BDlogo

# SYSTEM INSTALLATION PLAN

**FOR**

**COMBINED SYSTEM DEVELOPMENT SERVICES**

**FOR**

**LICENSING SELF-CERTIFICATION PORTAL**

**OF**

**BUILDINGS DEPARTMENT**

**Version: 0.1**

? The Government of the Hong Kong Special Administrative Region

| ------------- | ------------------------------------- | N/A | --- | --- | N/A |
| --- | --- | --- | --- | --- | --- |

# TABLE OF CONTENTS

[2. Project Environment Description](#project-environment-description)

* [2.2 Hardware Specification](#hardware-specification)
* [2.3 Software Specification](#software-specification) [3. Application Deployment Procedure for Production](#X7b7da364f5368a9d1539fc301c43d2c2ac93d8d)
* [3.1 Database Server](#database-server)
* [3.3 Frontend Servers](#frontend-servers)
  + [3.3.1 sFTP Server Setup](#sftp-server-setup) [4. System Installation Schedule and Result](#system-installation-schedule-and-result)
* [4.1 System Installation Schedule](#system-installation-schedule)

# Introduction

The System Installation plan describes the procedure and schedule for deploying the application in the production environment, including 3 parts of the system:

* Backend Server
* Frontend and Web Portal Server

# Project Environment Description

Below is a logical network diagram in 1/F West Kowloon Government Office for production and UAT site. [DIAGRAM HERE]

A two-tier firewall setup will be used to form the trusted zone and DMZ.

## Hardware Specification

List of machines and virtual machines:

| Hostname (Physical Machine) | Hostname (Virtual Machine) | Purpose | IP | N/A |---------------------------|---------------------------|---------|-----| N/A |---|---|---|---| N/A | Machine | Hostname | Software Requirement | N/A |---|---|---| N/A | vCenter Server | prd-scs-vcenter-01 | vCenter 8.0.3 Build 24322831 | N/A |---|---|---| Development Frameworks:

|-----------|---------| N/A |---|---| N/A | React (frontend) | 18.2.0 | N/A |---|---|

# Application Deployment Procedure for Production

## Database Server

1. Remote login to PRD-DB-01
2. Install Microsoft SQL Server Management Studio 19.1
3. Configure SQL Server
4. Configure database backup schedule
5. Configure database maintenance plan
6. Configure database monitoring and alerts

## Frontend Servers

1. Remote login into PRD-WEBAPP-01 and PRD-WEBAPP-02
2. Install prerequisites: IIS, Application Request Routing
3. Install frontend application
4. Configure application settings
5. Configure Windows services
6. Configure SSL certificates
7. Configure IIS
8. Configure monitoring

### sFTP Server Setup

1. Install OpenSSH server
2. Configure OpenSSH server
3. Configure logging and monitoring

# System Installation Schedule and Result

## System Installation Schedule

|---------------|------------|----------|------------|----------| N/A |---|---|---|---|---| N/A | Database Server Installation (Production and DR) | N/A | | N/A | | N/A |---|---|---|---|---| N/A | Frontend Server Installation (Production and DR) | N/A | | N/A | | N/A |---|---|---|---|---| N/A | Functionality test (VM & Networking) | N/A | | N/A | | N/A |---|---|---|---|---| N/A | Deployment for 1st version of frontend server | N/A | | N/A | | N/A |---|---|---|---|---| N/A | Deployment for 1st version of backend server | N/A | | N/A | | N/A |---|---|---|---|---| N/A | Deployment for Latest Mobile Application | N/A | | N/A | | N/A |---|---|---|---|---| N/A | Final Check Production Web Server | N/A | | N/A | | N/A |---|---|---|---|---| N/A | Final Check DR Web & Database server | N/A | | N/A | | N/A |---|---|---|---|---| N/A | Final Check IIS & Framework | N/A | | N/A | | N/A |---|---|---|---|---|

## System Installation Result

| Pre-Requisite | Actual Start Date | Actual End Date | Actual Start time | Actual End Time | Status/Result | N/A |---|---|---|---|---|---| N/A | Database Server Installation (Production, UAT and DR) | N/A | | N/A | | N/A | |---|---|---|---|---|---| N/A | Backend Server Installation (Production, UAT and DR) | N/A | | N/A | | N/A | |---|---|---|---|---|---| N/A | Functionality test (VM & Networking) | N/A | | N/A | | N/A | |---|---|---|---|---|---| N/A | Database setup | N/A | | N/A | | N/A | |---|---|---|---|---|---| N/A | Deployment for 1st version of backend server | N/A | | N/A | | N/A | |---|---|---|---|---|---| N/A | Application Health Check | N/A | | N/A | | N/A | |---|---|---|---|---|---| N/A | Final Check Production Web Server | N/A | | N/A | | N/A | |---|---|---|---|---|---| N/A | Final Check Production Database Server | N/A | | N/A | | N/A | |---|---|---|---|---|---| N/A | Final Check IIS & Framework | N/A | | N/A | | N/A | |---|---|---|---|---|---| ```

Okay, I've reviewed the provided documents and will answer your questions based on the BD CDPSS - Prod Installation & Operation Manual (network) v1.0 and the BD - VM & Network Upgrade for CDPSS Site Infra Configuration Information - 20230427\_v0.1 documents.

**1. External Firewall**

* **BD CDPSS - Prod Installation & Operation Manual (network) v1.0 Section 1:** This section should contain the details regarding the external firewall configuration. You will need to consult this section directly for specific information.
* **BD - VM & Network Upgrade for CDPSS Site Infra Configuration Information - 20230427\_v0.1:** Refer to the tabs "Prod - FW port" and "Prod - FW VIP policy" for production environment firewall rules and VIP policies. Also, refer to the "DR - FW port" and "DR - FW VIP policy" tabs for the disaster recovery environment firewall rules and VIP policies. These tabs should specify the ports that need to be opened on the external firewall, the source and destination IP addresses, and the protocols allowed.

**2. Internal Firewall**

* **BD CDPSS - Prod Installation & Operation Manual (network) v1.0 Section 2:** This section should contain the details regarding the internal firewall configuration. You will need to consult this section directly for specific information.
* **BD - VM & Network Upgrade for CDPSS Site Infra Configuration Information - 20230427\_v0.1:** Refer to the tabs "Prod - FW port" and "Prod - FW VIP policy" for production environment firewall rules and VIP policies. Also, refer to the "DR - FW port" and "DR - FW VIP policy" tabs for the disaster recovery environment firewall rules and VIP policies. These tabs should specify the ports that need to be opened on the internal firewall, the source and destination IP addresses, and the protocols allowed.

**3. Windows NLB**

* **BD CDPSS - Prod Installation & Operation Manual (network) v1.0 Section 3:** This section should contain the details regarding the Windows Network Load Balancer (NLB) configuration. You will need to consult this section directly for specific information.

**4. Switches - Prod DMZ Port**

The image provided shows the network diagram for the Prod DMZ switch port configuration. You'll need to examine the diagram to determine the specific VLANs, connected devices, and port configurations.

**5. Switches - Prod INT SW Port**

The image provided shows the network diagram for the Prod Internal switch port configuration. You'll need to examine the diagram to determine the specific VLANs, connected devices, and port configurations.

**6. Switches ? DR DMZ SW Port**

The image provided shows the network diagram for the DR DMZ switch port configuration. You'll need to examine the diagram to determine the specific VLANs, connected devices, and port configurations.

**7. Switches ? DR INT SW Port**

The image provided shows the network diagram for the DR Internal switch port configuration. You'll need to examine the diagram to determine the specific VLANs, connected devices, and port configurations.

**8. Software Inventories**

The provided tables list the software installed on various servers in the Production (WKGO and GCIS P1/P2), UAT (WKGO and GCIS T1), DEV (WKGO and GCIS T1), and DR (AIA) environments. The tables include the machine name, hostname, and the software installed on each. Note that the NAS software is listed as "???" and needs to be filled in.

**9. Security and Backup**

* **System Control:** Authentication mechanisms remain largely unchanged, with OSDP being the primary method for BD staff. External users will continue to use OTP via email. Password complexity will be updated.
* **Backup:** Production, UAT, DEV (WKGO), and DR (AIA) environments are backed up by dedicated backup servers. GCIS P1/P2 environments are backed up by GCIS-provided services. Database servers perform local backups in addition to the VM image backups. Details of backup schedules and retention policies are provided.
* **Security:** The system conforms to BD and DPO security policies. Data transmission is encrypted via HTTPS over TLS. Data storage uses RAID mirroring and encryption. Regular security patching and antivirus updates are performed. Physical security measures are in place for server rooms.
* **Change Control:** GIT repository is used for version control of the LSCP source code.
* **Disaster Recovery:** GCIS uses automatic failover to Prod 2. BDSCS uses NGINX for load balancing and VM replication to the DR environment.
* **Database Backup Strategy:** Full database export backups are performed daily in addition to VM backups. Recovery procedures and downtime estimates are provided for various failure scenarios. A backup schedule is provided.

**10. Database Administration**

* Instructions are provided for cleaning database transaction logs and performing database backups using SQL Server Management Studio (SSMS).

**11. System Constraints and Limitations**

* URL path length limit is 250 characters.
* Specific special characters are not allowed in filenames/folders.

**12. Log Management**

* A list of activities to be included in the logs is provided.
* Logs are retained for 180 days and managed by a Syslog server.
* Logs are reviewed regularly.

**User Requirements Specifications (URS)**

The URS document outlines the user requirements for the Self-Certification System, including:

* **Proposed System Overview:** Description of the system and user profiles.
* **Future Business Processes:** List of processes supported by the system.
* **Functional Requirements:** Detailed list of functional requirements.
* **Non-Functional Requirements:** Requirements related to security, usability, and interfaces.
* **Technical Requirements:** Technical specifications for the system.

**Important Considerations:**

* **Consult the Manuals:** The BD CDPSS - Prod Installation & Operation Manual (network) v1.0 is the primary source of information for the firewall and NLB configurations. You *must* refer to the specific sections mentioned to get the detailed settings.
* **Configuration Information Spreadsheet:** The BD - VM & Network Upgrade for CDPSS Site Infra Configuration Information - 20230427\_v0.1 spreadsheet is critical for understanding the specific port rules and VIP policies for the firewalls.
* **Network Diagrams:** The network diagrams for the switches are essential for understanding the VLAN configurations and device connectivity.

This response provides a summary of the information available in the documents. For specific configuration details, please refer to the sections and tabs mentioned above.

Okay, I've analyzed the provided document and extracted the functional and non-functional requirements. Here's a summary, organized for clarity:

**I. Functional Requirements (REQ-GR, REQ-WR, REQ-FRM, REQ-PRO):**

These define *what* the system should do.

**A. General Requirements (REQ-GR):**

* **REQ-GR-01 to REQ-GR-06:** User Registration, Login, iAM Smart Login, Change Password, Forget Password, Logout. *Status: Not Applicable* (Applicant will use reference number and OTP instead).
* **REQ-GR-07:** Single Sign On (SSO) for BD, EDB, and SWD users via their respective OSDP portals. *Priority: High*
* **REQ-GR-08:** Preview Document (PDF, JPEG, PNG, TIFF). *Priority: High*
* **REQ-GR-09:** Print Document (Application form, Layout Plans, Acknowledgment email, Proforma, Inspection Report, Letter of Requirement, Reply Letter, e-Certificates/ Certificates and e-Notice/Notice/Schedule of PTS for TPPE, Others (i.e. S.J. Report, APP-13), Register of PTS for TPPE). *Priority: High*
* **REQ-GR-10:** Upload Document (Layout plans, supporting documents). Virus scanning required. PDF (flattened, digitally signed, <= 25MB each), total files <= 100MB. Configurable maximum size. *Priority: High*
* **REQ-GR-11:** Management Statistics and Reports (Total Received Cases, Total Replied Cases, Total Outstanding Cases, Total Overdue Cases, Total Audit Cases and corresponding results, Total applications through e-submission and paper submission, Total opted and Non-opt cases, Total accepted and rejected PTS cases, Outstanding cases with reminder, Performance report). *Priority: High*
* **REQ-GR-12:** e-submission (Mobile-friendliness, Field validations, Cross-field validations, Conditional display, Form pre-filling function using iAM Smart, or with other government backend systems where applicable, Single and multiple digital signatures using iAM Smart, Single and multiple digital signatures using digital certificates issued by recognised certification authorities in Hong Kong, Saving of filled-in forms for later completion e.g. multiple digital signatures, provide Photo compression option for system administrator, Form Version control and duplicate submission checking, Submission of attachment file(s) ( photo, form, plan, and according to PNAD of BD ), with size control and digital signatures, Creation of PDF form template and generation of PDF file with data submitted by public users incorporated, serving as a record of the submitted data, for reference by the submission party and users; send application number to user via email and sms, Preparation of an Excel template, if needed, for each of the form to facilitate users to extract form data to Excel for processing and analysis. Technical know-how on producing the template file will be provided at the start of the assignment, Form data encryption, Save draft application in GCIS for two weeks). *Priority: High*
* **REQ-GR-13:** e-processing (Workflow-based processing of applications). *Priority: High*
* **REQ-GR-14:** e-tracking (Tracking of application status). *Priority: High*
* **REQ-GR-15:** Centralized data repository for application supporting documents. *Priority: High*
* **REQ-GR-16:** Search and Capture (See REQ-WF-17). *Priority: High*
* **REQ-GR-17:** Handle new applications (EP/CCC). *Priority: High*
* **REQ-GR-18:** Handle alteration applications (EP/CCC). *Priority: High*
* **REQ-GR-19:** Handle Self Certification Submissions. *Priority: High*
* **REQ-GR-20:** Handle Periodic Inspection for CCC. *Priority: High*
* **REQ-GR-21:** Handle PTS for TPPE. *Priority: High*
* **REQ-GR-22:** Data repository (Centralized storage in Database and File System). *Priority: High*
* **REQ-GR-23:** Easy retrieval of records (Search function - see REQ-WR-17). *Priority: High*
* **REQ-GR-24:** User and Delegation Administration (Delegate tasks to other users for a period). *Priority: High*
* **REQ-GR-25:** Generate Application Number (YYYY(12 or 13)NNNN). *Priority: High*
* **REQ-GR-26:** Withdraw Application (Allow applicant to withdraw). *Priority: High*

**B. Workflow Requirements (REQ-WR):**

* **REQ-WR-01:** Input Application Data (Registry). Structural address with autocomplete function shall be provided, including on Tradional Chinese and English. *Priority: High*
* **REQ-WR-02:** Create Structural Information Report (TO). *Priority: High*
* **REQ-WR-03:** Provide Comment via SSE (SE). *Priority: High*
* **REQ-WR-04:** Perform Site Inspection (SO). Record Site Inspection, retrieve approved plans from BRAVO and prepare / generate inspection report. The Site Inspection data should include: Date of Site Inspection, Site photo, Others. Also, the system allows SO to draw annotation on PDF file of Layout Plan and upload site photos. *Priority: High*
* **REQ-WR-05:** Building Safety Requirements Check (BS) using 3-tier BSR System. *Priority: High*
* **REQ-WR-06:** Generate Reply Letter, e-Certificates and e-Notice (BS/SBS). Digitally signed by BD officer. *Priority: High*
* **REQ-WR-07:** Generate Letter of Requirement (LoR) (BS/SBS). *Priority: High*
* **REQ-WR-08:** Endorse Application (SBS). *Priority: High*
* **REQ-WR-09:** Endorse Objection (CBS). *Priority: High*
* **REQ-WR-10:** AP/RSE Verification (Registry). Verify identity against MWMS 2.0 (User Name, Registration Number, Registration Status, HKID, Expiry Date, Hand writing signature (for paper application)). Data synchronized daily from MWMS 2.0. *Priority: High*
* **REQ-WR-11:** Check Essential Documents (SO/BS). *Priority: High*
* **REQ-WR-12:** Digital Signing of document (Applicant/AP/RSE/ BD Users). Hong Kong Post e-cert or iAM Smart+. Reply Letter, e-Certificates and e-Notices will be digitally signed using BD certificate. *Priority: High*
* **REQ-WR-13:** Random Audit Check (BD Users). 60% probability (configurable). *Priority: High*
* **REQ-WR-14:** Outstanding Application Alert (SO/TO/BS/SE/SSE/SBS). Email notification for due/overdue/outstanding applications and audit cases. *Priority: High*
* **REQ-WR-15:** Input Application Form (Applicant). Submit application form, layout plans and other documents for application of new/ alteration of EP and CCC. The submitted documents will be digitally signed by Hong Kong Post e-Cert or iAM Smart app. Once the application form is submitted, the system will trigger a new workflow for internal BD users to handle the application. *Priority: High*
* **REQ-WR-16:** Input memo data (EDB/SWD). BD/EDB/SWD users can submit memo data including uploading documents in SCS. *Priority: High*
* **REQ-WR-17:** Search Case Information (BD Users). BD/SWD/EDB users can search all case information including uploaded documents, BSR status?etc in SCS. *Priority: High*

**C. Form Requirements (REQ-FRM):**

* **REQ-FRM-1:** Verify certificate against the copy from Hong Kong Post and DigiSign. The certificate to sign documents will be verified if the CA is from Hong Kong Post and DigiSign. The other CA certificate will not be accepted. *Priority: High*
* **REQ-FRM-2:** Route form to corresponding user. In the workflow, the case will be routed to delegated person base on user mapping from BCIS. *Priority: High*
* **REQ-FRM-3:** Encrypt restricted data in the form. The system will encrypted classified data before storing in database and handle up to Restricted Information. *Priority: High*
* **REQ-FRM-4:** Submit public form via online. Please refer to REQ-WR-15. *Priority: High*
* **REQ-FRM-5:** Extract data from form. All data of submitted form by applicant/AR/RSE will be saved in database. *Priority: High*
* **REQ-FRM-6:** Store the extracted data in the database. All data of submitted form by applicant/AR/RSE will be saved in database. *Priority: High*
* **REQ-FRM-7:** Search function for all record. Please refer to REQ-WR-16. *Priority: High*
* **REQ-FRM-8:** Auto reply to acknowledge receiving the form. An acknowledge letter will be generated and send to application (for 1st submission only). *Priority: High*
* **REQ-FRM-9:** Maintenance function of the form. In case the form data or layout is change, a Change Request will be made in order to change coding. *Priority: High*
* **REQ-FRM-10:** Resubmit the form data. Applicant can re-submit the revised layout plan or other documents once he receives LoR from BD. *Priority: High*
* **REQ-FRM-11:** Update of the disclaimer of the forms. The disclaimer of the forms can be directly updated in the program file i.e. .aspx. *Priority: High*
* **REQ-FRM-12:** Handle e-form and hardcopy form. The system will handle e-form and hardcopy form submitted by applicant. *Priority: High*

**D. From Processing Requirement (REQ-PRO):**

* **REQ-PRO-1:** Verify CRM certification record. The system will automatically verify AP/RSE information against CRM record. However, if paper application, BD user i.e. Registry is required to manually verify the handwriting signature and other data of AP/RSE. *Priority: High*
* **REQ-PRO-2:** Reassign case to other officer. The assigned task can be re-assigned to another person in ad-hoc by system administrator. *Priority: High*
* **REQ-PRO-3:** Form status query. Please refer to REQ-WR-17. *Priority: High*
* **REQ-PRO-4:** Automatically bring up outstanding cases. Please refer to REQ-WR-14. *Priority: High*
* **REQ-PRO-5:** To-Do List. The system provides a tasks list i.e. to-do list for all BD users to handle the case in the workflow. *Priority: High*
* **REQ-PRO-6:** Case History Summary. Please refer to REQ-WF-17. *Priority: High*
* **REQ-PRO-7:** Mark notes and remark for internal use. The workflow provides comments or notes to BD users to handle the case. *Priority: High*
* **REQ-PRO-8:** Re-direct to BCIS for case checking. There will be a hyperlink to BCIS to see the case information when the case is save in BCIS. *Priority: High*
* **REQ-PRO-9:** Handle upload soft copy. All uploaded documents will be saved in centralised file system. *Priority: High*
* **REQ-PRO-10:** Export outstanding case. Please refer to REQ-GR-11. *Priority: High*
* **REQ-PRO-11:** Handle referral case. Please refer to REQ-WR-16. *Priority: High*

**II. Non-Functional Requirements (REQ-CR, REQ-UR, REQ-SR, REQ-IR):**

These define *how* the system should be.

**A. Communication Requirements (REQ-CR):**

* **REQ-CR-01:** SMS Alert (Acknowledgement of form submission, Notification of LoR issued, Notification of Certificate and Notice issued). *Priority: High*
* **REQ-CR-02:** Email Notification (Acknowledgement of form submission, Notification of LoR issued, Notification of Certificate and Notice issued, Reminder to AP/RSE for o/s audit case). *Priority: High*
* **REQ-CR-03:** Fax Copy of LoR, Certificates, and Notice. *Priority: High*

**B. Webpage Requirements (REQ-UR):**

* **REQ-UR-01:** Common Look & Feel (CLF) of HKSAR government. Responsive web/mobile friendly design. W3C HTML5 standard. Compatible with popular browsers, OS, screen readers. *Priority: High*
* **REQ-UR-02:** W3C WCAG 2.1 Level AA compliance. Code scanning, visual review, assistive technology testing, human testing. *Priority: High*
* **REQ-UR-03:** Privacy Disclaimer (Conform to Personal Data (Privacy) Ordinance). *Priority: High*
* **REQ-UR-04:** Assistive Technology Testing (Screen readers, screen magnifiers, voice controls). *Priority: High*

**C. Security Requirements (REQ-SR):**

* **REQ-SR-01:** Security Risk Assessment Audit (SRAA). Address all security issues. *Priority: High*
* **REQ-SR-02:** Privacy Impact Assessment (PIA) and Privacy Compliance Audit (PCA). Address all privacy issues. *Priority: High*
* **REQ-SR-03:** Encryption and Decryption of Classified Data (HKID, etc.). Strong symmetric encryption (AES 256bit) or Hash function (SHA-256). *Priority: High*
* **REQ-SR-04:** System Audit (Log important events). *Priority: High*
* **REQ-SR-05:** System Control. *Priority: High*

**D. Interface Requirements (REQ-IR):**

* **REQ-IR-01:** Interface with BCIS. *Priority: High*
* **REQ-IR-02:** Interface with BD Website. *Priority: High*
* **REQ-IR-03:** Interface with Minor Works. *Priority: High*
* **REQ-IR-04:** Interface with ESH. *Priority: High*
* **REQ-IR-05:** Interface with ERKS. *Priority: High*
* **REQ-IR-06:** Interface with BRAVO. *Priority: High*

**III. Constraints:**

* Complexity of Address Identification
* Signature of AP/RSE

**Key Observations and Considerations:**

* **High Priority:** Almost all requirements are marked as "High" priority. This means careful prioritization and potentially phased implementation will be crucial.
* **External Interfaces:** The system relies heavily on interfaces with other government systems (BCIS, BD Website, Minor Works, ESH, ERKS, BRAVO, MWMS 2.0). The success of the project depends on the stability and accessibility of these interfaces.
* **Security and Privacy:** Security and privacy are paramount, given the handling of sensitive data (HKID, classified information). SRAA, PIA, PCA, and strong encryption are essential.
* **Accessibility:** WCAG 2.1 Level AA compliance is a key requirement, ensuring the system is usable by people with disabilities.
* **Workflow Focus:** The system is heavily workflow-driven, requiring careful design and implementation of the various processes.
* **Digital Signatures:** Digital signatures are a core component, using both Hong Kong Post e-certs and iAM Smart.
* **e-Submission:** The e-submission requirement is very detailed, outlining many specific features.

This detailed breakdown should be helpful for planning, development, and testing of the Self-Certification System (SCS). Let me know if you have any other questions.

# System Installation Plan - SCS (Simplified Case System)

This document outlines the system installation plan for the Simplified Case System (SCS), covering functional and technical requirements, constraints, and appendices.

## 1. Introduction

This document details the requirements and constraints for the installation of the SCS system. The SCS aims to streamline case management and improve efficiency through integration with various internal and external systems.

## 2. Functional Requirements

The SCS system must fulfill the following functional requirements:

### 2.1. REQ-SR-05 System Control

* **Priority:** High
* **Description:** Security control to access the system will be guarded using tools such as Firewall, network control, physical access control, etc.
* **Frequency of Use:** Ad-hoc

### 2.2. Interface Requirements

* **Priority:** High
  + **REQ-IR-01 Interface with BCIS (Building Control Information System)**
    - **Description:** Provide interfaces with BCIS to complete certain tasks, including:
      1. Receiving master data from BCIS for case creation.
      2. Sending application data to BCIS for case creation (batch, to be confirmed).
      3. Updating application data in BCIS.
      4. Providing a reference link between SCS and BCIS.
      5. Transferring data from SCS to BCIS for statistical reports.
      6. Selecting blocks for new address creation in BCIS via to-do-list and email.
      7. Handling 12 and 13 file Licensing cases in SCS instead of BCIS.
      8. Mapping BCIS users (username, post, file reference, DP login ID, case officer).
      9. Including Licensing nature Enquire.
      10. Linking to DV tables of BCIS.
      11. Conducting a detailed study for easy retrieval of records from SCS by comparing data storage against a reference link from the two systems of SCS and BCIS, and determine a solution most suited to user requirements.
    - **Frequency of Use:** Ad-hoc
  + **REQ-IR-02 Interface with BD Website**
    - **Description:** Display a list of Pre-accepted Proprietary Temporary structure data on the BD website.
    - **Frequency of Use:** Ad-hoc
  + **REQ-IR-03 Interface with Minor Works (MWMS 2.0)**
    - **Description:** Provide sFTP upload account to MWMS 2.0 to collect AP/RSE data (User Name, Registration Number, HKID, Expiry Date, etc.) daily. SCS will set up an sFTP server to receive AP/RSE data and update the database accordingly. The SCS system can use Departmental Portal link to redirect to CRM of MWMS to view the detail AP/RSE information as same as ESH.
    - **Frequency of Use:** Ad-hoc
  + **REQ-IR-04 Interface with ESH**
    - **Description:** Provide case information and hyperlinks from SCS to ESH to view related case information and redirect to SCS, respectively.
    - **Frequency of Use:** Ad-hoc
  + **REQ-IR-05 Interface with ERKS**
    - **Description:** Import e-Certificates, e-notices, reply letters, and other documents into the ERKS system for record keeping. Detailed interface specification and implementation will be done in the SM&S stage.
    - **Frequency of Use:** Ad-hoc
  + **REQ-IR-06 Interface with BRAVO**
    - **Description:** Provide redirection to BRAVO via URL: <https://dp2.bd.hksarg/bravo/intranetSignOn>. Also, the SCS system could be redirected to BRAVO through a URL call with specified parameters.
    - **URL Syntax:** <Departmental Portal URL>/bravo/BuildingSearchRedirection?
    - **Parameters:**
      * CASE\_NUMBER=<CASE\_NUMBER>&YEAR=<YEAR>
      * BLOCK\_ID=<BLOCK\_ID>
      * SEARCH\_TYPE=<SEARCH\_TYPE>&SUBJECT\_CODE=<SUBJECT\_CODE>&CASE\_NUMBER=<CASE\_NUMBER>&YEAR=<YEAR>&SPECIAL\_CAT=<SPECIAL\_CAT>
    - **Frequency of Use:** Ad-hoc

## 3. Technical Requirements

The SCS system must adhere to the following technical requirements:

| Req. ID | Requirement Name | Target Users | Priority | N/A | :-------- | :------------------------------------- | :----------- | :------- | N/A |---|---|---|---| N/A | REQ-TR-01 | 24x7 Internet and Intranet | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-02 | Integrated Cloud GCIS and On Premises | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-03 | Input Validation | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-04 | Record Relocation from GCIS to On Premises | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-05 | High Availability | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-06 | Monitoring and Alert Generation | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-07 | DR Drill | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-08 | UTF-8, Unicode or HKSCS | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-09 | System Logging | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-10 | High Configurable | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-11 | Backup and Recovery | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-12 | Operation System and Browser Compatibility | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-13 | Review and Update privilege | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-14 | Health Check | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-15 | Encryption on All Communications | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-16 | Version Control for application | System Admin | NA | N/A |---|---|---|---| N/A | REQ-TR-17 | Monthly Usage Statistics and Ad-hoc Statistics | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-18 | Check-in and Check-out | System Admin | NA | N/A |---|---|---|---| N/A | REQ-TR-19 | Language support (EN/TC/SC) | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-20 | System Performance | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-20 | Record relocation | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-21 | Reports and statistics for monitor system performance | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-22 | Ad-hoc and periodic updates on the contents | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-23 | Provide refined Login & Authentication / FULL Audit features | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-24 | Login user account login by user ID & password | BD/SWD/EBD/MC | H | N/A |---|---|---|---| N/A | REQ-TR-25 | Version control of source code | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-26 | System log tracking | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-27 | Scalable system frame design | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-28 | Data exchange with other system securely | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-29 | Security measurement | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-30 | Help check email notification | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-31 | Email notification for all batch jobs | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-32 | Conform to the Interoperability Framework | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-33 | Manage System Parameters | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-34 | Allow System Access by EBD and SWD | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-35 | Independent System (Not depended on other BD system) | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-36 | Logout automatically for inactive for 30 minutes | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-37 | Centralized log Management | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-38 | Handle around 300 user accounts of EDB and SWD for single sign on | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-39 | Paper Less | System Admin | H | N/A |---|---|---|---| N/A | REQ-TR-40 | PDF template and mapping field for letter generation | System Admin | H | N/A |---|---|---|---|

### 3.1. Detailed Technical Requirements

* **REQ-TR-01: 24x7 Internet and Intranet:** The system must be accessible 24/7 via the internet for AP/RSE and via intranet/GNET for BD users, maintaining high availability except during maintenance or exceptional handling.
* **REQ-TR-02: Integrated Cloud GCIS and On Premises:** The system will integrate GCIS in the Cloud and On Premises in BD. Front-end functions for AP/RSE will be in GCIS, while back-end functions for BD users will be on-premises.
* **REQ-TR-03: Input Validation:** All data input must be validated to prevent security attacks (e.g., SQL Injection). CAPTCHA will be implemented for form submission to prevent DDOS attacks.
* **REQ-TR-04: Record Relocation from GCIS to On Premises:** Functionality to relocate records from GCIS to on-premises must be provided.
* **REQ-TR-05: High Availability:** The system should maintain high availability with active-active application servers and DR capability.
* **REQ-TR-06: Monitoring and Alert Generation:** A log server will monitor server health and alert administrators via email in critical situations. Security audit logs will be kept for 12 months. System, Application, equipment will be monitoring and alert email will be triggered if any warning and failure.
* **REQ-TR-07: DR Drill:** DR drill tests will be conducted to test disaster recovery procedures. RTO is 1 day.
* **REQ-TR-08: UTF-8, Unicode or HKSCS:** The system must support UTF-8, Unicode, or ISO10646 Standard and Hong Kong Supplementary Character Set (HKSCS) coded in ISO10646.
* **REQ-TR-09: System Logging:** The system must record and track all functions, tasks, processes, and user actions. System logs, user activity logs, and transaction logs should be produced and kept for at least 12 months and achieve all logs.
* **REQ-TR-10: High Configurable:** The system should be highly configurable in coding, avoiding hard coding as much as possible.
* **REQ-TR-11: Backup and Recovery:** Periodic backups to external storage devices are required:
  + Incremental backup daily.
  + Full backup weekly.
  + Full backups kept for 6 months.
  + Archive outdated information, when required but no more than twice per year.
* **REQ-TR-12: Operation System and Browser Compatibility:** The system must support the following OS/Browser combinations:
* | Operating System / Browser | Microsoft Windows 8.1 | Microsoft Windows 10 and 11 | Mac OS X | Linux | iOS | Android | N/A |---|---|---|---|---|---|---| N/A | :------------------------- | :-------------------- | :-------------------------- | :------- | :---- | :-- | :------ | N/A |---|---|---|---|---|---|---| N/A | Microsoft Edge | Not applicable | Yes | Not applicable | Not applicable | Not applicable | Not applicable | N/A |---|---|---|---|---|---|---| N/A | Safari | Not applicable | Not applicable | Yes | Not applicable | Yes | Not applicable | N/A |---|---|---|---|---|---|---| N/A | Mozilla Firefox | Yes | Yes | Yes | Yes | Yes | Yes | N/A |---|---|---|---|---|---|---| N/A | Google Chrome | Yes | Yes | Yes | Yes | Yes | Yes | N/A |---|---|---|---|---|---|---|
* **REQ-TR-13: Review and Update Privilege:** Functionality to review and update user privileges must be provided.
* **REQ-TR-14: Health Check:** The system must provide a health check function for regular system monitoring.
* **REQ-TR-15: Encryption on All Communications:** Communication and data transfer between client and server or server to server will be encrypted using HTTPS.
* **REQ-TR-16: Version Control for application:** Programming versioning shall be maintained.
* **REQ-TR-17: Monthly Usage Statistics and Ad-hoc Statistics:**
  1. Allow data administrator to run ?Select? SQL statement through the application website. Results shall be exportable as CSV excel file. (e.g. No contain HKID )
  2. Appendix 4 - Utilisation Survey
  3. Active and Inactive User Account Report by selection date and time
* **REQ-TR-18: Check-in and Check-out:** The system shall able to check-in or check-out documents in order to prevent duplicate update on same document.
* **REQ-TR-19: Language Support (EN/TC/SC):** The system shall provide web page in 3 languages that is English, Traditional Chinese and Simplified Chinese for users to choose.
* **REQ-TR-20: System Performance:** The system performance will be periodically monitored in order to dig out any performance bottleneck
* **REQ-TR-21: Reports and statistics for monitor system performance:** The reports and statistics of system performance can be generated using system monitoring tool.
* **REQ-TR-22: Ad-hoc and periodic updates on the contents:** The system allows authorized BD users to edit the case information. Develop an automatic function to delete the records by customization
* **REQ-TR-23: Provide refined Login & Authentication / FULL Audit features:** The Login information will be record in audit and stored in database.
* **REQ-TR-24: Login user account login by user ID and password:** In case the OSDP is malfunctioned, the system provide another interface for BD/EDB/SWD users to login the system using username and password.
* **REQ-TR-25: Version control of source code:** The source code of the system will be kept in Version Control System and providing versioning support.
* **REQ-TR-26: System log tracking:** The system provides logging to file for all functions and events.
* **REQ-TR-27: Scalable system frame design:** The system provides High Availability (HA) in the system design so that to minimize single point of failure. Also, it can increase the HA by adding extra nodes whenever it needs.
* **REQ-TR-28: Data exchange with other system securely:** The system will connect other system using secure method such as HTTPS if it is applicable.
* **REQ-TR-29: Security measurement:** The system will be designed with security in first priority and security control will be added in different layers such as application, network, database?etc.
* **REQ-TR-30: Help check email notification:** The system will send email notification using internal BD email server and external GCIS email server. The email server should be monitored by system administrator.
* **REQ-TR-31: Email notification for all batch jobs:** Once the batch job is finished, an email notification will be sent to system administrator.
* **REQ-TR-32: Conform to the Interoperability Framework:** The system is designed and developed using standard and well-design application framework i.e. .Net 6
* **REQ-TR-33: Manage System Parameters:** The system parameters will be placed in configuration file and will not hardcode in the coding.
* **REQ-TR-34: Allow System Access by EDB and SWD:** The EDB/SWD users are required to login their OSDP and access SCS. The user authorization control will be maintained in SCS.
* **REQ-TR-35: Independent System (Not depended on other BD system):** The system is designed to separate the front-end program for applicant/AP/RSE and the back-end program for internal BD users. Also, the system will be run independently no matter there were down time of other system, except BCIS.
* **REQ-TR-36: Logout automatically for inactive for 30 minutes:** For SSO users, the logout will be done on ODSP. For special case i.e. login using username and password, the system will terminate the session after a certain time such as 30 mins.
* **REQ-TR-37: Centralized log management:** The log files will be stored in centralized folder if it is applicable
* **REQ-TR-38: Handle around 300 user accounts of EDB and SWD for Single Sign On:** The system will be tested to handle concurrent users to access SCS. In case there is any bottleneck in hardware level, it can increase the throughput by adding more nodes.
* **REQ-TR-39: Paper Less:** The system will generate and save different documents in the system and BD users will keep the documents in hard copy of the filing system.
* **REQ-TR-40: PDF template and mapping field for letter generation:** The generated documents will be in PDF format.

## 4. Constraints

The following constraints may impact the system design and implementation:

* **Complexity of Address Identification:** Due to the complexity of address identification, the system may not be able to create cases. Case creation will be passed to BCIS, and data will be sent back to SCS for workflow processing.
* **Signature of AP/RSE:** When applicants send applications by post, the system shall verify the AP/RSE information provided by MWMS 2.0. However, handwriting signatures need to be verified by the Registry using eyeball.

## 5. Appendices

* **Appendix 1 ? 3-Tier BSR System:** (Diagram of the system architecture)
* **Appendix 2 ? Sample of School and CCC Certificates and Notices:** (Examples of certificates and notices)
* **Appendix 3 ? Sample of Letter of Requirement (LoR):** (Example of a Letter of Requirement)
* **Appendix 4 ? Information Security Requirement:** (Detailed security requirements)
* **Appendix 5 ? Sample of Utilisation Report:** (Example of a utilization report)

### 5.1. Appendix 4 ? Information Security Requirement

| # | Item | N/A | :--- | :---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------- | N/A | | **Network security controls** | N/A |---|---| N/A | 1 | Ensure all unnecessary services are disabled in the network devices (e.g. unnecessary ping traffic and requests from unauthorised network ports) | N/A |---|---| N/A | 2 | Ensure administrative consoles are not Internet-accessible and/or can only be accessible from trusted addresses. | N/A |---|---| N/A | 3 | Ensure networks are properly segregated so that critical and normal services can utilise different network connections. | N/A |---|---| N/A | 4 | Review firewall rules, intrusion detection and protection systems and remove obsolete rules or established connections, especially for temporary rules that may have been left beyond their expected lifetime. | N/A |---|---| N/A | 5 | Review DDoS response plans including roles and responsibilities for various stakeholders (e.g. ISP and anti-DDoS service providers), internal procedures and escalation protocols etc. | N/A |---|---| N/A | 6 | Check that networks protected by a content delivery network (CDN) solution only allow incoming traffic from the specific source IP addresses of the CDN and the original Internet-facing IP addresses are not disclosed to unauthorised parties | N/A | | **Endpoint protection** | N/A |---|---| N/A | 7 | Ensure anti-malware software is installed and confirm that it is active on all systems and that signatures are updating correctly. | N/A |---|---| N/A | 8 | Ensure the latest security patches are applied to the operating systems and applications, in particular for Internet-facing systems and websites. | N/A | | **Access controls** | N/A |---|---| N/A | 9 | Review user accounts and remove any obsolete accounts. If multi-factor authentication (MFA) is enabled, check if it is properly configured. | N/A |---|---| N/A | 10 | Carefully review the user privileges and activities so as to identify and cease suspicious users from gaining unauthorised access.? Management may tighten user privilege and grant permissions only when strictly necessary. | N/A |---|---| N/A | 11 | Ensure strong password policy is adopted, in particular for all mission ciritical sytems and information systems containing classified data. | N/A | | **Logging and monitoring** | N/A |---|---| N/A | 12 | Review the existing logging mechianism to ensure sufficient logs are retained.? For email systems and internet access service, ensure that your logs are kept for at least six months.? | N/A |---|---| N/A | 13 | Ensure all security solutions including intrusion detection/prevention system (IDPS) and web application firewall (WAF), are properly configured for identifying and reporting any suspicious activities. | N/A |---|---| N/A | 14 | Ensure log records are in place with regular checking, especially for alerts generated by anti-malware and security solutions.?? | N/A |---|---| N/A | 15 | Allocate sufficient manpower and resources for monitoring and responding to potential cyber attacks. | N/A | | **Backup** | N/A |---|---| N/A | 16 | Ensure backups of data and systems are reliable and secure.? Perform restoration tests from your backups to assure speedy system recovery.?? | N/A |---|---| N/A | 17 | Ensure multiple generations of offline backups are maintained and detached from the network and system. | N/A | | **Incident response** | N/A |---|---| N/A | 18 | Review the existing incident response procedure is up to date and confirm that escalation routes and contact details are all up to date. | N/A |---|---| N/A | 19 | Ensure the escalated incident response plan covers web defacement apart from typical cyber attacks.? | N/A |---|---| N/A | 20 | Review the inventory list of the IT systems, important assets and keys for effective monitoring and resources management in emergency situations is up to date | N/A |---|---|

## 6. Conclusion

This document provides a comprehensive overview of the system installation plan for the SCS. Adherence to these requirements and consideration of the identified constraints will ensure a successful implementation.