Market Research for
Design, Supply, Delivery, Installation, Configuration, Implementation, Commissioning, System Support and Maintenance, and other Related Services for Modules Comprised in the Smart Customs Information Technology Infrastructure (SCITI)

1. Points to Note

This market research is issued solely for understanding the responses of the market to facilitate the planning for the project for the Design, Supply, Delivery, Installation, Configuration, Implementation, Commissioning, System Support and Maintenance, and other Related Services for Modules Comprised in the Smart Customs Information Technology Infrastructure (SCITI, or the System).

This market research is not part of a tendering process and will not be used to short-list or select suppliers/products. It does not entail any commitment on the Government, either financial or otherwise, for any supply or service whatsoever. Submission of the response to this market research is made on the understanding that the Government will not incur any liabilities nor be liable to pay any costs arising out of the preparation or submission of the response.

Suppliers shall indicate which parts of their responses, if any, are "commercial in confidence". All information, including personal data and commercially sensitive information (if any), provided in the response to this market research will be used for this exercise only.

2. Project Overview

2.1. Objective

The objective of this market research is to gather responses of the market for planning the SCITI project.

2.2. Background

In 2019, the Customs and Excise Department (C&ED) promulgated the "Smart Customs Blueprint" to steer the development of Smart Customs, covering all core aspects of C&ED's business. A pivotal objective of the "Smart Customs Blueprint" is to build up an all-in-one Smart Customs, through using innovative technology in the formulation, development and deployment of various systems, equipment, devices and tools, as well as enabling data sharing within C&ED.

In tandem with the "Smart Customs Blueprint", C&ED completed an Information Systems Strategy Study (ISSS) in 2020, which put up recommendations for C&ED to better utilise information technology (IT) to achieve digital transformation and make effective use of data in its business. Recommended under ISSS, SCITI provides the foundation for upgrading existing IT systems, accommodating new IT initiatives, and assisting C&ED in meeting existing operational needs and future developments.

SCITI includes four (4) modules, namely Cloud Infrastructure Platform (CIP), Security Information and Event Management System (SIEM), Revamp of Central Information Repository System (rCIRS) and Customs Big Data Application System (CBDAS). They are briefly described as below -

(a) To implement the CIP module to be a scalable, modular and expandable private cloud computing infrastructure which shall be a Government Cloud Infrastructure Services (GCIS) Type-2 Satellite Site. CIP shall form the infrastructure of the System, and will act as a new central hosting infrastructure with enhanced operational efficiency for application systems of C&ED in the future. CIP shall fully comply with the requirements as stipulated in the Government Cloud Adoption Framework (GCAF);

(b) To implement the SIEM module to collect, monitor and analyse log data generated throughout the C&ED's IT equipment, either in the CIP or in existing C&ED's IT equipment, including servers, network devices, security devices and endpoint protection system, and to improve the efficiency of locating the possible threat through the log analysis by correlation rules and security analytics;

(c) To redevelop and convert the data of the existing Central Information Repository System (CIRS) by migrating it to the CIP with an aim to improve its performance, scalability and interoperability through redesigning its infrastructure and software components such that it shall seamlessly integrated as one of the modules of SCITI, viz. revamp of Central Information Repository System (rCIRS) module; and

(d) To implement the CBDAS module which will include infrastructure and functionalities for data acquisition and transformation, data warehouse and data lake, as well as data visualisation and dashboard for fully utilising big data to facilitate C&ED's operation.

2.3. Scope of work for SCITI

2.3.1. The scope of work shall include at least the following core tasks with high level requirements specified for implementing the System -

I. Project Management

(a) Provide project management services during all the stages of implementation of the System, which include project monitoring and coordination of the implementation activities of all relevant parties including other contractors, in-house project teams and other bureaux/departments (B/Ds) of the Government.

II. System Design, Supply and Implementation

(a) Design, build, document, test and implement the System.

(b) Conduct system analysis and design for a new system infrastructure of cloud-native platform in government and/or non-government data centres, software applications (i.e. custom programs) to cover all four modules of SCITI. High-level functional requirements of the System are provided in **Appendix 1**.

(c) Provide hardware and software for the System. Lists of hardware and software are provided in **Appendix 2** for reference.

(d) Implement the System for provision of the new system infrastructure and software applications to meet the functional and business requirements within twenty-one (21) months.

(e) Be responsible for overall planning, study, design, implementation and provision of data conversion and migration services for converting and migrating all necessary data and programs of existing systems to be replaced by SCITI.

(f) Develop test plans, prepare test data and perform the tests required, evaluate test results, perform corrective actions and re-testing.

(g) Conduct functional tests, system integration tests, acceptance tests, connectivity tests, resilience tests, rehearsal, load test, reliability test and installation test.

(h) Coordinate relevant activities with in-house project teams and other parties as required by the Government.

III. System Hosting Services, Site Preparation and related Facilities

(a) Primary Production Environment (PROD-1) and Secondary Production Environment (PROD-2) shall be hosted in two (2) different locations.

(b) Provide data centre hosting services ("System Hosting Services") for the hardware and software mentioned in **Section 2.4.1** below in data centres sourced by the supplier (“Outsourced Data Centres”) **if** any of the system environments of the proposed System cannot be hosted within the maximum available space provided by the Government and maximum total power provided at C&ED data centres as depicted in the following tables. **Section 3 of Appendix 2** lists out the required service (if applicable).

Data Centre	Maximum Available Space provided by the Government	Maximum Total Power provided at C&ED Data Centre[a]
C&ED Primary Data Centre (CED-PDC)[b]	22 racks	108 kW
C&ED Secondary Data Centre (CED-SDC)	46 racks	249 kW
C&ED Disaster Recovery Data Centre (CED-DRDC)	2 racks	8 kW

Data Centre Location	Hosted Environment
CED-PDC or Outsourced Data Centres (if applicable)	PROD-2 and / or Testing Environment
CED-SDC or Outsourced Data Centres (if applicable)	PROD-1 and / or Testing Environment
CED-DRDC	N/A[c]

Note:

(a) Each rack shall normally consume at most 8 kW.

(b) Available space in CED-PDC was made up of three (3) area with below specification:

Name of area in CED-PDC	Maximum Available Space provided by the Government for the Zone	Maximum Total Power provided at C&ED Data Centre for the Zone
Zone A of CED-PDC	5 racks	30 kW
Zone B of CED-PDC	4 racks	18 kW
Zone C of CED-PDC	13 racks	60 kW

(c) CED-DRDC is a separated site to deploy site monitoring equipment if necessary.

(c) All hardware in CED-PDC shall be housed in maximum weight of 1000 kilogram per square meter (kg / m^2) of each computer rack;

(d) All hardware in CED-SDC shall be housed in maximum weight of 680 kg / m^2 of each computer rack; and

(e) All hardware in CED-DRDC shall be housed in maximum weight of 750 kg / m^2 of each computer rack.

(f) Provide all necessary cabling services, racks, network setup, hardware and software installations, configurations and tuning, and environment facilities monitoring (applicable for Outsourced Data Centres) for all the system environments. Please refer to **Section 2.4.1** below for the system environments required.

(g) Coordinate with other Government contractors and related parties such as the Architectural Services Department (ArchSD) and the Electrical and Mechanical Services Department (EMSD) on site preparation related matters.

(h) Provide the required communication lines for the System, with sufficient bandwidth and resilience, as stipulated in **Section 2 of Appendix 2**.

IV. Production Rollout, Transitional Arrangement, and System Nursing

(a) Conduct data and account migration from existing replaced systems to SCITI.

(b) Propose rollout approach and planning, and conduct rollout drill before formal system rollout.

(c) Roll out the System and coordinate with other contractors and parties as requested by the Government.

(d) Provide 4 months system nursing services for the implementation of the System.

V. Training

(a) Provide adequate training (including classroom training, where applicable) which includes technical training, internal users training, and train the trainer training, etc.

(b) Provide, customise and maintain training facilities such as hardware, software, training manual, and training materials.

(c) Provide at least ten (10) different types of classes for different attendants. The total number of sessions shall be at least ninety (90) and the duration for each session shall be at least half day.

VI. System Support and Maintenance for Hardware, Software and related Facilities

(a) Provide system support and maintenance to the System during the Maintenance Period of ten (10) years after the System Acceptance Date, including the hardware, software, custom programs, communication lines, and System Hosting Services (if applicable).

VII. Security Risk Assessment and Audit, Government Cloud Adoption Framework Security and Compliance Audit, and Privacy Impact Assessment

(a) Engage, at its own costs and expenses, an independent third party contractor to perform an IT security risk assessment for the System at the stage of system analysis and design, and an IT security risk assessment and audit exercise for the System before production rollout.

(b) Provide assistance in security risk assessment and audit and fix all vulnerabilities and risks identified.

(c) Engage, at its own cost and expense, an independent auditor to perform Government Cloud Adoption Framework (GCAF) Security and Compliance Audit of the GCIS Satellite Site upon completion of integration with GCIS and before the production rollout.

(d) Provide assistance in GCAF Security and Compliance Audit and fix all non-compliance items to gain the compliant status from GCIS Management Team.

(e) Appoint, at its own costs and expenses, an independent third party consultant to be agreed by the Government to conduct Privacy Impact Assessment (PIA) and Privacy Compliance Audit (PCA) for the System at the stage of system analysis and design and before production rollout.

2.4. System Environments and Workload

2.4.1. This section aims to provide essential information of the system environments and workload.

I. System Environments

(a) The System shall include at least the following environments -

- Primary Production Environment (PROD-1) at C&ED Secondary Data Centre (CED-SDC) or Outsourced Data Centres (if applicable);
- Secondary Production Environment (PROD-2) at C&ED Primary Data Centre (CED-PDC) or Outsourced Data Centres (if applicable); and
- Development and testing environment (Testing Environment) at CED-PDC or CED-SDC or Outsourced Data Centres (if applicable).

(b) The PROD-1 and PROD-2 shall equip with local resilience for each system component of the CIP and SIEM modules and the required system components of the rCIRS module to provide high availability.

(c) The PROD-2 will be set up in a data centre different from that for PROD-1 to serve as a hot-standby remote resilience site. The PROD-2 shall take over the required system role of PROD-1 during site disaster in PROD-1 except CBDAS module which shall be hosted in PROD-1 only.

(d) In case of disaster recovery required, CIP, SIEM, and rCIRS modules in PROD-1 shall failover to the other production environment PROD-2, and vice versa. Time required for such failover shall be less than two (2) hours.

(e) The Testing Environment shall be used for development, testing and training such as user acceptance test, system integration test, training, data conversion and migration test. Equipment for Testing Environment shall be securely separated from those for production environments.

II. Workload

(a) The System shall provide sufficient capacity to support workload for at least ten (10) years from the system production date.

(b) The System shall support the operating hours at 24 hours a day, seven days a week throughout the year.

(c) System support and maintenance services for the System shall be provided throughout the prime maintenance period as follows -

System environment	The prime maintenance period
PROD-1 and PROD-2 environments	7 days a week x 24 hours a day including public holidays throughout the year
Testing Environment	8:30 am to 6:25 pm, Monday to Friday (excluding public holidays)

(d) The centralised backup and restore solution for the System shall be able to backup all four (4) modules of SCITI with one (1) full copy and 27 incremental copies. It is assumed to have 3% of delta change for all the components each day.

(e) For SIEM module, the estimated daily log volume for production and development environments would be around 100 GB and 72 GB per day respectively.

(f) For rCIRS module,

i) The estimated number of users shall be around 1 200.

ii) The estimated maximum number of concurrent users shall be around 120.

iii) The current Data Warehouse Database stores the structured data. It contains 3 800 tables, 2 800 views, 1 800 triggers, 600 stored procedures and 200 stored functions.

iv) The estimated data volume for the raw data at the time of rCIRS launch shall be around 31 TB then shall grow to 160 TB throughout the Maintenance Period. Suppliers shall calculate and include additional data volume required to house the system overheads for indexes, archive logs, temporary table-spaces, audit trails, data and logs of system software, database replication and resilience.

v) The User Acceptance Test environment of rCIRS shall be able to support at least 30 testers to conduct user acceptance test at the same time.

(g) For CBDAS module,

i) The estimated number of users shall be around 1 200.

ii) The estimated maximum number of concurrent users shall be around 100.

iii) The estimated data volume for the structured data at the time of CBDAS launch shall be around 62 TB then shall grow to 374 TB throughout the Maintenance Period.

iv) The estimated data volume for the unstructured data at the time of CBDAS launch shall be around 34 TB then shall grow to 126 TB throughout the Maintenance Period.

v) When estimating disk storage space for CBDAS, suppliers shall consider the overall requirements including but not limited to the storage requirements for structured data and unstructured data (including semi-structured data) of the data lake and the databases of different formats (including but not limited to row-based database, graph-based database, tree-based database, etc.), staging areas, archive logs, temporary storage spaces, audit trails, data replication and resilience.

i) The User Acceptance Test environment of CBDAS shall be able to support at least 30 testers to conduct user acceptance test at the same time.

2.5. Staff Requirement of the Project

2.5.1. This section aims to provide essential information of the minimum staff requirement for implementation and for system support and maintenance.

I. Staff Requirement for Implementation

(a) The implementation team shall comprise at least the following roles -

Role	Number of Staff for Each Role	Total Man-months (for all staff with same role)
Project Manager	1	21
For CIP		
Infrastructure Architect cum Team Leader	1	6
IT Specialist	2	12

Role	Number of Staff for Each Role	Total Man-months (for all staff with same role)
Network Specialist	2	12
System Engineer	3	24
For SIEM		
System Analyst cum Technical Team Leader	1	6
Analyst Programmer	1	12
For rCIRS		
Application Architect cum Team Leader	1	12
System Analyst	4	48
Programmer	8	84
Programmer	10	60
For CBDAS		
Application Architect cum Team Leader	1	21
Lead System Analyst	2	42
System Analyst	2	42
Data Conversion Analyst	1	15
Data Lake Administrator	1	15
Analyst Programmer	4	60
Programmer	4	60
Web Designer	1	6
Technical Writer	1	6

II. Staff Requirement for System Support and Maintenance

(a) The system support and maintenance team shall comprise at least the following roles (except rCIRS which system support is not required) -

Role	Number of Staff for Each Role	Total Man-months (for all staff with same role)
Maintenance Manager	1	1
For CIP		
IT Specialist	1	2
System Analyst	2	24
Database Administrator	1	4
System Engineer	1	12
For SIEM		
System Analyst	1	6
Analyst Programmer	1	10
For CBDAS		
Team Leader	1	12
System Analyst	2	24
Analyst Programmer	2	24

2.6. Government Standards and Guidelines References

Suppliers shall comply with and adopt Government standard and guidelines as well as the security related policy and guidelines in C&ED. Brief descriptions on the standards and guidelines are available for reference on the website https://www.ogcio.gov.hk/.

3. Required Information

Suppliers interested in responding to this market research shall provide the following information -

(a) Company and contact information;

(b) Implementation approach and plan;

(c) Estimated cost with breakdown for one-off implementation and on-going system support and maintenance, including -

i. implementation services including project management, quality assurance, site preparation, installation / configuration of hardware / software and related facilities, cabling services, system analysis and design, program coding, conducting system integration tests, assisting user acceptance tests, data conversion and migration, system tuning, disaster recovery setup, production rollout and nursing;
ii. provision of hardware and software for the System;
iii. provision of communication lines;
iv. provision of System Hosting Services (if applicable);
v. training services for system users and application users;
vi. Security Risk Assessment and Audit (SRAA), Government Cloud Adoption Framework (GCAF) Security and Compliance Audit, and Privacy Impact Assessment and Privacy Compliance Audit (PIA and PCA);
vii. system support and maintenance for a ten (10)-year maintenance period; and
viii. any other services.

4. Submission for Market Research

4.1. Participation to Market Research

To respond to this market research, suppliers shall provide the required information listed in **Section 3** above on or before the submission date and time mentioned below.

Any enquiries shall be made through the following channels -

- by email to arthur_yc_chan@customs.gov.hk; or
- by mail to the Office of Information Technology, 27/F, Customs Headquarters Building, 222 Java Road, North Point, Hong Kong
(Attn: Systems Manager (ITU10))

4.2. Submission Date and Time

The deadline for submission of the required information to this market research is **12:00 noon of 2 April 2024** Hong Kong time.

4.3. Submission Method

Required information to this market research, including materials listed in "**Section 3 – Required Information**" shall be prepared using the submission template (**Appendix 3**) and submitted through the following channels -

- by email to arthur_yc_chan@customs.gov.hk; or
- by mail to the Office of Information Technology, 27/F, Customs Headquarters Building, 222 Java Road, North Point, Hong Kong
(Attn: Systems Manager (ITU10))

- End -

High-level Functional Requirements of SCITI

1. Introduction

1.1. SCITI (the System) shall cover four modules and shall meet the following high-level functional requirements.

1.2. The CIP module shall provide a cloud infrastructure platform for SIEM, rCIRS, CBDAS modules and shall pave the way for future C&ED systems.

1.3. SIEM, rCIRS and CBDAS modules shall be hosted on CIP module.

2. High-level Functional Requirements of CIP module

Virtualisation Infrastructure

2.1. Support live migration of virtualisation machines (VMs) across PROD-1 and PROD-2.

2.2. Provide an integrated platform for provisioning, management and monitoring of resources including the compute, storage and network resources of the System.

2.3. Provide customised templates of commonly used operating system (OS) platforms and software stack.

2.4. Provide a web-based self-service portal.

2.5. Support sending system healthiness status and security alerts to Government Cloud Infrastructure Services (GCIS) Central Cloud of the Office of the Government Chief Information Officer (OGCIO) via custom Application Programming Interface (API).

Disaster Recovery (DR) Automation and Orchestration

2.6. Provide DR automation and orchestration solution to automate the failover processes by orchestrating with the hypervisor, virtualisation infrastructure manager (VIM), storages, software-defined network (SDN), as well as other components of the System.

2.7. Fully integrate with the replication solution of the System.

2.8. Support automatic failover and failback of VMs, containers, database service and other services between PROD-1 and PROD-2 environments.

2.9. Support non-disruptive testing of the recovery plans without causing any interruption to the data replication of storage system.

2.10. Failover to another production environment for all services shall be no more than two (2) hours.

Storage Systems

2.11. Use Software Defined Storage (SDS) except for components where local storage is used.

2.12. Implement with identical SDS for the PROD-1 and PROD-2 and the SDS shall support cross-site data replication to minimise data loss in case of disaster.

2.13. Provide data at rest encryption with Advanced Encryption Standard (AES) 256-bit key. The ultimate decryption keys shall be stored separately from the corresponding encrypted data.

Cloud Network

2.14. Comprise physical network equipment, SDN software and other related components for the System and shall be fully compatible with the existing C&ED network infrastructure.

2.15. Adopt an overlay-underlay network design. The overlay network shall make use of the underlay physical network infrastructure to transport Internet Protocol (IP) packets among physical servers and equipment.

2.16. Traffic to and from the System shall only pass through the edge gateway. All possible physical and logical connections between the System and existing C&ED network shall be controlled by edge gateway.

Centralised Backup and Restore Solution

2.17. Separate from other storage of the System.

2.18. Support disconnection of backup data from the System by physical or logical means.

2.19. Support data replication to the remote production environment to support one (1) off-site secondary copy.

2.20. Support encryption of all data stored on backup repository.

2.21. Meet the usable storage size requirement in item 4.1 of **Table 1.1 in Appendix 2**.

Container Orchestration

2.22. Provide Kubernetes based or compatible clusters using a cloud native approach.

2.23. Include Development and IT Operations (DevOps) services.

2.24. DevOps services shall cover at least below processes -

- continuous integration and continuous delivery (CI / CD);
- code repository and management;
- artifact repository and management;
- unit test; and
- deployment.

Database-as-a-Service (DBaaS)

2.25. Provide a fully managed database environment and support multi-tenancy in a cloud native approach.

2.26. Support MySQL-compatible or PostgreSQL-compatible database as relational database services for Online Transactional Processing (OLTP) workload for the System.

2.27. Support data replication between PROD-1 and PROD-2 for site recovery in no data loss mode such that the Recovery Point Objective (RPO) is zero.

2.28. Support encryption for all data at rest by AES-256 bit or above. Encryption keys shall be stored in a secure vault which is separated from the data.

3. High-level Functional Requirements of SIEM module

Basic Functions

3.1. Allow receiving and storing logs collected from different types of IT equipment.

3.2. Support and provide log collection software agent for collecting logs on servers.

3.3. Support collecting, analysing and searching logs in English, Traditional Chinese and Simplified Chinese language.

3.4. Support log normalisation to standardise the format of collected logs.

3.5. Support log indexing for speeding up the searching and analysis.

3.6. Support analysing logs collected from different types of IT equipment.

3.7. Support detection on abnormal system behavior or security breach.

3.8. Support log searching and setting up configuration with custom keywords, regular expression (Regex), wildcard or Boolean operator.

3.9. Allow users to define or import new security analytic rules, in addition to the built-in and vendor defined rules to detect new security threats and cater for business needs.

3.10. Provide web user interface (web UI) in English for users to make configuration and log searching.

3.11. Provide dashboard to display the latest and historical security detection and threat trend.

3.12. Support generation of summary report for the discovered security threat.

3.13. Support graphical display for the analysis result on web UI as well as on the report.

3.14. Allow users to export the collected logs or search results into text file or in PDF.

Scalability and Recovery

3.15. Support receiving logs from around 1 500 IT equipment devices in production environment and 600 devices for testing environment.

3.16. Support to store the collected logs for at least one (1) year.

3.17. Set up appropriate system architecture in order to eliminate single point of failure and data loss.

3.18. Support automatic switchover during disaster recovery.

3.19. Support system scale up and out without reinstalling the whole module for the increase in data volume or number of devices for security analysis.

3.20. Support license add-on for the increase in data volume or number of devices for security analysis.

Security

3.21. Support off-internet operation and on-premises deployment.

3.22. Support encryption for the connection to the web UI.

3.23. Support log segmentation based on user, user group or device group.

3.24. Support permission customisation on the user roles.

3.25. Support manually disable alert temporarily.

3.26. Support severity classification to the alert and notification.

3.27. Support detection for the known suspicious internet IP addresses or URLs.

3.28. Allow upgrading or performing vulnerability patch by using pre-downloaded software files.

3.29. Allow updating system security detection database by using pre-downloaded package files.

3.30. Provide audit trail in order to record user activities.

Integration

3.31. Integrate with C&ED Customs Portal (CP) for single-sign on (SSO) to the web user interface of SIEM module.

3.32. Integrate with C&ED user directory and database servers to collect user information for role creation.

3.33. Automatic generate alerts and integrate with C&ED centralised IT systems health monitoring and ticketing system when threat was detected by the module.

3.34. Generate monitoring and statistic reports and integrate with C&ED email system.

3.35. Support sending security notifications through API.

4. High-level Functional Requirements of rCIRS module

4.1. Consist of two sub-modules, namely rCIRS Data Warehouse (rCIRS-DW) and rCIRS Operational Master (rCIRS-OM). The rCIRS-DW facilitates users in timely accessing the structured operational data collected from different systems, whereas the rCIRS-OM facilitates data interchange among different systems of C&ED.

For rCIRS-DW

Web Portal

4.2. Provide a web portal to allow users to access various online functions of rCIRS after authentication. The functions shall be grouped according to the predefined functional areas, namely General Function, Performance Dashboard Enquiry, Statistics Centre Enquiry, Single Search Enquiry, Routine Report Enquiry, Ad-hoc Enquiry, User Data Collection and System Administration.

Performance Dashboard Enquiry

4.3. Consist of a grid of content frames that contain contents selected from the list of accessible online reports. Each user can customise his or her own performance dashboard page.

4.4. Support personalised page content for each dashboard frame that allows users to select a report from the repository of accessible reports to be displayed in the frame. Users can specify the title of the content in English or Chinese and set the desirable heights and width of the content frame. There are around 45 performance dashboard reports required to be developed for users' selection.

Statistics Centre Enquiry

4.5. Provide user function for displaying the list of deliverables produced in a structured manner. There are four (4) groups of reports, namely "Customs Performance and Achievements", "Time-series", "Regular Returns" and "Dynamic Statistics".

4.6. Provide user function for customisation of dimensions and measurements of Dynamic Statistics Reports. By selecting different options in the selection boxes, users can dynamically refresh the statistics reports of different combinations of breakdowns and groupings. Different dimensions and measurements are available for customisation for different subject areas.

4.7. Cover around 401 of reports in the following categories. They will be generated on a daily basis during the daily batch window. Generation of all these reports is required to be completed within four (4) hours from 0200 hrs to 0600 hrs.

No.	Category of Reports	Number of Reports
1	Customs Performance and Achievements Reports	184
2	Time-series Reports	58
3	Regular Returns Reports	148
4	Dynamic Statistics Reports	11

Single Search Enquiry

4.8. Support searching of information on predefined set of fields in different subject areas across multiple sources of data.

4.9. Provide user function for users to define the searching criteria. Users have to provide a "Search Reference Number" as a mandatory field to declare the purpose of the search.

4.10. Support searching strings in English, Traditional Chinese and Simplified Chinese Languages. Automatic language translation is not required.

4.11. Support users to select the "field type" such as the search string, the search data range and the target subject areas to search. One field type can be searched at a time. After selecting a particular filed type, users can select different associated subject areas.

4.12. Support users to refine the search result based on previously submitted searching criteria with additional selection criteria provisioned. To perform the refine search, users select the new "field type" such as the search string, the search data range and the target subject areas to search. Users can keep on refining the search result by invoking this function until reaching the pre-defined limit.

4.13. Support submitting a search request to rCIRS-DW so that the request shall be handled by one of the processing threads of the thread pool based on pre-defined scheduling logics.

4.14. Provide user function to display a list of search requests previously submitted by a user and show the processing status.

4.15. Display the searching result as a summary list showing the number of records matched with the given search string in respective subject area. The list also provides links for downloading the matched records in CSV format.

Routine Report Enquiry

4.16. Provide users function for displaying the list of Formation's pre-defined routine enquiry reports in this report repository. List of reports in the repository is dynamically adjusted with respect to the right granted to the users.

4.17. Support users to save a bookmark link of an online report to the Personal Repository so to shorten the time to search a frequently used report.

4.18. Develop around 302 predefined routine reports based on the logics given by different users. The reports can be generated on an ad-hoc basis and users can adjust the filtering conditions to refine the expected result of the report.

Ad-hoc Enquiry

4.19. Leverage off-the-shelf Business Intelligence (BI) software to develop predefined data models to facilitate users in conducting ad-hoc inquiries of the data.

4.20. Support row-level data access control for some data models such that users can only retrieve those data being granted with proper access.

4.21. Support users to refine, including but not limited to the filtering criteria, sorting sequence, visualisation effect and output format of the enquiry result.

4.22. Support saving the user-defined enquiry template for future use and the BI software shall also allow users to schedule the enquiry template to be executed according to user preference.

4.23. Support users to retrieve, modify and run their user-defined enquiry templates whenever necessary. The templates, developed by users, are usually for retrieving related data in the form of record list based on simple selection criteria.

4.24. Pre-define around 140 data models to facilitate users, granted with proper access right, to conduct ad-hoc enquiry of the data through the BI software. Most of the data models are straightforwardly mapped to corresponding views in the database.

4.25. Maintain around 210 user-defined enquiry templates in the personal folders of different users. Most of the enquiries are extracting the interested fields from the pre-defined data models with simple filtering conditions defined and the result are usually presented in a table list format.

User Data Collection

4.26. Provide user function for downloading the administrative data input form template of respective formations in Excel format. Each formation is customised with its own template of administrative data input form which is generated by batch program on a monthly basis.

The function only allows users to download respective formation template for offline update using Excel software.

4.27. Allow users to update the required data of respective formation into the administrative data input using Excel software.

4.28. Provide user function for uploading the input forms. After the form is uploaded to the rCIRS-DW, the function retrieves the data from the worksheet and validate the data according to the validation result embedded in Excel file. In case of any irregularity, the interface displays the list of errors found in the input form, and users have to rectify and re-upload the input form.

4.29. Provide function to scan through the status of administrative data input form submissions and automatically generate and send reminder emails to target recipients if they have not uploaded respective forms. Specific user function is provided for users to view the submission status of administrative data input forms of each formation.

4.30. Update the monthly statistics datasets by integrating the data of current month and previous month.

4.31. Generate a full set of Customs Performance and Achievements (CPA) reports, Directorates Reports (Operational Statistics and Enforcement Results), Time Series reports and Regular Return reports in PDF or Excel format according to the existing report generation schedule.

System Administration of rCIRS-DW

4.32. Grant user access rights to the system functions and access rights at function level and role level.

4.33. View the activity logs maintained by rCIRS-DW through online reports. Through this function, log files can be downloaded to support audit and review purposes.

4.34. Maintain up-to-date code tables used by rCIRS-DW by a generic function where the addition of a new code table does not require writing a new program. Instead, it can simply be done by adding configuration data of the new code table to the database.

System Interfaces

4.35. Leverage different technologies including, but not limited to Extract, Transform, and Load (ETL), Secure File Transfer Protocol (SFTP) and Web services, to facilitate data to be collected from and forwarded to different systems under different usage scenarios.

4.36. Support different usage scenarios as listed below.

No.	Technology	No. of Systems	No. of Interfaces	Interface Frequency
ETL - Data Collected from Source System				
1.	MS SQL Server	5	1 279	Daily
2.	Oracle	7	552	Minute or daily
ETL - Data Forwarded to Target System				
3.	MS SQL Server	2	41	Minute or daily
4.	Oracle	1	28	Minute or daily or monthly
Web Services - Data Forwarded to Target System				
5.	SOAP and Java	1	17	Ad-hoc
SFTP Services - Data Collected from Source System				
6.	CSV over SFTP	2	63	Weekly or monthly
7.	XML over SFTP	2	124	Daily
SFTP Services - Data Forwarded to Target System				
8.	CSV over SFTP	1	17	Monthly

Batch Functions

4.37. Develop batch jobs for different purposes, including but not limited to support online functions as listed below.

No.	Category	No. of Jobs	Jobs Frequency
1.	System Monitoring and Maintenance	4	Hourly or daily
2.	System Administration	8	Hourly or daily
3.	Statistics Centre Enquiry	15	Daily
4.	Routine Report Enquiry	11	Daily
5.	Single Search Enquiry	2	Minute
6.	Miscellaneous	5	Daily

For rCIRS-OM

4.38. Leverage different technologies, including but not limited to ETL and SFTP services, to facilitate data to be collected from and forwarded to different systems of C&ED.

4.39. Facilitate interfaces directly from and to the database of source and target systems without generation of temporary interface files.

4.40. Facilitate interfaces which involve file transfer amongst systems.

4.41. Facilitate interfaces frequency, including but not limited to on a minute, daily or monthly basis.

4.42. Support data collection from the following types of source systems to rCIRS-OM.

No.	**Source System Technology**	**No. of Systems**	**No. of Interfaces**	**Interface Frequency**
1.	MS SQL Server over ETL	9	80	Minute or hourly or daily or weekly
2.	Oracle over ETL	7	72	Minute or hourly or daily or weekly
3.	XML over SFTP	1	1	Minute

4.43. Support data to be forwarded to target systems from rCIRS-OM.

No.	**Target System Technology**	**No. of Systems**	**No. of Interfaces**	**Interface Frequency**
1.	DB2 over ETL	1	1	Minute
2.	MS SQL Server over ETL	15	121	Minute or hourly or daily or weekly or monthly
3.	Oracle over ETL	7	79	Minute or hourly or daily
4.	PostgreSQL over ETL	1	1	Minute

4.44. Support transformations, including but not limited to data type conversions, string manipulations, simple calculations, lookup and replace operations, aggregations, matching and character-encoding conversion.

4.45. Support the processing of transformation logics via computing resources other than the source and target databases such that the required processing power from the source and target systems could be offloaded.

4.46. Facilitate impact analysis of metadata to indicate the relationships amongst objects, including but not limited to columns and tables to be presented in the form of data lineage in a tabular and graphical form.

5. High-level Functional Requirements of CBDAS module

5.1. The objectives of CBDAS are as follows -

- provide data extraction tools, system interfaces and web scrapping functions to collect data from various sources;
- serve as the data warehouse and data lake for both structured and unstructured data in standardised data format;
- provide tools and functions to support pre-processing of the data;
- provide data management tools and functions to construct data assets, and provide administration functions to support data management and governance;
- provide a workspace to deploy machine learning and artificial intelligence (AI) models, provide a centralised repository for storage and sharing of the source codes of analytics models, and implement API and system interfaces to facilitate deployment of analytics models in other systems; and
- provide visualisation tools to present analysis results.

CBDAS Portal

5.2. Provide a one-stop web portal to users for all integrated services which provides the following tools on top of CIP -

- tools to be used throughout the data lifecycle (e.g. data pre-processing tools, data analytic tools, data visualisation tools, etc.);
- enterprise tools (e.g. AI workspace, code and image repository, etc.); and
- data lake tools (e.g. object storage).

Data Collection and Import

5.3. Allow users to create web crawler requests to collect information from websites, including social media platforms, online marketplaces, forums, other customs websites and news websites.

5.4. Allow users to upload textual or non-textual files (image, audio and video) to the CBDAS's data lake.

5.5. Receive row-based data from rCIRS-DW.

Data Pre-Processing

5.6. Perform Optical Character Recognition (OCR) to extract textual data, such as bank transactions and call detail records, with satisfactory accuracy.

5.7. Convert row-based data into graph-based data according to the list of entities, including but not limited to company, person, vehicle and consignment.

5.8. Perform pre-processing on image, audio and video, such as data cleansing, data augmentation and data annotation.

5.9. Transform speech into textual data with satisfactory accuracy.

5.10. Allow users to perform data ETL.

Data Storage

5.11. Maintain the CBDAS's data lake consisted of row-based database, online analytical processing (OLAP)-type database, graph-based database, key-value database, document-based or tree-based database and object storage, to store both structured and unstructured data.

Data Analytics

5.12. Perform image and video analytics, including image comparison, object detection (e.g. facials and vehicles) and action detection.

5.13. Generate the list of accounts participated and their interactions during Facebook or Instagram live videos, including their user ID and name, activities (e.g. join live, leave comment, give like, leave live, etc.).

5.14. Perform keyword extraction and Named Entity Recognisation (NER) from free text.

5.15. Perform pattern and conveyance analytics on trading and vehicle crossing records.

5.16. Perform relationship analytics on person, company, vehicle and consignment. Navigate the networks and perform path detection.

Data Searching

5.17. Perform full-text search and image search across data sets within the CBDAS's data lake.

Data Visualisation

5.18. Allow users to create different types of charts, reports and dashboards by simple drag and drop.

Model Training

5.19. Provide Jupyter Notebook with variety of tools and libraries installed as a web-based workspace. Allow technical staff to conduct advanced model training or retrain existing models, then export and deploy the trained models to the corresponding operation systems for future use.

5.20. Allow users to develop code free models for classical machine learning, image recognition, and face recognition by simple drag and drop following the machine learning pipeline.

System Administration

5.21. Synchronise user and posting information with CBDAS user profile.

5.22. Allow system administrators to maintain access rights, application parameters and system codes.

5.23. Record all user activities and system activities to audit log files.

5.24. Produce common administration and management reports and statistics for system administrators.

System Interface

5.25. Integrate with C&ED CP for SSO to the web user interface of CBDAS module.

5.26. Integrate with OGCIO's Big Data Analytics Platform (BDAP) to allow users to search images and capture live broadcast video clips from various media sources.

Migration of the Existing Pilot Systems

5.27. Transform, migrate and consolidate the data and functions of the existing four (4) pilot systems.

i) System A – Performs pattern analytics and data visualisation on cargo and vehicle data. Dashboards, relationship graph, full-text search and model training are included.

ii) System B – Uses artificial intelligence technologies with big data analytics in intelligence processing, case investigation and crime detection. Web crawling, dashboards and relationship graph are included.

iii) System C – Screens data on selected social media platforms (including Facebook and

Instagram) and conducts in-depth investigations on high risk message threads. Web crawling is included. Selected components would be incorporated by means of virtual machine (VM).

iv) System D – Allows cross-platform cyber patrol, gathers and compares information on different popular online platforms for analysing and identifying prevailing and emerging trends, and traces possible sources of the perpetrators. Web crawling, dashboards, relationship graph and image search are included.

5.28. Based on the Feasibility Study of CBDAS, there are around 100 functions to be implemented for the above functional requirements for CBDAS.

- End of Appendix 1 -

Required Facilities for the System

1. Hardware and Software Requirement

1.1. The SCITI comprising four (4) modules (the System) shall be set up mainly in two (2) data centres, (i.e. C&ED Primary Data Centre (CED-PDC) and C&ED Secondary Data Centre (CED-SDC)), and comprises at least three (3) system environments -

- primary production environment (PROD-1), say at CED-SDC or data centre(s) for System Hosting Services ("Outsourced Data Centres") (if applicable);
- secondary production environment (PROD-2), say at CED-PDC or Outsourced Data Centres (if applicable); and
- development and testing environment (Testing Environment), say at CED-PDC, CED-SDC or Outsourced Data Centres (if applicable).

1.2. The following sections are provided for reference only. Tables 1.1 and 1.2 below list out the hardware and software for setting up the CIP (which provides cloud service as Type-2 Satellite Site of Government Cloud Infrastructure Services (GCIS) (https://www.ogcio.gov.hk/en/our_work/infrastructure/e_government/gcis/index.html)), SIEM, rCIRS and CBDAS modules. Section 2 of this Appendix lists out the communication lines for the data centres. Section 3 lists out the System Hosting Services involved.

1.3. Suppliers shall base on the requirements provided in this market research document to propose necessary hardware and software to implement the System.

1.4. The System shall comprise at least the following hardware components. The minimum quantity with unit requirements for each individual item are given below.

Table 1.1 Hardware for all system environments.

Item	**Major Hardware Components**	**Environment**			**Unit**
		PROD-1	**PROD-2**	**Testing Environment**	
1	**Server**				
1.1	Servers for management workload group (at least 2x16 cores CPUs, 256 GB memory)	To be proposed by suppliers			Unit
1.2	Servers for tenants' workload group (at least 2x32 cores CPUs, 1 024 GB memory)	29	15	5	Unit

Item	Major Hardware Components	Environment			Unit
		PROD-1	PROD-2	Testing Environment	
1.3	Database-as-a-Service (DBaaS) Hardware	1	1	1	Set
	(a) Number of servers(at least 2x24 cores CPUs, 1 024 GB memory)	4	4	2	Unit
	(b) Total usable storage capacity to be provided by DBaaS	11	11	3	TB
1.4	Database Servers for rCIRS (at least 2x24 cores CPUs, 512 GB memory)	9	3	3	Unit
	(a) Total usable storage capacity to be provided by database servers for rCIRS	160	10	6.4	TB
1.5	Servers for CBDAS				
1.5.1	(a) GPU servers for model training (at least 2x32 cores CPUs, 1 024 GB memory)	3	-	2	Unit
	(b) GPU cards for model training [note 1]	24	-	16	Card
1.5.2	(a) GPU servers for model inference (at least 2x32 cores CPUs, 1 024 GB memory) ● AI model inference ● Entry-level model inference	4	-	1	Unit
	(b) GPU cards for model inference [note 2] ● AI model inference	24	-	6	Card
	(c) GPU cards for model inference [note 3] ● Entry-level model inference	8	-	2	Card
1.5.3	CPU servers (at least 2x32 cores CPUs, 1 024 GB memory)	18	-	18	Unit
	(a) Total usable storage capacity to be provided by CPU servers for data lake	510	-	10	TB
1.5.4	(a) GPU servers for Large Language Model (LLM) (at least 2x32 cores CPUs, 1 024 GB memory) [note 4]	1	-	-	Unit
	(b) GPU cards for LLM [note 4]	8	-	-	Card

Item	Major Hardware Components	Environment			Unit
		PROD-1	PROD-2	Testing Environment	
2	**Storage**				
2.1	Software Defined Storage System	1	1	1	Set
	(a) Total usable block storage capacity to be provided by each Software Defined Storage System	1 548	446	241	TB
	(b) Total usable object storage capacity to be provided by each Software Defined Storage System	600	100	95	TB
2.2	Hardware Security Module (HSM) with Key Management Service (KMS)	2	2	2	Unit
3	**Network Equipment**				
3.1.	Spine switches	2	2	2	Unit
3.2	Leaf switches	To be proposed by suppliers			Unit
3.3	Global Site Load Balancers (GSLB)	2	2	2	Unit
3.4	Edge Router (for CIP)	2	2	2	Unit
3.5	Edge Router (for existing C&ED network)	2	2	2	Unit
3.6	External Firewalls	2	2	1	Unit
3.7	Out-of-band Network-based Intrusion Detection and Prevention System (IDPS)	2	2	1	Unit
3.8	Software Defined Network (SDN) Controller	2	2	2	Unit
3.9	Inter-site Connection between Data Centres	4	4	-	Unit

Item	Major Hardware Components	Environment			Unit
		PROD-1	PROD-2	Testing Environment	
4	**Centralised Backup and Restore Solution**				
4.1	Centralised Backup and Restore Solution	1	1	1	Set
	(a) Total usable storage capacity to be provided by backup and restore solution	4 332	4 332	655	TB
5	**Others**				
5.1	Computer Racks (with Automatic Transfer Switch (ATS) for 13A sockets and PDU for 32A sockets)	To be proposed by suppliers			Unit
5.2	IP-KVM	2	1	1	Unit

Notes:

(1) For model training, suppliers shall propose both Scenario 1 and 2 to fulfil the accumulated GPU computing power requirements below if applicable and indicate clearly in Appendix 3.

Description	PROD-1	PROD-2	Testing Environment
GPU computing power (FP16 Tensor Core) (TFLOPS)	36 000	N/A	24 000

Scenario 1

Each GPU card shall deliver at least 1 500 TFLOPS (FP16 Tensor Core).

Scenario 2

Each GPU card shall deliver at least 160 TFLOPS (FP16 Tensor Core).

(2) For AI model inference, suppliers shall propose both Scenario 1 and 2 to fulfil the accumulated GPU computing power requirements below if applicable and indicate clearly in Appendix 3.

Description	PROD-1	PROD-2	Testing Environment
GPU computing power (FP16 Tensor Core) (TFLOPS)	36 000	N/A	9 000

Scenario 1

Each GPU card shall deliver at least 1 500 TFLOPS (FP16 Tensor Core).

Scenario 2

Each GPU card shall deliver at least 160 TFLOPS (FP16 Tensor Core).

(3) For entry-level model inference, suppliers shall propose both Scenario 1 and 2 to fulfil the accumulated GPU computing power requirements below if applicable and indicate clearly in Appendix 3.

Description	PROD-1	PROD-2	Testing Environment
GPU computing power (FP16 Tensor Core) (TFLOPS)	12 000	N/A	3 000

Scenario 1

Each GPU card shall deliver at least 1 500 TFLOPS (FP16 Tensor Core).

Scenario 2

Each GPU card shall deliver at least 18 TFLOPS (FP16 Tensor Core).

(4) For LLM, each GPU card shall deliver at least 1 500 TFLOPS (FP16 Tensor Core) to fulfil the accumulated GPU computing power requirements below.

Description	PROD-1	PROD-2	Testing Environment
GPU computing power (FP16 Tensor Core) (TFLOPS)	12 000	N/A	N/A

1.5. The System shall comprise at least the following software components. The requirements and minimum quantity for each individual unit or set are given below.

Table 1.2 Software for all system environments

Item	Major Software Components	Environment			Unit
		PROD-1	PROD-2	Testing Environment	
1	**Virtualisation Software**				
1.1	Hypervisor	To be proposed by suppliers			Set
1.2	Virtualisation Infrastructure Manager (VIM) and Orchestration	To be proposed by suppliers			Set
1.3	Database-as-a-Service (DBaaS) Software	To be proposed by suppliers			Set
1.4	Container Orchestration Software (Each server has 2 CPUs, with 32 cores per CPU)	2	2	1	Server
1.5	DR Automation and Orchestration Software	To be proposed by suppliers			Set
2	**Operating System**				
2.1	Red Hat Enterprise Linux for Virtual Datacenters (each server has 2 CPUs, with 32 cores per CPU)	2	2	2	Server
2.2	Windows Server Operating System (Datacentre edition) (each server has 2 CPUs, with 32 cores per CPU)	5	5	3	Server

Item	Major Software Components	Environment			Unit
		PROD-1	PROD-2	Testing Environment	
3	**Network Related Software**				
3.1	Software Defined Network Software	To be proposed by suppliers			Set
3.2	Application Delivery Controllers Software	To be proposed by suppliers			Set
3.3	Out-of-band Network-based IDPS Software and related licences	To be proposed by suppliers			Set
4	**Centralised Backup and Restore Solution**				
4.1	Centralised Backup and Restore Solution	To be proposed by suppliers			Set
5	**System Software Related to SIEM**				
5.1	SIEM software	To be proposed by suppliers			Set
6	**Common Application Software Used by rCIRS and CBDAS**				
6.1	Business Intelligence Software	To be proposed by suppliers (PROD-2 not required)			Set
6.2	Data Integration Software	To be proposed by suppliers (PROD-2 not required for CBDAS)			Set

Item	Major Software Components	Environment			Unit
		PROD-1	PROD-2	Testing Environment	
6.3	Web Application Hosting Software	To be proposed by suppliers (PROD-2 not required for CBDAS)			Set
7	**Application Software Related to rCIRS**				
7.1	Data Warehouse Software	To be proposed by suppliers			Set
7.2	Reporting Software	To be proposed by suppliers			Set
8	**Application Software Related to CBDAS**				
8.1	Software for Data Management	To be proposed by suppliers (PROD-2 not required)			Set
8.2	Relational Database Software	To be proposed by suppliers (PROD-2 not required)			Set
8.3	Graph-based Database Software	To be proposed by suppliers (PROD-2 not required)			Set
8.4	Key-value Database Software	To be proposed by suppliers (PROD-2 not required)			Set
8.5	Document-based or Tree-based Database Software	To be proposed by suppliers (PROD-2 not required)			Set
8.6	Object Storage Software	To be proposed by suppliers (PROD-2 not required)			Set
8.7	Big Data Processing Software	To be proposed by suppliers (PROD-2 not required)			Set
8.8	Job Scheduler Server Software	To be proposed by suppliers (PROD-2 not required)			Set

Item	Major Software Components	Environment			Unit
		PROD-1	PROD-2	Testing Environment	
8.9	API Gateway and Management Software	To be proposed by suppliers (PROD-2 not required)			Set
8.10	Optical Character Recognition (OCR) Software	To be proposed by suppliers (PROD-2 not required)			Set
8.11	Web Crawling Software	To be proposed by suppliers (PROD-2 not required)			Set
8.12	Search Engine Software	To be proposed by suppliers (PROD-2 not required)			Set
8.13	Image Analytics Software	To be proposed by suppliers (PROD-2 not required)			Set
8.14	Video Analytics Software	To be proposed by suppliers (PROD-2 not required)			Set
8.15	Automatic Speech Recognition (ASR) Software	To be proposed by suppliers (PROD-2 not required)			Set
8.16	Named Entity Recognition (NER) Software	To be proposed by suppliers (PROD-2 not required)			Set
8.17	Model Training Software with Programing Development Tools	To be proposed by suppliers (PROD-2 not required)			Set
8.18	Model Training Software with Codeless Development Templates	To be proposed by suppliers (PROD-2 not required)			Set
8.19	SFTP Server Software	To be proposed by suppliers (PROD-2 not required)			Set
8.20	Web Server Software	To be proposed by suppliers (PROD-2 not required)			Set

Item	Major Software Components	Environment			Unit
		PROD-1	PROD-2	Testing Environment	
8.21	LLM Software	To be proposed by suppliers (PROD-2 not required)			Set

2. Communication Lines for Inter-site Connection between PROD-1 and PROD-2

2.1. Provide four (4) Wide Area Network (WAN) links with path diversity and from two different legally licenced operators shall be provided for resilience for the inter-site connections between PROD-1 and PROD-2 for data replication and offsite backup traffic.

2.2. Each WAN link shall support at least 10 Gbps bandwidth.

2.3. Each WAN link shall support network encryption such as Media Access Control Security (MACSec) with at least AES-256 encryption.

3. System Hosting Services

3.1. Subject to the need of System Hosting Services for inclusion as scope of work as specified in **Section 2.3.1 of this market research document**, suppliers shall provide the services based on the requirements as stated in below Sections 3.2 to 3.8.

3.2. The Outsourced Data Centres shall be located in Hong Kong and located at least two (2) kilometres away from each other if more than one data centre is needed.

3.3. The Outsourced Data Centres shall provide sufficient area to host at least one system environment and the area can be expanded with at least fifteen percent (15%) additional area for future expansion.

3.4. The hosting area shall be isolated from other area of the Outsourced Data Centres by physical barrier with the implementation of locked server room. Physical access control at entry and exit points of the locked server room shall be managed by C&ED remotely.

3.5. The hosting area shall comply with Level II Security in Guidelines for Security Provisions in Government Office Buildings and relevant physical security requirements stated in the GCAF.

3.6. The Outsourced Data Centres shall have the following facility provision:

- air-conditioning system with backup cooling capacity;

- automatic fire detection and suppression system;

- water detection system;

- emergency power supply system such as dual power supply and uninterruptible power supply (UPS) and diesel generator support;

- remote facilities for physical security monitoring and alert system;

- physical intrusion detection system at the main entrances and all exits; and

- sufficient number of CCTV cameras.

3.7. There shall be at least two (2) WAN links from each data centre of the Outsourced Data Centres to both CED-PDC and CED-SDC. Each WAN link shall support at least 10 Gbps bandwidth.

3.8. If there are equipment in Cloud Arbitrary Site (CAS), two (2) WAN links from each of Outsourced Data Centres to C&ED Disaster Recovery Data Centre (CED-DRDC) shall be provided.

- End of Appendix 2 -