/repos/yum/9.6/redhat/rhel-7-x86_64/pgdg-centos96-9.6-3.noarch.rpm)
3. Install all of the required packages for assure (yum install -y gcc gcc-c++ jq nginx nodejs openssl-devel perl-devel perl-CPAN perl-DBD-Pg postgresql96 postgresql96-contrib postgresql96-devel postgresql96-server python-devel python-pip redis)
4. Update all packages (yum -y update)
5. Install Sqitch
   a. Run the following command (curl -L http://cpanmin.us | perl - --sudo App::cpanminus)
   b. Run the following command (/usr/local/bin/cpanm --quiet --notest App::Sqitch)
7. Exit the SSH session and log back in
8. Install nodejs v6.9.5 (nvm install 6.9.5 && nvm use 6.9.5)
9. Upgrade Python PIP (pip install --upgrade pip)
10. Install PostgreSQL Extension Network Client (pip install pgxnclient)
11. Create a symbolic link for pg_config in /usr/bin/ (ln -s /usr/pgsql-9.6/bin/pg_config /usr/bin/pg_config)
12. Install the multicomp postgresql extension (pgxn install multicomp)
13. Install the foreign-keycloak-wrapper postgresql extension (pgxn install foreign-keycloak-wrapper)
14. Create the application directory (mkdir /opt/assure-server)
15. Create the local assure user (useradd assure -d /opt/assure-server/)
16. Set ownership of the application directory to the assure user (chown -R assure:assure /opt/assure-server/)
17. Initialize the PostgreSQL database cluster (/usr/pgsql-9.6/bin/postgresql96-setup initdb)
18. Edit the PostgreSQL configuration to force md5 authentication (vi /var/lib/pgsql/9.6/data/pg_hba.conf)
   a. Edit line 82 to change the method from ident to md5 (example: host all all 127.0.0.1/32 md5)
   b. Edit line 84 to change the method from ident to md5 (example: host all all ::1/128 md5)
19. Enable the postgresql-9.6 service (systemctl enable postgresql-9.6)
20. Enable the redis service (systemctl enable redis)
21. Enable the redis-sentinel service (systemctl enable redis-sentinel)
22. Enable the nginx service (systemctl enable nginx)
23. Reboot the server

Deque Systems can work with the customer to resolve issues with the required versions documented herein. The use of unsupported versions of required components may require the purchase of additional support hours.

Assure Application Installation

We currently provide guided assistance in executing the installation of WorldSpace Assure, whereby the customer systems administrator will execute deployment of files and executing commands along with a Deque installation engineer. This activity will be coordinated and scheduled to ensure success. During a pre-installation discussion we can provide more specific steps if so desired.

Creating an Organization

WorldSpace Assure supports multiple independent organizations which share a server, but have no access to each other’s data. A minimum of 1 organization other than the “master” administrative organization is required.

To create organizations, log into the master organization:

https://master.my-assure-instance.com/

Once authenticated, you will be prompted for the Keycloak installation credentials and the realm admin username and password for the Assure realm (not the master realm!).
The credentials can be found in the Keycloak admin console by selecting the organization realm, navigating to Clients > assure-confidential > Installation, and selecting the Keycloak OIDC JSON format.

After setting up the Assure organization client, you may choose to add more organizations, or log in to the organization you just created as an administrator to choose the Deque Way content version and allowed standards for testing.

Assure Browser Extension Requirements

The full functionality of WorldSpace Assure requires the user to add a browser extension on their asset. This browser extension is required for the automated and guided testing features of WorldSpace Assure. Manual testing does not require the browser extensions.

The following extensions are supported:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>50+</td>
<td>Windows, MacOS</td>
</tr>
<tr>
<td>Firefox</td>
<td>45+</td>
<td>Android</td>
</tr>
<tr>
<td>Safari</td>
<td>9+</td>
<td>MacOS</td>
</tr>
</tbody>
</table>
The Assure Server will make the extensions available to end-users to download. The Chrome extension install requires a connection to the Chrome Web Store.

If there is an alternative distribution system for browser add-ons in your organization, Deque Systems can work with you to make them available via that.

See the document WorldSpace Assure Browser Extensions for additional details on this subject.

**Assure PostgreSQL Setup**

PostgreSQL can be configured either by manually editing `postgresql.conf` or by using the `ALTER SYSTEM` command in a `psql` session with the server running. Access control is accomplished via the `pg_hba.conf` file.

`shared_buffers` determines the available memory PostgreSQL can use to cache data. The default value is very low; ¼ of total memory is the recommended starting value for modern systems.

**Assure Redis and Sentinel Setup**

Redis and Sentinel stock configuration ships with differing master names (Redis’ as master and Sentinel’s as `mymaster`). Ensure that these are synchronized.

To be fault-tolerant, at least three sentinels must be running.

**Assure nginx Setup**

Assure ships with an nginx configuration file: `conf/nginx.conf`. Place this in `/etc/nginx`, where there should already be a default configuration file. Be sure to edit the `server_name` parameter under the server declaration appropriately.

Place your certificate and key files in `/etc/nginx/cert`. The server’s `ssl_certificate` and `ssl_certificate_key` parameters may need to be updated.

**Assure Log Aggregation**

WorldSpace Assure, PostgreSQL, Redis, and nginx all run as systemd units. Since systemd offers multiple options for StandardOutput, logging for the WorldSpace Assure unit may be configured as required. By default, logging is routed to the systemd journal, and application logs may be accessed through `journalctl`. 
To retrieve logs for Assure between two dates (times are optional):

```
journalctl -u assure-server --since="yyyy-mm-dd hh:mm:ss" --until="yyyy-mm-dd hh:mm:ss"
```

For more options, please consult the `journalctl` man pages or online documentation.

**WorldSpace Assure Extension**

The WorldSpace Assure extension is required to perform automation during the manual assessments on all properties that are only available from the internal network. The extensions will be deployed using the STIG Chrome deployment process.

**WorldSpace Attest API**

The Attest API components will be deployed to the teams via secure FTP site.

WorldSpace Attest is an API that can be run inside your automation test suite, enabling development teams to catch accessibility errors as code is being written. This minimizes the impact of accessibility on cost and schedule.

**WorldSpace Attest Extension**

The extensions will be deployed using the STIG Chrome deployment process.

**WorldSpace Attest AGet**

The AGet application will be deployed via secure FTP site.

**Dependencies**

Attest AGet requires:

- Chromedriver or Selenium (with Firefox or Chrome)
- *Only if you want to use SonarCube*, SonarCube Scanner (recommended default launcher for SonarCube versions 4.5.1+) or SonarCube Runner (for older SonarCube versions 3.7+) installed locally to analyze project data with SonarCube.
- Sonar-Runner
**Installation Methodology for On Premise WorldSpace Comply and Assure Internal Servers**

The typical steps in a five-phase project to deploy a new instance of WorldSpace Comply and Assure are outlined hereafter.

**INITIATE: System installation planning**

- Conduct meeting to clarify requirements, expectations, timelines, roles, and responsibilities
- Model workload – the number of organizations, number of projects, size of scan, scanning frequency, document types
- Model users – organization, roles, permissions
- Specify hardware and network requirements
- Specify special considerations – PIV, Proxy services, and other special requirements
- Specify external dependencies
- Identify people required for installation and collect contact information

**PREPARE: Provision and configure servers**

- Procure servers
- Install servers
- Complete readiness checklist
- Conduct meeting to confirm all readiness items and personnel availability

**INSTALL: Install WorldSpace software**

- Install WorldSpace on servers
- Perform Go-live validation, security, and ATO process

**STARTUP: Setup the first or an example project**

- Create users and groups
- Create one organization
- Create remaining VA organization structures and groups on additional servers
- Configure organization metadata attributes
- Configure organization to lock down rules
- Configure projects
- Configure scans
- Set up scan templates
- Set up scan execution
- Configure VA testing standards and Custom rules
- Set up a scan to be able to spider PIV authenticated sites
- Run Pilot Automated Tests
• Setup manual testing methodology
• Perform pilot manual testing
• Setup pilot Manual test
• Test dashboards
• Test pages, issues
• Test access to help

HANDOVER: Provide training

• Conduct training for System Adminstration, WorldSpace Administration

*Installation Methodology for Attest*

The WorldSpace Attest HTML - Bootstrap Service will equip a web UI development team to begin using WorldSpace Attest to perform automated tests for accessibility as part of their code, build, test, and code-quality reporting process. The Deque Services team will work with VA development teams (Developers, DevOps Engineer, and Build Automation Engineer) to help them integrate WorldSpace Attest into their development and testing tool chain so they can begin to enjoy the benefits that WorldSpace Attest can provide.

This means:

1. **Access to WorldSpace Attest package** - Deque will work with the team to implement access to the WorldSpace Attest API, browser extension, and several executables from the development environment.

2. **Integration test on developer’s machine** - WorldSpace Attest will be integrated into an integration test and will be configured to work on a developer’s machine.

3. **Integration test in Continuous Integration environment** - WorldSpace Attest will be integrated into an integration test and will be configured to work in the Continuous Integration environment.

4. **Accessibility reporting** - The WorldSpace Attest integration test (in the Continuous Integration environment) will be modified to log the results for reporting purposes.

5. **Orientation** - The development team will be trained in the effective usage of WorldSpace Attest.

The installation process for Attest begins with a discovery session to understand the automation and continuous integration process as well as the development environment, framework, methodology, and tools. The Deque team will interview the DevOps Engineer, Build Automation Engineer, and Development Lead to identify what unique attributes need to be considered to create a configuration package.
Configuration Requirements

In order to configure WSVV, the following information needs to be identified:

1. Organizational structure
2. Organization groups
3. Organization users
4. Section 508 policy and associated rules
5. VA manual testing methodology

Configuration

Comply and Assure reporting configuration

Once the Report Planning is complete we will plan how the data design maps onto configuration for the Comply projects and organizations. We will use Comply’s custom project properties to collect the appropriate filtering and aggregation metadata. We will use the Assure test case attributes to collect the appropriate filtering and aggregation metadata.

Custom Rules

WorldSpace custom rules exist from the prior Deque contract. These must be installed onto the Assure and Comply servers. This work will be done as part of the Comply and Assure instances implementation.

For teams using the Attest API or Attest AGet, the custom rules will be distributed via secure FTP server.

Attest Extension

Every extension user must be setup as a user in WorldSpace Comply so that the locked-down rules can be delivered to the user.
Users

1. To begin this process, users will need to submit a request to the VA Section 508 Office and provide:
   a. the name of the tool being requested
   b. their VA email address
   c. their phone number

2. Once the complete information is provided, the team will assist the user in the installation of the tool, if applicable.

3. Team will provide orientation to the tool.

Business Process Integration Implementation

Deque will work with VA stakeholders and business owners to identify WSVV integration points (process and technologies) via a discovery process. After documenting the findings from the discovery sessions, Deque will work with the VA Section 508 Program Office to validate integrations. Deque is proposing an initial set of integration points and creation of epics for each of those integrations based on requirements in the PwS. This list will be revised after the technical kick-off meeting.

Create Business process integration epics for

   a. Reporting and Dashboard
   b. TeamSite Content Management System
   c. Agile development VIP Process and tools
   d. Sustainment Process
   e. Section 508 Automated Custom Rules maintenance and roll-out procedures
   f. Section 508 Manual test reconfiguration process and procedures
   g. Non-compliant content quarantine process, scope and notification procedures
   h. Web Application scripts maintenance procedure
   i. User authentication and access permissions for contractors
   j. User authentication and access for VA employees
   k. Establishing a maintenance schedule
   l. Establishing and testing backup and restore procedures
   m. Establishing server security maintenance procedures
   n. Establish log file management procedure
   o. Establish database management tasks
   p. Maintenance of organization structure model in the tool
   q. Establish user (employee and contractor) onboarding process
   r. Maintenance of user access, role and authorization in the tool
   s. Offboarding of employees and contractors
   t. Periodic user security audits
u. Monthly maintenance of server software to maintain patch-level currency
v. Specify process for upgrades to WorldSpace
w. Periodic testing of disaster-recovery and business continuity procedures
x. VA User training plan modifications
y. Modifications to user training implementation
z. Categorization of Help Desk requests and associated procedures per request category (credentials to tools, password reset, report interpretation etc.)

**Testing Approach**

**Testing Methodology**

Assessment will be performed using the following methodology:

1. Property is identified as next in line based on prioritization
2. External Property scanning setup
3. Automated analysis:
   a. A project will be set up in Comply/Attest
   b. Scanning level will be set
   c. Appropriate tags are applied to the project
   d. Scan is performed
   e. Results are triaged to ensure accuracy
   f. Results are exported to report server
4. Manual testing according to the VA Manual testing process. Project is set up in Assure
   a. Test cases are set up
   b. Automated regression scan is performed
   c. Manual testing is performed
   d. Results are exported to report server

**Automated Testing Approach for Web Applications**

Testing of web applications requires the ability to navigate through a dynamic sequence of screens and submit tasks. A prerequisite to testing web applications is to have all the required test data.
WSVV can handle testing of web applications in several different ways. WorldSpace Attest AGet component, a JavaScript API and Command Line Application (CLI) for fetching and scanning web pages for accessibility issues using the Attest rules engine, can be used to script a path in a “english” like language for a “robot” to follow and record. AGet can be used as a form of codeless testing when you want to fetch and scan web pages for accessibility issues against the Attest automated accessibility rules engine.

This is the recommended method of testing web applications.

An AGet Script sample is included below:

```
"projects": [
    {
        "name": "example",
        "id": "example-id",
        "pageList": [
            {
                "name": "homepage",
                "url": "https://dequeuniversity.com/",
                "actions": [
                    "click element \".loginLink\"",
                    "wait for element \".loginUsername\" to be found",
                    "type \"user@example.com\" into element \".loginUsername\"",
                    "type \"secretpassword\" into element \"#loginPassword\",
                    "click element \"input[type=submit]\"",
                    "wait for element \".logoutLink\" to be found",
                    "analyze page"
                ]
            }
        ]
    }
]
```

Alternatively, WorldSpace Attest Browser Extensions can be used to upload issues to WorldSpace Comply.
Tasks to be performed for Web Application automated testing include:

1. **Actions for tool requestor**
   a. To begin this process, users will need to submit a request to the VA Section 508 Office and provide:
      1. Name of Web Application
      2. Versioning Information
      3. Testing Environment (Production, Pre-production, Development, QA, etc.)
      4. Organization (VHA, VBA, NCA, VACO) responsible for the web application
      5. VA POC email address
      6. VA POC phone number
      7. URL
      8. Additional Instructions on how to access the web application, as needed
      9. Access to the web application has been established, provided, and verified to be working.
      10. Any additional information to test the web application has been provided, if necessary, to include:
          a. Any steps or process required to access the web application (for example, if the tester has to log in through a portal and then the user has to enter information in order to access the web application that is to be tested)
          b. Any test cases required to access portions of the web application
          c. Any other information that is required to operate or navigate the application
   b. Once the complete information is provided, the Government PM will approve the request

2. **Actions for Government PM**
   a. The Government PM will receive, review, and approve the request
   b. The Government PM will notify the team of the approval

3. **Actions for tool admin**
   a. Upon receipt of an approved audit request, the tool admin will
      1. Validate that the information provided can be accessed
      2. Validate that the information provided is complete to include:
         a. Name of Web Application
         b. Versioning Information
         c. Testing Environment (Production, Pre-production, Development, QA, etc.)
         d. Organization (VHA, VBA, NCA, VACO) responsible for the web application
e. VA POC email address
f. VA POC phone number
g. URL
h. Additional Instructions on how to access the web application, as needed
i. Access to the web application has been established, provided, and verified to be working.
j. Any additional information to test the web application has been provided, if necessary, to include:
   1. Any steps or process required to access the web application (for example, if the tester has to log in through a portal and then the user has to enter information in order to access the web application that is to be tested)
   2. Any test cases required to access portions of the web application
   3. Any other information that is required to operate or navigate the application.

3. Once the request has been validated, the Tool Administrator will set up the audit, including:
   a. Creating, uploading and testing scripts, if required
   b. Ensuring the scan settings are set up appropriately for the audit
   c. Ensuring the correct ruleset is applied to the audit
   d. Running a test audit to ensure audit runs as expected
   e. Verifying the audit runs as expected
   f. Verifying the results are as expected

4. Once the audit is ready, the Tool Administrator will set the audit to the appropriate levels and run the scan.

5. If any further auditing needs to occur, the Tool Administrator will notify the team member who will be continuing the audit.

4. Actions for tool operator
   a. If an audit has been previously conducted, the tool operator will receive the audit request. The Tool Operator will:
      1. Verify that the project has already been created in the tool.
         a. If not, the Tool Operator will send the request to the Tool Administrator.
         b. If it is, then the Tool Operator will process the request. This may include but not be limited to:
            1. Verifying the account credentials are current and working
            2. Verifying any scripts previously created are valid
            3. Running the audit
4. Verifying the results are as expected  
5. Performing any additional testing, as required  
6. Triaging the results, as required  
7. Conducting quality assurance, as required  
8. Preparing the audit report and submitting it to the appropriate personnel.

At a minimum, ninety-five per cent (95%) of web application audits will be completed within 15 business days of submission by stakeholder and approval for auditing by government PM.
## Overall Work Plan/Schedule Tasks

<table>
<thead>
<tr>
<th>Task Id</th>
<th>Task Description</th>
<th>Duration</th>
<th>Location</th>
<th>Government Personnel</th>
<th>Deque Personnel</th>
<th>Roles &amp; Responsibilities</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Clearances Paperwork Submission</td>
<td>3 days</td>
<td>Deque office</td>
<td>COR</td>
<td>PM</td>
<td>Deque PM to coordinate completion of required forms. VA COR to forward paperwork to security office</td>
<td>Identification of personnel to be assigned</td>
</tr>
<tr>
<td>2</td>
<td>Fingerprinting</td>
<td>unknown</td>
<td>VA Office</td>
<td>COR, Fingerprinting office</td>
<td>All Deque Team members</td>
<td>Deque PM to submit fingerprinting forms to all Deque team members. Each Deque Team member will complete the form (including subcontractors). Deque PM will submit the forms to the VA COR. The VA COR will coordinate with the VA Security Officer</td>
<td>Receipt of fingerprinting forms, identification of personnel to be assigned to VA</td>
</tr>
<tr>
<td>3</td>
<td>Submission and Obtaining clearances</td>
<td>unknown</td>
<td>VA Office</td>
<td>COR, VA Security Officer</td>
<td>PM</td>
<td>Deque PM will distribute the security clearance forms to all Deque team members (including subcontractors). All Deque Team members will complete the security forms. The Deque PM will submit the forms to the COR via secure mail transmission. VA COR will submit forms to VA Security Office for processing</td>
<td>Receipt of forms, identification of personnel to be assigned to VA, availability of security team to process clearances</td>
</tr>
<tr>
<td>4</td>
<td>Setup of VA Email Accounts</td>
<td>unknown</td>
<td>VA office</td>
<td>COR</td>
<td>PM</td>
<td>Deque PM will provide contractor staff roster to the VA COR and PM. VA COR will request email accounts for Deque team members. Additional &quot;service&quot; email accounts such as accounts for WorldSpace account, help desk will be provided to the VA COR during the installation process and setting up of the help desk</td>
<td>Security clearance approved, Technical Kick-off meeting, Installation commencement</td>
</tr>
<tr>
<td>5</td>
<td>Perform Mandatory Training/Sign ROB</td>
<td>2 days</td>
<td>Deque Office</td>
<td>COR, PM</td>
<td>All Deque Team members, PM</td>
<td>The VA COR will initiate a request for Deque team members to get access to the mandatory courses in the VA TMS. The Deque PM will coordinate the completion of the courses with every team member. Team members will submit the mandatory course completion certificates to the VA PM and COR</td>
<td>Security clearances, VA Email setup complete</td>
</tr>
<tr>
<td>Task Id</td>
<td>Task Description</td>
<td>Duration</td>
<td>Location</td>
<td>Government Personnel</td>
<td>Deque Personnel</td>
<td>Roles &amp; Responsibilities</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------</td>
<td>----------</td>
<td>-------------------</td>
<td>----------------------</td>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>JIT Completion</td>
<td>unknown</td>
<td>VA Office</td>
<td>COR</td>
<td>PM</td>
<td>The VA COR will complete the JIT information for each Deque team member and request any additional information needed from Deque PM. VA COR to provide notification of JIT completion</td>
<td>Security clearances, VA Email setup complete</td>
</tr>
<tr>
<td>7</td>
<td>Obtain PIVs</td>
<td>unknown</td>
<td>VA Office</td>
<td>COR, VA Badging office</td>
<td>PM, All Deque team members</td>
<td>All Deque team members will need to make appointments with the VA Badging Office</td>
<td>JIT completion</td>
</tr>
<tr>
<td>8</td>
<td>Get 21 GFE laptops, 3 iOS devices, 2 Android tablets</td>
<td>unknown</td>
<td>VA Office</td>
<td>COR, VA PM</td>
<td>PM</td>
<td>VA COR will request GFE with required software for Deque team members</td>
<td>PIV issuance</td>
</tr>
<tr>
<td>9</td>
<td>Sync GFE to PIV Cards</td>
<td>1 day</td>
<td>VA Office, NSD</td>
<td>PM, all Deque team members</td>
<td>Deque team members with GFE will schedule appointments with National Service Desk (NSD). NSD will enable PIV authentication for GFE equipment</td>
<td>GFE issuance, PIV Card Issuance</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Get PIV exemption for iOS and Android devices</td>
<td>unknown</td>
<td>VA Office, NSD, ISO (?)</td>
<td>COR</td>
<td>VA COR will request PIV exemptions for iOS and Android devices</td>
<td>Issuance of iOS and Android GFE</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Listing of WSVV components for TRM submission</td>
<td>1 day</td>
<td>Deque Office</td>
<td>COR, PM, CO</td>
<td>PM</td>
<td>Deque PM will provide a list of software along with version numbers in the WSVV that need to be submitted for TRM approval</td>
<td>Draft Plan of Approach</td>
</tr>
<tr>
<td>Task Id</td>
<td>Task Description</td>
<td>Duration</td>
<td>Location</td>
<td>Government Personnel</td>
<td>Deque Personnel</td>
<td>Roles &amp; Responsibilities</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>----------</td>
<td>----------</td>
<td>-----------------------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>12</td>
<td>Content Inventory by technology (HTML, SharePoint, Native Mobile, eLearning, Mobile content), location (internal vs. external to firewall), security requirements (PIV, NTLM etc.), and organization (VACO, VBA, VHA, OIT, etc.)</td>
<td>unknown</td>
<td>VA Office</td>
<td>PM</td>
<td>PM</td>
<td>The VA PM will coordinate collection of content inventory with VA Technical resources so that Deque can size installations of WSVV. The VA PM will provide the content inventory (by technology, location, security requirements and organization) to the Deque PM. The Deque PM will provide this information to the WSVV installation and implementation team</td>
<td>Draft Plan of Approach</td>
</tr>
<tr>
<td>13</td>
<td>Technical Kick-off meeting agenda</td>
<td>1 day</td>
<td>VA Office</td>
<td>COR, PM, Section 508 Program Office Director, CO</td>
<td>PM, CTO, CEO, Installation &amp; Implementation Architect, VP of Services, Project Lead</td>
<td>The Deque PM will coordinate with key Deque team members to create a draft agenda and submit it to the VA PM and COR. VA PM and COR will provide input and revisions to the agenda.</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Technical Kick off meeting</td>
<td>1 day (August 28, 2018)</td>
<td>VA Office</td>
<td>COR, PM, Section 508 Program Office</td>
<td>PM, CTO, CEO, Installation &amp; Implementation Architect, VP of Services, Project Lead</td>
<td>VA and Deque team members will follow the agenda including understanding program goals/objectives, review of Plan of Approach and review of CPMP</td>
<td>Technical Kickoff meeting agenda, availability of attendees, scheduling of meeting, Drafts of Plan of Approach and CPMP</td>
</tr>
<tr>
<td>15</td>
<td>Content Cataloging</td>
<td>TBD</td>
<td>VA Office/Deque Office</td>
<td>COR, PM, Section 508 Program Office</td>
<td>Project Lead, PM, Product Installation team</td>
<td>Jointly, VA and Deque team will catalog the content and document decisions.</td>
<td>Content Inventory and Technical Kick-off meeting complete</td>
</tr>
<tr>
<td>16</td>
<td>Scan Prioritization</td>
<td>5 days</td>
<td>VA Office/Deque Office</td>
<td>COR, PM, Section 508 Program Office</td>
<td>Project Lead, PM, Product Installation team</td>
<td>Jointly, VA and Deque team will establish content scan priorities</td>
<td>Content Cataloging complete</td>
</tr>
<tr>
<td>Task Id</td>
<td>Task Description</td>
<td>Duration</td>
<td>Location</td>
<td>Government Personnel</td>
<td>Deque Personnel</td>
<td>Roles &amp; Responsibilities</td>
<td>Dependencies</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------</td>
<td>----------</td>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>17</td>
<td>Content Categorization</td>
<td>5 days</td>
<td>VA Office/Deque Office</td>
<td>COR, PM, Section 508 Program Office</td>
<td>Project Lead, PM, Product Installation team</td>
<td>Jointly, VA and Deque team will tag the collected data with appropriate metadata.</td>
<td>Content Cataloging complete</td>
</tr>
<tr>
<td>18</td>
<td>Stakeholder interviews</td>
<td>5 days</td>
<td>VA Office/Deque Office</td>
<td>COR, PM, Section 508 Program Office, Agile teams, WSVV users, Content Managers, Document Creators (this list is not complete)</td>
<td>Project Lead, PM, Product Installation team</td>
<td>Deque PM and team will coordinate Stakeholder list and interview schedule with the VA PM</td>
<td>Technical Kick-off meeting complete</td>
</tr>
<tr>
<td>19</td>
<td>Reporting Requirements discovery session</td>
<td>1 day</td>
<td>VA Office/Deque Office</td>
<td>VA Reporting Stakeholders</td>
<td>Project Lead, PM, Product team</td>
<td>The Deque Project lead, PM, product configuration team will work with VA PM to identify report stakeholders and schedule discovery sessions</td>
<td>Technical Kickoff meeting complete</td>
</tr>
<tr>
<td>20</td>
<td>Data design and sample reports</td>
<td>4 days</td>
<td>Deque Office</td>
<td>PM</td>
<td>Project Lead, PM, Product team</td>
<td>The Deque product configuration team will design the data export pipeline and sample reports based on finding of the discovery session</td>
<td>Reporting Requirements Discovery session conducted</td>
</tr>
<tr>
<td>21</td>
<td>Stakeholder validation</td>
<td>5 days</td>
<td>VA office</td>
<td>VA Stakeholders</td>
<td>Project Lead, PM, Deque Product team</td>
<td>The Deque PM will coordinate a review of the reports with the VA PM to get feedback from reporting stakeholders</td>
<td>Content Inventory, categorization, Cataloging</td>
</tr>
<tr>
<td>22</td>
<td>System Sizing</td>
<td>5 days</td>
<td>Deque Office</td>
<td>Product team, Installation architects, PM, Project Lead</td>
<td></td>
<td>The Deque Installation and Implementation team will perform system sizing for the internal instances and SaaS instance of WSVV</td>
<td>Content Inventory, categorization, Cataloging</td>
</tr>
<tr>
<td>Task Id</td>
<td>Task Description</td>
<td>Duration</td>
<td>Location</td>
<td>Government Personnel</td>
<td>Deque Personnel</td>
<td>Roles &amp; Responsibilities</td>
<td>Dependencies</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------</td>
<td>----------</td>
<td>---------------------------------</td>
<td>----------------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>23</td>
<td>TRM approvals/waivers</td>
<td>unknown</td>
<td>VA Office</td>
<td>COR</td>
<td></td>
<td>The VA COR will submit the list of software components not currently approved in the TRM for approval or waivers, as appropriate</td>
<td>TRM Approval List Submission</td>
</tr>
<tr>
<td>24</td>
<td>WSVV installation</td>
<td>3 days</td>
<td>VA Office/Deque Office</td>
<td>COR, PM, CO, VA System Admins</td>
<td></td>
<td>Deque Installation and implementation team will perform the installation. Deque PM will notify the VA COR, PM, CO within 24 hours of installation completion. Deque PM will provide an installation report 5 days after installation.</td>
<td>Sizing requirements, TRM Approvals/Waivers, Servers being available for internal to firewall, onPremise installation, VA System Admin availability</td>
</tr>
<tr>
<td>25</td>
<td>WSVV Setup Configuration</td>
<td>7 days</td>
<td>VA Office/Deque Office</td>
<td>PM, Section 508 Program Office</td>
<td>Configuration team, Project Lead, PM</td>
<td>The Deque product configuration team will configure all components of WSVV</td>
<td>WSVV Installation</td>
</tr>
<tr>
<td>26</td>
<td>Server validation</td>
<td>4 days</td>
<td>VA Office/Deque Office</td>
<td>PM, Section 508 Program Office</td>
<td>Installation and configuration team</td>
<td>The Deque PM will work with the VA PM to validate results from test scans</td>
<td>WSVV Configuration</td>
</tr>
<tr>
<td>27</td>
<td>Business Process Integration discovery sessions</td>
<td>25 days</td>
<td>VA Office/Deque Office</td>
<td>PM, Section 508 Program Office, VA Stakeholders</td>
<td>Project Lead, PM, Integration specialists</td>
<td>The Deque PM will work with the VA PM to schedule stakeholder interviews for business process that will need to integrate/interface with WSVV</td>
<td>Server Validation</td>
</tr>
<tr>
<td>28</td>
<td>Business Process Integration epic creation and validation</td>
<td>30 days</td>
<td>VA Office/Deque Office</td>
<td>PM, Section 508 Program Office, VA Stakeholders</td>
<td>Project Lead, PM, Integration specialists</td>
<td>The Deque Integration specialists will create epics for each integration and backlog of required changes to WSVV</td>
<td>Business Process Integration Discovery sessions</td>
</tr>
<tr>
<td>29</td>
<td>Integration Implementation</td>
<td>unknown</td>
<td>VA Office/Deque Office</td>
<td>Project Lead, PM, Integration specialists</td>
<td></td>
<td>Deque Integration specialists/Dev Services team will perform agreed upon integrations</td>
<td>Business Process Integration epic creation and validation</td>
</tr>
<tr>
<td>30</td>
<td>2 Course Plans Draft</td>
<td>5 days</td>
<td>VA Office/Deque Office</td>
<td>PM</td>
<td>Training Lead</td>
<td>The Deque PM will work with the Deque Training lead and VA PM to create and approve draft course plans for 2 courses. Training will be customized after approval of the course plans and will be provided to the VA PM as SCORM compliant modules for import into the VA TMS</td>
<td>Server Validation and Technical Kick-off</td>
</tr>
</tbody>
</table>
Training Plan

All project employees will have to be trained on the correct use of the WSVV systems in order to ensure that the generated data will contain the correct reporting metadata. Deque will implement this training once the correctly configured systems begin to become available.

1. Develop Training Courses
2. Perform SCORM Testing with VA TMS
3. Contact TMS for TMS submission process (Government Action Item)

The gathering of information of what the VA wants included, and how information should be segregated in the two courses, Getting Started and Advanced Course, will need to occur during a discovery session. This will result in the creation of Course Plans for VA PM/COR’s review and approval prior to the courses becoming available on TMS.