PART 2B

TECHNICAL SPECIFICATION

TABLE OF CONTENTS

1. OVERVIEW

1.1. INTRODUCTION

1.1.1. The information presented in this section serves to provide the Tenderer an understanding of the existing Singapore Customs Technical Infrastructure.

1.1.2. All applications and systems listed in **Part 2A** are deployed on this infrastructure.

1.1.3. The Supplier shall leverage on the Customs Technical Infrastructure environment for the application maintenance and support of all applications and systems listed in **Part 2A.**

1.1.4. The Tenderer shall propose their maintenance and support scope of services based on Customs Technical Infrastructure environment and its services.

1.1.5. The Tenderer may propose new services currently unavailable in Customs Technical Infrastructure environment and services.

1.2. SERVICES

1.2.1. The following are the application services used by all applications and systems in Customs' Technical Infrastructure environment:

Type of Services	**Description**	**Platform**	**Standards**	**Software**
Authentication Service	The Microsoft Active Directory Service provides authentication service to applications.	Microsoft Windows	LDAP	Active Directory
SFTP	The File Transfer service provides uploading and downloading of files.	Microsoft Windows	SSH	F-Secure
SMTP Gateway	The SMTP gateway provides a shared environment to route emails for application systems.	SG-Mail Application Mail Relay (AMR)	SMTP	N.A.

1.2.2. Storage is managed centrally via a dedicated SAN, provisioned by Customs.

1.2.3. Due to the nature of IT products and systems, the above listed services, software and software versions may change over time. Supplier shall work with Facilities Management (FM) on all testing to support the applications and systems.

1.2.4. Customs' current FM services include an on-site team that manages the following:

Type of Services	**Description**
Helpdesk Support Services	Serves as a point of contact for all IT incidents and requests submitted by users, or escalated from any of Customs' IT service provider.
Desktop Support Services	Includes all tools, processes and designs, necessary for the implementation, operation, management and maintenance of Customs' Desktop Services e.g. File & Print, Desktop Access Control, Agency's owned apps and Desktop Security.
Inventory Management	Tracks all Customs' hardware and software inventory.
Server Management	Provides installation, un-installation, re-installation and customization of operating systems, specified application software, drivers, storage and testing of server patches, hotfixes etc
Managed Network Services	Provides administration services for Customs' application networks, equipment, resources, accessibility and provides network maintenance.
Data Centre Management	Manages Customs' data centre operations.
Administration Services	Provides administration services such as security clearance, audit, etc.

1.3. HOSTING

1.3.1. The application, systems and data are hosted in the Server room located in Revenue House.

1.3.2. The infrastructure comprises of physical servers and virtualized servers with different Windows OS versions.

1.3.3. The systems have been hardened based on the following hardening and secured coding guidelines adopted by Customs:

i. Windows Hardening Guide

ii. IIS Server Hardening Guide

iii. System Integrity & Security Controls Checklist

iv. IM Guidelines to secure web services

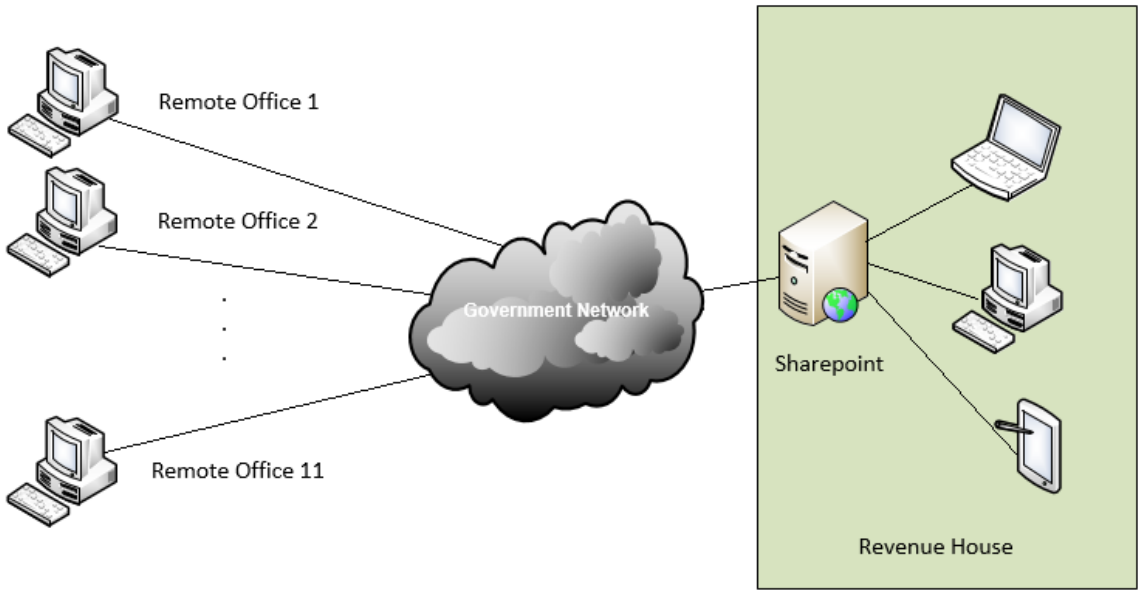
v. Server Security Configuration Guide

vi. Application Design and Development Guidelines and Best Practices

1.4. NETWORK ENVIRONMENT

1.4.1. Customs has offices located island-wide across Singapore. The Corporate Headquarter is located at Revenue House.

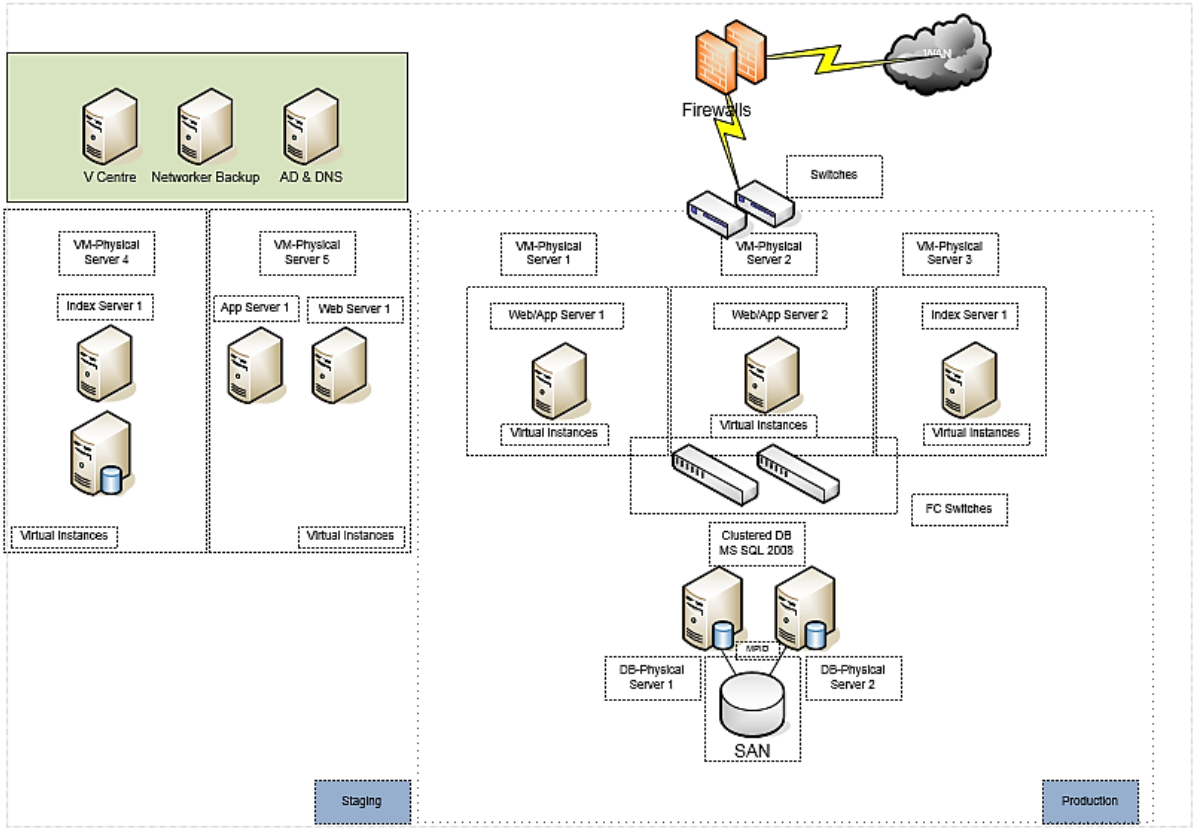
1.4.2. Below is the current network connectivity architecture to the application and data hosted in the Data Centre in Revenue House.



2. SYSTEM ARCHITECTURE

2.1. SharePoint 2007 farm

2.1.1. The following is the Physical System Architecture



2.1.2. The following is the hardware specification

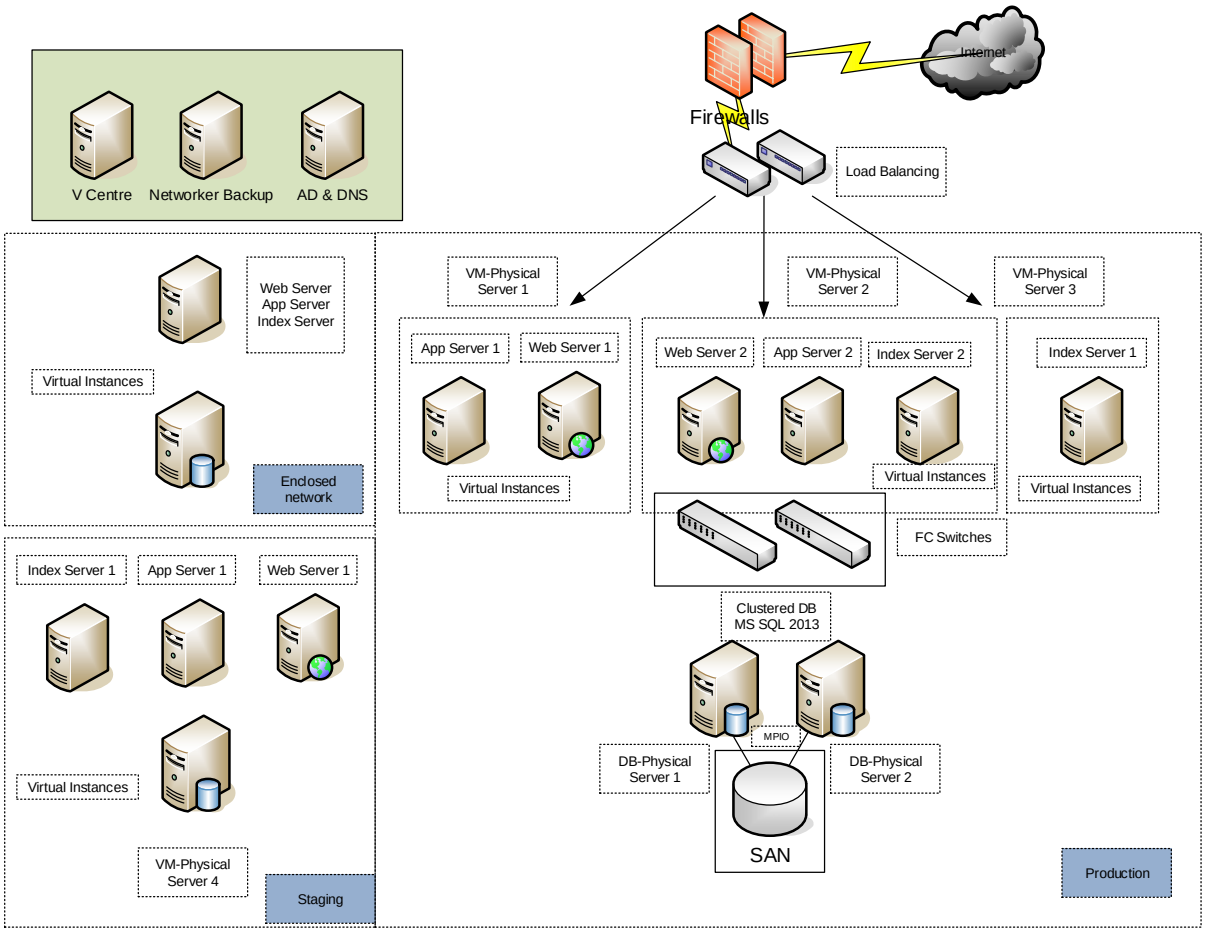
Description	**Specification**	**Quantity**
Production Servers - Web, Application & Index	VM Instances *2 Virtual CPUs* *12GB RAM`*	3
Production Servers - Database	Physical Server *2 way 8-core CPU,* *256 GB RAM,* *2 x 450GB HDD,* *4 x 1GB NIC Card,* *2 x Single FC ports*	2
UAT Servers - Web, Application, Index and Database	VM Instances *2 Virtual CPUs* *12GB RAM*	4

2.1.3. The following is the SharePoint 2007 information

Total Number of SharePoint Farm	1
Total Number of Web application	5
Total Number of Site Collections	14
Total Number of Sites	69
Total Number of Content Database	40
Total Database Size	508 GB
Total Number of Users	1600
Number of Concurrent user	200

2.2. SharePoint 2013 farms

2.2.1. The following is the Physical System Architecture



2.2.2. The following is the hardware specification

Description	**Specification**	**Quantity**
Load Balancers	8GB Memory	2
Production Servers - Web, Application & Index	VM Instances *2 Virtual CPUs* *16GB RAM* *500GB*	6
Production Servers - Database	Physical Server *2 way 8-core CPU,* *256 GB RAM,* *2 x 450GB HDD,* *4 x 1GB NIC Card,* *2 x Single FC ports*	2
UAT Servers - Web, Application, Index and Database	VM Instances *2 Virtual CPUs* *16GB RAM* *500GB*	4
Enclosed Servers - Web/Application/Index	VM Instances *2 Virtual CPUs* *16GB RAM* *500GB*	1
Enclosed Servers - Database	VM Instances *2 Virtual CPUs* *16GB RAM*	1

2.2.3. The following is the SharePoint 2013 information

Total Number of SharePoint Farm	2
Total Number of Web application	3
Total Number of Site Collections	45
Total Number of Sites	5
Total Number of Content Database	42
Total Database Size	650 GB
Total Number of Users	1600
Number of Concurrent user	200

3. CLIENT DESKTOP ENVIRONMENT

3.1. Customs' client machines are currently part of the WOG ICT Infrastructure setup using Microsoft Active Directory.

3.2. Any configurations or installations to be done on the client machines are to be prepared by the Supplier. The configuration or installations files will be sent to the Agency Facility Management (AFM) team to be packaged and certified before deploying to the client machines.

3.3. The applications and systems shall be accessible from the client machines with the following minimum requirements:

- Intel Core
- 4/8GB Memory
- 500 GB Harddisk
- Microsoft Window 7 or higher (64 bit)
- Microsoft Internet Explorer 11 and above
- Microsoft Office 2010/2016 and above

3.4. Do note that all Customs' client machines will be migrated to Windows 10 with IE 11 and Microsoft Office 2016 by the end of year 2016. Supplier shall ensure that all services rendered must take into account of the aforementioned client machine migration.

4. SECURITY REQUIREMENTS

4.1. The Supplier shall fully comply with the latest version of the following policies, standards and guidelines:

i. Singapore Government IM8;

ii. IDA Infocomm Security Best Practices;

iii. Customs IT Security Policy;

iv. Any other security policies, standard and guideline that may be issued by Customs from time to time.

4.2. Customs reserves the right to audit and scan the application system periodically.

4.3. The Supplier shall ensure that proper controls are established for the compliance with this Contract. The Supplier shall cooperate with and provide support, information and assistance to the Government for the purpose of such audits.

4.4. Customs reserves the right to conduct the audit by itself or appoint a third-party auditor. The audit shall cover sufficiency of Supplier's checks and controls which are in place to ensure the integrity of Customs' data and to prevent (if practical) any computer misuse or abuse by the Supplier or any third party.

4.5. The Supplier shall adhere to the Government policies, standards and guidelines.

4.6. The Supplier shall review the existing security features put in place and propose any improvements required for the maintenance of the system.

4.7. The Tenderer shall rectify any shortcomings discovered during the audit within the next three (3) months from the date such findings are reported, or otherwise agreed by Customs. Any cost incurred shall be borne by the Tenderer. Customs shall verify the rectifications through spot-checks or walkthroughs conducted with the Tenderer.

4.8. The Supplier shall provide application maintenance and support for the applications and systems with the objective of maintaining data and software integrity and confidentiality.

4.9. Ensure the application and systems have different levels of system access capabilities to control access by the development staff, system maintenance staff etc. All staff shall only be granted access with valid logon-ids and passwords.

4.10. The Supplier shall ensure that audit trail capabilities and reports which log staff's activities and access to the applications and systems are available. It must also be capable of generating access control reports for Customs' review.

5. AUDIT LOGS

5.1. The Supplier shall configure the system to log all privilege level accesses as well as commands issued to modify the system configuration or parameters where the equipment or system permits.

5.2. The Supplier shall configure the system to log all transactions, personnel's activities, attempted access and security violations.

5.3. The Supplier shall implement audit trail and audit log for system and database activities.

5.4. The Supplier shall also implement the system such that users are able to view the audit trail on screen and print a report if required.

5.5. The audit trail shall be available for six (6) months online, and thereafter, it shall be archived and retained for a period of at least one (1) year. The online duration shall be configurable by the user.

5.6. The Supplier shall ensure that all forms of audit trail shall be appropriately protected against unauthorised access, modification or deletion.

5.7. The Supplier must keep an audit trail of all access to the System for all services and tools. The following items must at least be recorded:

5.8. Successful logon and logoff;

i. Failed logon attempts / failed actions

ii. User ID;

iii. Login Location (IP address);

iv. Date and Time of transaction / logon / logoff

v. Name of File and Service Access.

vi. Action taken

vii. Value before and after changes

viii. Security Policy Changes

ix. Restart, shutdown and system reboot

x. User and group management

6. PERFORMANCE AND RESILIENCY

6.1. The System response time shall be measured as the elapsed time between the moment a user initiates a computer process by pressing a key or clicking a mouse or other input device and the moment the last display of the first screen of the resulting computer-generated output is seen on the screen of the PC. A computer process can be a query or an update to a database, a request of an electronic document or any other logical unit of business transactions that involve interactive responses.

6.2. The maximum System response time of the System when running on Customs LAN shall be as follows:

i. For general usage of the System, the maximum System response time shall not exceed three (3) seconds 90% of the time and five (5) seconds for the remaining 10% of the time. General usage of the System shall include but not limited to the following type of transactions:

Type of Transaction	**Response Time**
Display of webpages	Shall not exceed 3 seconds for 90% of the transactions and 5 seconds for the remaining 10%.
Online Update	
Online Enquiry	
Error Notification	
Online Navigation	

ii. For complex usage of the System, the response time shall not exceed five (5) seconds 90% of the time and eight (8) seconds for the remaining 10% of the time. Complex usage of the System shall include but not limited to the following type of transactions:

Type of Transaction	**Response Time**
Online Search (search results of <= 10,000 records)	Shall not exceed 5 seconds for 90% of the transactions and 8 seconds for the remaining 10%.
Online Filing (filesize <= 5MB)	
Online Report Generation	

6.3. In the event the end-to-end performance from the client is not satisfactory, the Supplier shall investigate the cause of the poor performance and carry out all possible remedial actions and services. In the event the Supplier diagnoses and shows concrete evidence that the problem is due to components not managed by them, the Supplier shall be required to propose the necessary recommendations to Customs to resolve the problem.

6.4. The Supplier shall work with Customs' FM or appointed vendor to review Customs' existing network infrastructure in ensuring that the required System Response Time

could be met. The Supplier shall highlight to Customs, in detail, all necessary actions required for the existing network infrastructure, if according to its expert opinion, the existing network infrastructure could not satisfy the performance requirements. Customs will decide whether to accept the recommendation. Failing which, the Tenderer shall bear all costs required to achieve the required System Response Time.

6.5. The Supplier shall describe the methods and calculations used for computing the expected response time subject to the above conditions in their proposal.

6.6. The Supplier shall proactively monitor and fine-tune the System to ensure that the System meets the performance standards and system availability as stated in the contract.

6.7. The Supplier shall ensure that failure of a transaction or reporting at one workstation shall not affect users at other workstations.

6.8. The Supplier shall ensure that failure of any transaction or a software fault in any of the functions in the System shall not affect the integrity of the data captured / stored or lead to any loss of data in the System.

6.9. The Tenderer shall ensure that the System performs the necessary checking on data transmission to detect failure of improper or missing data.

6.10. The System shall be required to run unattended after operating hours for System operations such as backup of databases, and run end-of-the-day processes.

6.11. For System operations, the Supplier shall be responsible to ensure that these System jobs will not affect existing Customs operations or the System Performance during its execution.