Terms of Reference

Implementation of eCabinet System for Office of the Cabinet Ministers

ICTA/SG2/GOSL/CON/QCBS/2018/001

1. Introduction

The Office of the Cabinet of Ministers has been established and functions with the aim of providing all support services efficiently to the decision making process of the Cabinet of Ministers in fulfilling duties pertaining to the direction and control of the Government of the Republic, vested with the Cabinet of Ministers in terms of Sub-Article 42(1) of the Constitution.

Below listed functions are being carried out by the Cabinet Office in government decision making and related scope of activities;

a) Issuing instructions to Ministries on the preparation of Cabinet Memoranda and guiding the Secretaries to the Ministries and Senior Officials, and providing clarifications to them in this regard.
b) Conducting in-depth studies relating to the legal and policy aspects of Cabinet Memoranda received and making submissions to the Cabinet of Ministers and Cabinet Sub-Committees, to facilitate coherent and knowledgeable decision making on such Memoranda in the discharge of functions vested with the Cabinet of Ministers with regard to policy formulation and direction and control of the Government of the Republic.
c) Referring Cabinet Memoranda to the relevant Ministers for their observations.
d) Listing Cabinet Memoranda after perusal, on the Agenda of Meetings of the Cabinet of Ministers.
e) Submitting Cabinet Memoranda together with the relevant observations, to the Cabinet of Ministers and Cabinet Sub-Committees, for consideration.
f) Preparation of Minutes of the Meetings of the Cabinet of Ministers, and Cabinet Sub-Committees in all three languages and referring such Minutes to the Hon. Ministers, Secretaries to the relevant Ministries and to the other authorities.
g) Conveying decisions taken by the Cabinet of Ministers to the relevant Ministries.
h) Monitoring the implementation of important Cabinet decisions.

2. Background

The existing IT systems of the Office of the Cabinet of Ministers which covers most parts of the scope of work of the Cabinet Office has been running obsolete since a considerable period of time. It has been further observed that the technological as well as functional incompatibilities are critical performance factors and the system itself is running in an acute

state, creating a high-risk situation. Additionally, in a backdrop where the manual working systems are rarely encouraged within the government context with latest ICT initiatives, this has been identified as a scenario that needs to be addressed carefully, offering high priority.

Hence, with the identification of the existing system, the existing functionalities of the Office of the Cabinet of Ministers and the application of aforementioned ICT initiatives which are strongly backed by the Government of Sri Lanka, it has been observed that an Information System to facilitate the Cabinet Office, better known as eCabinet, is a powerful tool that the Government shall use to streamline its decision-making process.

The proposed information system is aimed to improve and enhance all the functions of the existing systems within the Cabinet Office, namely WinMinutes, CPIS and Dec2005. The proposed system will further cater as a Document Archiving and Management System and a Work Flow Management System.

3. Objectives of the Contract

ICTA intends to procure and obtain the services of a consultant firm to implement eCabinet system for Office of the Cabinet of Ministers.

The consultant firm is required to design and develop and implement as well as maintain the implemented eCabinet system, which will be streamlined and improve the decision-making process while enhancing the efficiency and the effectiveness within the Cabinet Office of Sri Lanka as well as ensure proper dissemination of decisions to Line Ministries and other relevant Institution.

The total duration of the assignment must comprise of time for system design, development and final deployment including periodic user training and demonstrations as well as the support and maintenance (45 months).

4. Scope of the Project

4.1. The consultant should conduct a system requirements study of the processes. Moreover, consultant should propose a solution and repository model to save the cabinet memorandum and related documents with increased integrity and availability. Refer Annex 1 and Annex 2.

4.2. The solution should have the provision to facilitate eSignature facility in future.

4.3. The selected consultant should conduct requirement gathering when necessary to identify and verify the requirements with the relevant stakeholders. Furthermore, consultant should propose any improvement if required.

4.4. On completing the above, a Detailed Software Requirements Specification (DSRS) and a Detailed Software Technical Design (DSTD) document should be submitted.

Consultant should obtain approval from Office of the Cabinet of Ministers for the DSRS and approval from ICTA for the DSTD respectively.

4.5. Upon obtaining approval from the committee appointed by ICTA for the above, consultant should design and develop the system.

4.6. The consultant should submit all deliverables as specified in below item '5 – Final outputs, Reporting Requirements, Time Schedule for Deliverables'.

4.7. The consultant should implement security and governance including role-based security, user lifecycle management and complete audit-trails. Further, the independent third party will review and provide approvals respectively.

4.8. The web application should be compatible with latest technological components and best practices which proposed by ICTA and should be able to deploy into staging and production in cloud platform provided by ICTA.

4.9. The consultant should follow the proper coding standard, maintain project source code in the ICTA, SVN system, and upload documents to the ICTA, SCM.

4.10. The intellectual property rights of the software application and all artifacts in accordance with the conditions of the contract.

4.11. Solution should be adhered to Web 2.0 concepts, open standards and Service Oriented Architecture (SOA).

4.12. The consultant should study and propose suitable hardware requirements (such as scanners and printers, if required) to the proposed solution 4 months prior to the software deployment and should provide the detailed specifications.

4.13. If any commercial version of the software need to be used in the proposed solution (such as database), the consultant need to inform ICTA in advance with proper justification of the requirement. The cost of the product will be borne by ICTA.

4.14. The proposed solution should be able to generate reports quickly and in intuitive way from data exists in the database.

4.15. The consultant shall adhere to standards defined by ICTA such as Lanka Interoperability Framework (LIFe) and eGovernment Policy, the application must be compliant with the standards for Sinhala – SLS 1134: 2004: Parts 1 and 2 thereof and SLS 1126:2008 Tamil: Part 1

4.16. The consultant should understand and ensure the existing data volume and data complexity and provide data migration strategy accordingly. Moreover, data transformation strategy should follow the proper industry standers and proper control mechanisms have been used in transforming these data in to the new system.

4.17. Proposed solution should be browser independent and able to access with less configuration in the client workstation.

4.18. ICTA or relevant service provider will conduct security assessments periodically and the consultant should fix any vulnerability issues identified during assessments. (Prior to solution launch and during support and maintenance period).

4.19. The system should consume existing government authentication services and integrated with existing government software platforms (i.e. GOVSMS etc.) and also should expose API/web-services to external stakeholder organizations. (If required).

4.20. The consultant should follow templates if provided by ICTA for deliverables.

4.21. The consultant shall comply with the independent quality audit process, which will be carried by a team designated by the ICTA.

4.22. Consultant should submit test plan, test cases and UAT criteria and approval should obtain from Office of the Cabinet of Ministers and ICTA.

4.23. Obtain User Acceptance Test (UAT) for the implemented processes collaboratively with ICTA and Office of the Cabinet of Ministers against the approved UAT criteria.

4.24. The proposed solution should have proper data backup plan and equipped with high availability and fault tolerance.

4.25. The consultant should provide support and maintenance for 3 years to the developed solution from the date of launch of the system. Moreover, the consultant should adhere to the Service Level Agreement (SLA), during the support and maintenance (S&M) phase (Refer Annex 5 – Service Level Agreement for Support and Maintenance Services).

4.26. The consultant should develop proper alerting mechanism to monitor system performance issues, exception and system downtimes. Moreover, proposed alerting mechanism should able to send alert via SMS to designated offices by ICTA.

4.27. During the support and maintenance period of the eCabinet solution, the consultant should attend to any issue reported and carryout configuration changes (if required) and apply relevant security patches to make sure the security of the solution. Change requests (CR) should accommodate after obtaining the approval from the Change Control Board and as per the CR rate agreed in the contract.

4.28. The Consultant should accommodate change requests (CR) after obtaining the approval from the Change Control Board and as per the CR rate agreed in the contract.

4.29. At the end of the S&M period, the consultant should handover the source code and relevant documents to ICTA, with a proper knowledge transfer session to the ICTA technology team including updated artifacts such as DSRS, DSTD and deployment document).

4.30. Adhere to ICTA project management practices.

4.31. The solution should be deployed in Lanka Government Cloud 2.0 (LGC 2).

4.32. The consultant who engage with the assignment should sign a Non-Disclosure Agreement (NDA) where applicable.

4.33. Documents and Trainings

4.33.1. The consultant should provide user manuals in proper format. All manuals should be in tri-languages (Sinhala, Tamil and English). The user manuals should be available in electronic format and animation format.

4.33.2 The consultant should carry out overall application training to other authorized stakeholders takes place on a date determined by the Secretary to the Cabinet of Ministers.

4.33.3 The consultant should carry out overall application and administration training of the eCabinet system to other authorized stakeholders takes place on a date determined by the Secretary to the Cabinet of Ministers.

4.34. The consultant and developers should obtain security clearance from the Office of the Cabinet of Ministers.

4.35. Maintain project source code in the ICTA Source Code Management (SCM) system and upload documents to the ICTA Document Management System (DMS).

4.36. Participate for Project Review Committee meetings, Project management committee Meetings as a member, and present the status of the project when necessary.

4.37. The consultant should coordinate with a relevant service provider to conduct system vulnerability assessment including the support and maintenance period.

4.38. Adopt a proper release procedure to release the patches/updates and deployment into the staging /production environments after completion of successful User Acceptance Test (UAT).

4.39. The consultant should work collaboratively with all stakeholders and attend to weekly progress meetings and management meetings.

4.40. The consultant should obtain approval from the committee appointed by ICTA all deliverables mentioned in section ‘5 – Final outputs, Reporting Requirements, Time Schedule for Deliverables’.

4.41. During the support and maintenance period, the consultant should attend to resolve any issue through the Virtual Private Network (VPN) connections provide by ICTA.

4.42. Refer following Annexes, which form a part and parcel of the Terms of References.

Annex 1 - Overview of the Proposed System
Annex 2 - High Level Requirements of the Proposed System
Annex 3 - Non-Functional Requirements
Annex 4 - The Lanka Gate Initiative Overall Architecture & Design
Annex 5 - Service Level Agreement for Support and Maintenance Services

5. Final outputs, Reporting Requirements, Time Schedule for Deliverables

The total project duration is Forty-Five (45) months. Out of which 9 months for the implementation of the application including requirement gathering, designing, and developing and 36 months (03 Years) for the support and maintenance.

Consultancy firm is required to submit the following list of deliverables for eCabinet application development and support & maintenance project for system.

No	Deliverable	Phase
5.1	5.1.1 Inception Report 5.1.2 Implementation Schedule / Project Plan	Inception
5.2	5.2.1 Detailed Software Technical Design (DSTD) document 5.2.2 Data migration and integration plan (if applicable) 5.2.3 Release Management plan (Including staging, production and support and maintenance.) 5.2.4 API documentation (if applicable) 5.2.1 Details Software Requirement Specification (DSRS) 5.2.2 QA Plan and Test Cases 5.2.3 Specifications for devices if required (Eg. Mobile devices, Scanners, etc.) 5.2.4 Acceptance criteria for Deliverables, UAT	Elaboration
5.3	5.3.1 Proper maintenance of source code in SCM 5.3.2 Test Cases and Test Scripts	Construction
5.4	5.4.1 Solutions installation guide 5.4.2 User manual 5.4.3 Administrator manual 5.4.4 Government organization level training 5.4.5 Successful UAT acceptance of the eCabinet application and deployment 5.4.6 Test Results (Functional and Non-Functional)	Transition
5.5	5.5.1 Monthly support and maintenance report 5.5.2 Final S&M report should consist with comprehensive knowledge transfer documentation. 5.5.3 With the final S&M report provide updated DSTD, API documentation, DSRS and verified source code.	S&M

Refer http://en.wikipedia.org/wiki/IBM_Rational_Unified_Process for more information about RUP (Rational Unified Process) phases.

6. Services and facilities provided by ICTA and Office of the Cabinet of Ministers

6.1 Web-based access to the ICTA SCM system

6.2 Access to staging/ production servers

6.3 Web-based access to the ICTA SVN system and SCM.

6.4 Arrange meetings with relevant stakeholder (if required)

6.5 Arrange and facilitate the workshop/training with relevant stakeholders

7. Review Committees and Review Procedures

The Software Development Service Provider is required to work closely with the ICTA Technology Team and the Software Process Audit (SPA) consultants.

All versions of deliverables will be reviewed by the team appointed by ICTA.

All the deliverables must be verified and confirmed to be accurate and complete by the Project Implementation Committee (PIC) or the Project Management Committee (PMC).

References:

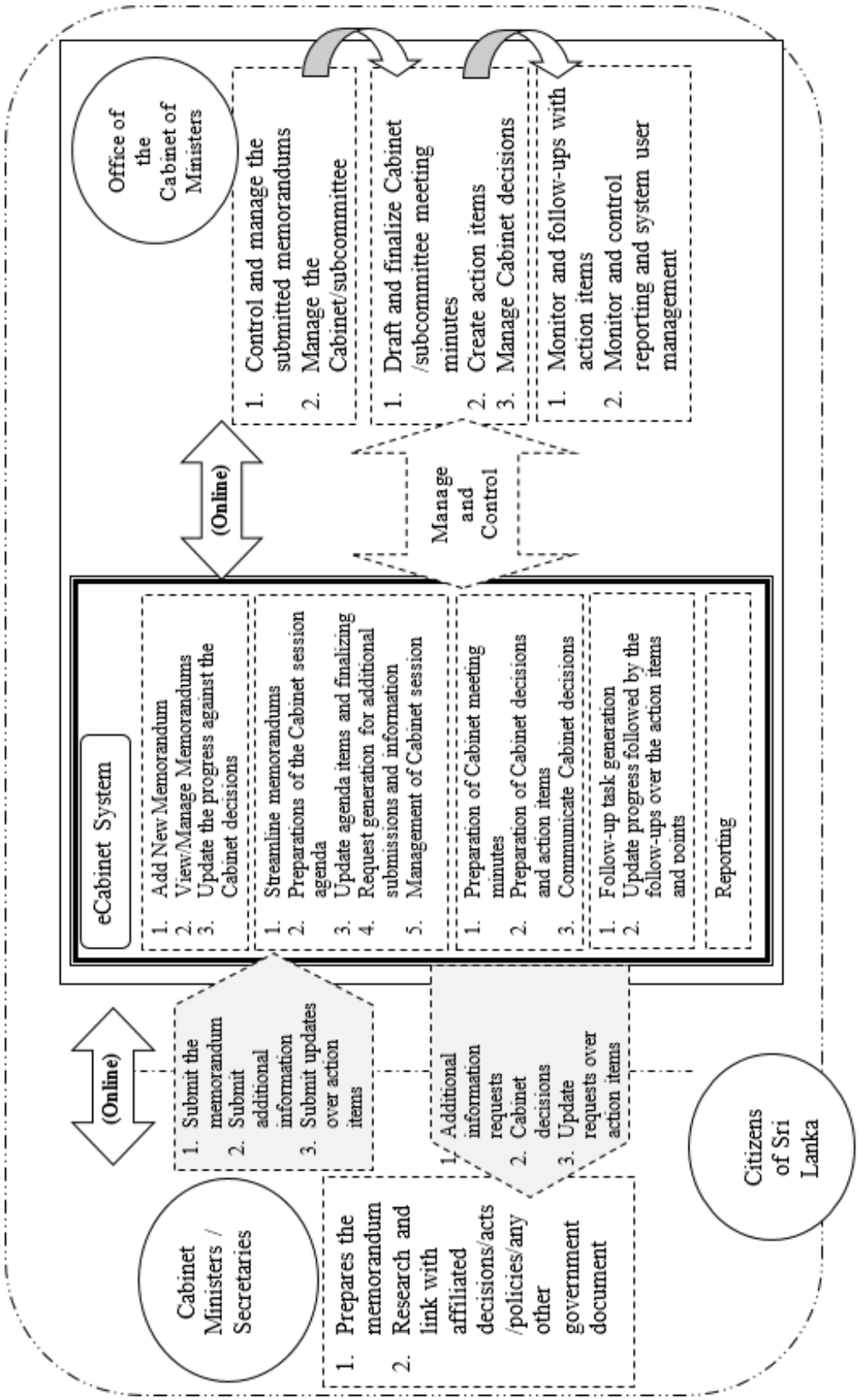
[1] eGovernment Policy Approved By Cabinet of Sri Lanka - https://www.icta.lk/icta-assets/uploads/2016/03/eGov-Policy-structured-v4-0.pdf

[2] Lanka Interoperability Framework - http://www.life.gov.lk/

- END -

[ANNEX 1]

OVERVIEW OF THE PROPOSED SYSTEM



[ANNEX 2]

HIGH LEVEL REQUIREMENTS OF THE PROPOSED SYSTEM

a) The Secretary to the Ministry with the approval of the Minister shall submit respective Cabinet Memoranda online through the given interface, which shall be checked by the staff of the Office of the Cabinet of Ministers through the system. The system must be capable to data feeding and documents creation in all three languages Sinhala, Tamil and English. The system must have facility to upload scanned documents that are belongs to each cabinet memorandum. Documents can have several categories.

b) The Secretaries to the Ministries are able to access the system online to review each agenda item for the next Cabinet Meeting, and comment on any required adjustments over the observations of the other Ministries updated by the Office of the Cabinet of Ministers. The Secretaries to the Ministries are able to submit any additional submission online with respect to the submitted memoranda where requested by the Office of the Cabinet of Ministers.

c) The Office of the Cabinet of Ministers shall prepare the weekly agenda for the cabinet meeting through the eCabinet system which is accessible by the Hon. Ministers (or the Secretary of the Ministry) as per the granted permission levels considering security aspects. The Ministers are able to view online, the corresponding papers along with the prepared agenda.

d) The Office of the Cabinet of Ministers shall update any decision/ recommendation on the agenda items of each meeting within the system. The Office of the Cabinet of Ministers shall create the minutes along with the decisions taken against each applicable Ministry through the system as well as the actions to be taken by each respective Ministry and will forward the same on-line to each applicable Ministry. The Minister and the Secretary are able to view these online.

e) The Office of the Cabinet of Ministers shall close/ re-open any action item raised against the respective Ministry, as well as, forward any actions to be assigned on behalf of the respective Minister (or the Secretary of the Ministry) within the system and all such actions will be traced.

f) The Hon. Chair of the Cabinet Meeting shall instruct on the highest National priority items and the system shall be updated accordingly or the relevant agenda item and shall be monitored through the reporting feature of the system and the same will be communicated to the Minister (or the Secretary of the Ministry) on-line.

g) The respective usage levels of the system shall be monitored/ traced by the authorized personnel as per the pre-defined system usage policy.

h) The system shall lead the Government to eliminate the need of printing and delivering thousands of pages of documents at each circle – a significant reduction in environmental impact and the applicable cost.

No	Module	Feature
01	Process of Receiving Cabinet Memorandum (CM)	The system should allow submitting Cabinet Paper (CP) by using three languages (Sinhala, Tamil and English) through following methods. I. Through the online system web portal II. Scan CP and upload to the system web portal
		Once user submit the Cabinet Paper (CP) the proposed system should allow to assigning a Cabinet Paper (CP) number according to the proper format and based on the some Cabinet Memorandum (CM) the system should allow to assign different number scheme for sub items.
		When Cabinet Memorandum is registered, the proposed system should allow to sending SMS, emailing and Pop-up alerts to the authorize user.
02	Process of check, correct and grant approval to proceed	Categorizing Cabinet Memorandum (CM) and grant approvals to proceed with the correct workflow.
03	Process of Detailed Study on Cabinet Memorandum (CM)	The proposed system should allow to below activities for the detailed study of the Cabinet Memorandum (CM) and data should feed to the system. a. Prepare official summary b. Comments by the Staff to the Cabinet Memoranda (CM) c. Blocking observation calling d. Orders by the Secretary e. Selecting for Press Briefings f. Selecting for Gazette Notifications
04	Process of observations on Cabinet Memorandum (CM)	Observations are called as per the direction of the authorized officer and the proposed system should allowing doing below activities, and data should feed to the system. a. Prepare observation calling letters b. Feed Need Time Letters c. Prepare Reminders d. Scan and Feed Received Observations e. Prepare Observation Summary (Journal) f. Feed other documents related to Cabinet Memoranda

No	Module	Feature
05	Process of Sub - Committee	When assign the sub committees to the relevant observation, proposed system should allow to do the below task as a workflow and need to feed all the information to the system. a. Preparation and Printing of Agenda b. Preparation of Supplementary Agenda c. Preparation of Journal d. Draft Recommendations e. Check and Approve Recommendations f. Print Sub-Committee Report
06	Process of Cabinet Meeting	Process of cabinet meeting below mentioned task should be covered in the proposed system and all the data should be feed to the system. a. Sending for observations of the Finance Ministry and the Advisors to the Cabinet. b. Preparing the Agenda c. Finalizing the Agenda d. Prepare the Supplementary Agenda e. Finalizing the Supplementary Agenda f. Printing the Main Journal g. Memoranda tabled at the Meeting h. Preparing Draft Decisions i. Checking, proof reading and finalizing the draft decisions j. Approving the finalized decisions k. Faxing urgent decisions l. Translate approved decisions m. Check, proof reading and finalizing the Translated decisions n. Approving the finalized translations o. Print Minute of the Cabinet Meeting
07	Process of Press Briefing	The proposed system should allow to feed below information to the system and printing and faxing facility allow to use based on the approval of the authorize officer. a. Selection of Items for the Press Briefing b. Drafting of the Press Briefing c. Print & Fax the Press Briefing d. Translation of the press briefing to English and Tamil e. Uploading the press briefing to the official website of the Cabinet Office
08	Process of Cabinet Decision	Scan and upload the Decision to the System Print relevant documents to send to Ministries Prepare Gazette Notifications

No	Module	Feature
09	Process of Monitoring	The proposed system should support to below features without effecting performance of the system. a. Categorizing Decisions b. Assigning Activities c. Printing and Sending Evaluation Forms d. Data Gathering and Feeding e. Data Analysis and Reporting
10	Process of Searching	Searching for a Cabinet Memorandum Searching for a Cabinet decision
11	User Authorization	Study and propose different workflow based dual authorization to approved, printing, editing,etc.. in different scenarios with the facility to alert the relevant user.
12	System Logging	An audit trail of all the user actions performed on the application must be maintained. The information to be maintained includes (not limited to), a. User / user role b. Date and Time c. Module / Feature Accessed d. Action Performed

[ANNEX 3]

NON - FUNCTIONAL REQUIREMENTS

1. Security

1.1. User authentication and authorization

All applications should be able to access via ICTA's common infrastructure/application itself and independently via respective department's web site if required. Any authorization requirements should be implemented within the specific web/mobile application.
However, the solution should have the provision to integrate with the ICTA's proposed Identity Management solution in future.
An administrative application need to be developed wherever applicable.
Wherever applicable internal small applications need to be developed to capture and store relevant data.

1.2. Confidentiality and Integrity

All developed web/mobile applications should ensure "confidentiality" and "integrity" whenever required by adhering to transport and message level security standards. (i.e.: HTTPS, WS-Security)

1.3. Authentication

The web/mobile application should be able to verify the users.

1.4. Authorization

The web/mobile application should be able to verify that allowed users have access to resources.

1.5. Non-repudiation

All Web/mobile applications should ensure non-repudiation by having standard audit-trails and provisions to have WS-Security using digital signatures.

1.6. Open Web Application Security Project (OWASP) Guidelines

All web/mobile applications should ensure that the OWASP guidelines for security are followed when designing, developing and deploying the web/mobile application.

1.7. Encryption and Decryption

All web/mobile applications should ensure have maintain proper encryption and decryption standards for the data and scan documents.

2. Audit Facilities

Wherever applicable, an audit trail of all activities must be maintained. On a service or operation being initiated, the system should log the event, creating a basic 'audit log entry'. It should not be possible for the operation to be executed without the log entry being made. The information recorded in the audit trail depends on the type of activity which takes place. Each service would be responsible for logging detailed information. The different types of operations are -

- Data Capture & Maintenance
- Creation of an entry / item
- Modification an item
- Deletion
- Control (or status change)
- Process execution
- Data synchronization
- Print (only selected item)
- Retrieval
- Monitor

Detail logging may be enabled or disabled for each type of operation, and/or for each business object. It should be possible to configure which attributes of a data item should be traced at the detail level. Tracing of some attributes may be considered mandatory, and they should not be turned off.

3. Backup and Contingency Planning

The main contingencies that should be considered and the training with regards to these shall be given to the relevant staff -

- Equipment failure
- Physical / natural Disaster
- Messaging or communication facilities.
- Changes in operations and policy
- Sudden absence of key personnel
- Breach in Security

Automatic Backups daily, weekly *and* monthly should be taken. All the backup procedures and backups needs to be tested regularly for restoration.

4. Performance Testing

Please find the below index as a guide to determine the benchmark values for the Application under the test.

Following performance criteria is provided as a guideline only. If the actual performance is falling below the stipulated figures, the consultant is to justify the reasons. However, the performance level must be accepted by the technical evaluation committee appointed by the client. The bandwidth is assumed at 1mbps (shared) with 1,000 concurrent users (50% load factor) in total.

Item	Performance
Screen Navigation: field-to-field	< 5 milliseconds
Screen Navigation: screen-to-screen	< 3 seconds
Screen Refresh	< 3 seconds
Screen list box, combo box	< 2 seconds
Screen grid – 25 rows, 10 columns	<3 seconds
Report preview – (all reports) – initial page view (if asynchronous)	<40 seconds in most instances. It is understood that complicated / large volume reports may require a longer period
Simple inquiry – single table, 5 fields, 3 conditions – without screen rendering	< 4 seconds for 100,000 rows
Complex enquiry – multiple joined table (5), 10 fields, 3 conditions – without screen rendering	< 6 seconds for 100,000 rows
Server side validations / computations	< 10 milliseconds
Client side validations / computations	< 1 millisecond
Batch processing (if any) per 100 records	< 120 seconds
Login, authentication, and verification	< 3 seconds
Daily backups (@Dept.) – max duration	1 hour (on-line preferred)
Total Restore (@Dept.) – max duration	4 hours

4.1 Performance Test Process Outputs

- Performance Test Scripts
- Performance Test Results

5. Usability

The web/mobile application should be extremely usable, even a greenhorn user should be able to handle the system and incorporate all the functionality of the system in a simple and user friendly interface. The web/mobile application should be internationalized and localized if needed. The web/mobile application should be responsive where it should be viewable on any computing device.

6. Interoperability

The web application should be able to view in standard compatible web browsers.

7. Availability

   The web/mobile application should be performed as follows,

   - 99.99% available unless the web/mobile application is designed with expected downtime for activities such as database upgrades and backups.
   - Hence to have high availability, the web/mobile application must have low downtime and low recovery time.

8. Robustness

   The web/mobile application should be able to handle error conditions gracefully, without failure. This includes a tolerance of invalid data, software defects, and unexpected operating conditions.

   - Failure Detection
     - Once deployed, there should be appropriate tools to discover anomalies and failures of the system

   - Fault Tolerance
     - Web/mobile application developer should anticipate exceptional conditions and develop the system to cope with them. The web/mobile application must be able to use reversion to fall back to a safe mode, meaning, the application should continue its intended functions, possibly at a reduced level, rather than falling completely.

9. Maintainability

   The code of web/mobile application should be properly documented with appropriate comments and no complex codes (highly cohesive and loosely coupled) to do modifications such as corrections, improvements or adaption.

10. Compliance to Standards

    The code of web/mobile application should be standardized by following web/mobile standards like W3C and ECMA – European Computer Manufactures Association, to save time, augment the extensibility of the code, increase web/mobile traffic and improve the accessibly and load time of your application.

11. Reusability

    The web/mobile application should be able to use of existing assets in some form with the software product development process. Assets are products and by-products of the software development life cycle and include code, software components, test suites, design and documentation.

12. Internationalization

The web/mobile application should be able to access in Sinhalese, English and Tamil. The web/mobile application should be able to view in a usable manner in all three languages in any computing device.

13. API Management

13.1. API Standards and Best Practices

API standards and best practices that *should be adhered* to the code.

13.2. API Documentation

- Swagger documentation should be provided.

13.3. API Security

The web/mobile application should be used appropriate API security protocol mentioned below.

- Basic API authentication
  - Basic authentication should never be used without TLS (formally known as SSL) encryption as user name and password combination can be easily decoded otherwise.
- OAuth1.0a
  - Uses cryptographic signature value that combines the token secret, nonce, and other request based information. Can be safely used without SSL.
  - Recommend for sensitive data applications
- OAuth2
  - No need to use cryptographic algorithms to create, generate and validate signatures as all the encryption handled by TLS.
  - Recommend for less sensitive data applications
- JWT (JSON Web/mobile Tokens)

14. Scalability

The web/mobile application should be both scalable and resilient. A well-designed application should be able to scale seamlessly as demand increases and decreases. It should be resilient enough to withstand the loss of one or more hardware resource.

15. Legal and Licensing

The web/mobile application should comply the national law.

16. Extensibility

The web/mobile application should be designed and developed in a way that it can cater to future business needs.

17. Testability

The web/mobile application should be designed and developed in a way that testability is high, meaning, the ease of testing a piece of code or functionality, or a provision added in software so that test plans and scripts can be systematically executed. In simple terms, the software should be tested easily with most famous 5 testing categories;

- Unit test
- Integration test
- System test
- Safety test
- Experience test

Refer Aden (2016)'s view on semantic testing for more information.

The web application should be working according to the given criteria in the latest version and 5 versions before in web browsers such as Mozilla Firefox, Google Chrome, Opera, and Apple Safari and the latest version and 2 versions before in Internet Explorer.

18. Notes

- Some of the none-functional requirements shall be excluded based on the project requirement with the approval of the ICTA Technology Team.
- The vendor can propose similar standards/requirements for the above-mentioned standards/requirements with the approval of the ICTA Technology Team.
- The design documents should be based on 4+1 architecture model.

BIBLIOGRAPHY

1. The White House. *White House Web/mobile API Standards*. Washington, D.C.: git hub.com, 2015. Print.

2. Aden, S. (2016). Semantic Testing. Retrieved August 30, 2017, from https://semantictesting.org/

[ANNEX 4]

THE LANKA GATE INITIATIVE
OVERALL ARCHITECTURE & DESIGN

a) Introduction to Lanka Gate

As an important component of the e-Sri Lanka initiative, it is envisioned that practically all the eServices and electronic information in Sri Lanka will be delivered via a comprehensive integration platform. This wide collection software infrastructure and systems which is envisioned to be the gateway for electronic information and electronic interactions in Sri Lanka, is generally referred to as the 'Lanka Gate' initiative.

Many eServices will be generated as a result of various projects done at the ICT Agency, such as the Population Registry project, the ePensions project and the Samurdhi Services project. In addition, many other eServices could be generated by government, public and private sector organizations as well as by community groups. Lanka Gate would include a comprehensive collection of infrastructural mechanisms to easily 'plug-in' an eService or to 'compose' a set of eServices in order to generate a composite eService, such that these eServices would be readily and easily available to other applications and portals that comprise Lanka Gate. For this purpose, it is envisioned that the projects within Lanka Gate would be designed to leverage Web 2.0 concepts, open standards and a Service Oriented Architecture (SOA), enabling dynamic, customizable, collaborative and compose-able services via multiple delivery channels.

Thus the collection of software systems that comprise Lanka Gate would collectively provide an enabling infrastructure for rapid integration and delivery of eServices, leveraging loosely-coupled architectural principles to encourage the creation of innovative applications, solutions, and business models, communication models, pricing models and service mash-ups by various stakeholders across the country.

The intention is that this architectural blueprint will guide the various software engineering projects that would eventually be integrated into Lanka Gate. Since Lanka Gate will always be in a state of flux with the continuous addition of eServices from new projects, removal of old eServices as well as the generation of new applications, portals or composite eServices via services mash-ups or services composition, it is hoped that this overall architectural blueprint would continue to 'live' as a vision of what the end result should embody. Furthermore, it is expected that the launch of the Lanka Gate initiative will be coupled with the roll-out of a strong SOA Governance Model.

b) Lanka Gate: The Core Components

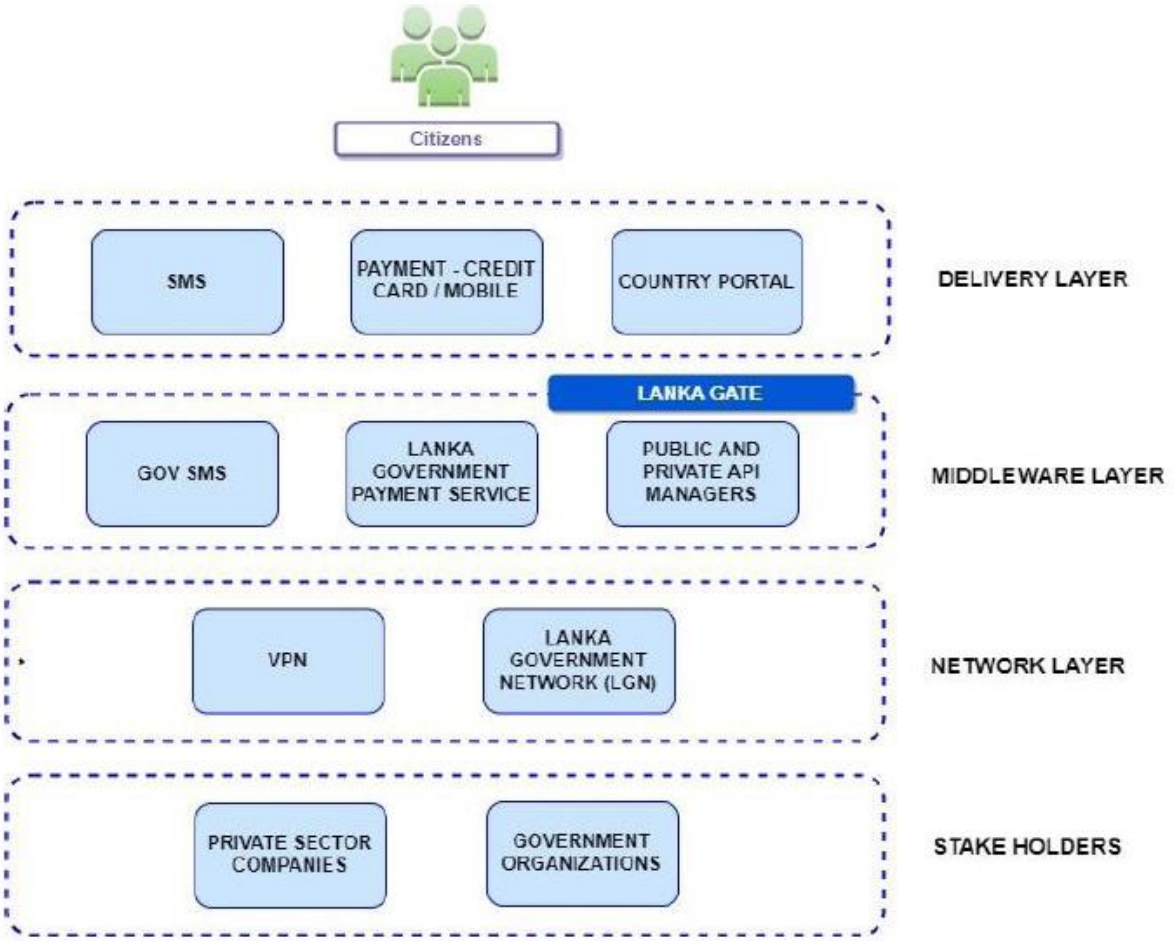


Figure 1 – The Conceptual Architecture

The conceptual design shown above in Figure 1 illustrates the loosely-coupled and flexibility of the Lanka Gate infrastructure. It is composed of following core components.

1. API Manager

The API Manager exposes it core processes, data and services as API to the public. External parties can mash up these APIs in innovative ways to build new solutions. However, leveraging APIs in collaborative manner introduces new challenges in exercising control, establishing trust, security and regulation. API Manager overcomes these challenges though a set of features for API creation, publishing, life cycle management, versioning, monetization, governance, security etc.

External consumers and partners, as well as internal users can publish secured, authenticated, authorized and protected APIs. API Manager supports publishing multiple protocols including SOAP, REST, JSON and XML style services as APIs. This includes extremely high performance pass-through message routing with sub-millisecond latency.

2. Country Portal (CP)

The Country Portal (www.gov.lk) serves as a primary web interface that connects users to the eServices provided within the Lanka Gate concept. Thus the Country Portal is a fundamental access point for citizens, non-citizens, businesses, agents and government employees to various government organizations and businesses in Sri Lanka. The Country Portal features multiple service delivery channels to accommodate various end user realities.

The Country Portal project is a container which provide access to eServices Web application which are self-contained front-end interfaces to either a single eService, several eServices from a specific project, or a transactional/mashup combination of eServices across several projects.

The web browser based delivery channel of the Country Portal features a highly user-friendly, dynamic interface, providing the end-user with the capability to design their own interactive user experience based on their particular needs and preferences. Most of the Web 2.0 capabilities available in Lanka Gate will be delivered through the web browser based delivery channel.

3. Credit Card On-line payment and Mobile payment Services

A system to enable credit card payments and payment via a mobile phone for government enabled eServices, thereby facilitating electronic commerce for credit card holders.

4. SMS Gateway (GovSMS)

A common interface open for mobile service providers to establish in-bound and out-bound Short Messaging Services (SMS) with Lanka Gate architecture. The mobile information and service gateway built as a part of Lanka Gate by ICTA to use the common, short telephone code "1919" should be used by all government organizations for delivery of such information and services.

c) E-Service Development for Lanka Gate

As mentioned above, the eServices to be implemented are NOT expected to implement any major systems or replace any of the existing systems at the various government departments. They are expected to tap into any existing services already implemented, or expose new services as required with minimal disruption and changes to these existing systems. Hence, there can be two basic scenarios that can be envisioned (See Figure 2).

Scenario 1: This is where a minimal changes are required. The considered department consists of a working application with a connected database OR even it may have well-written web services that can be exposed to Lanka Gate. If not, it will be a matter of exposing some according to the requirement.

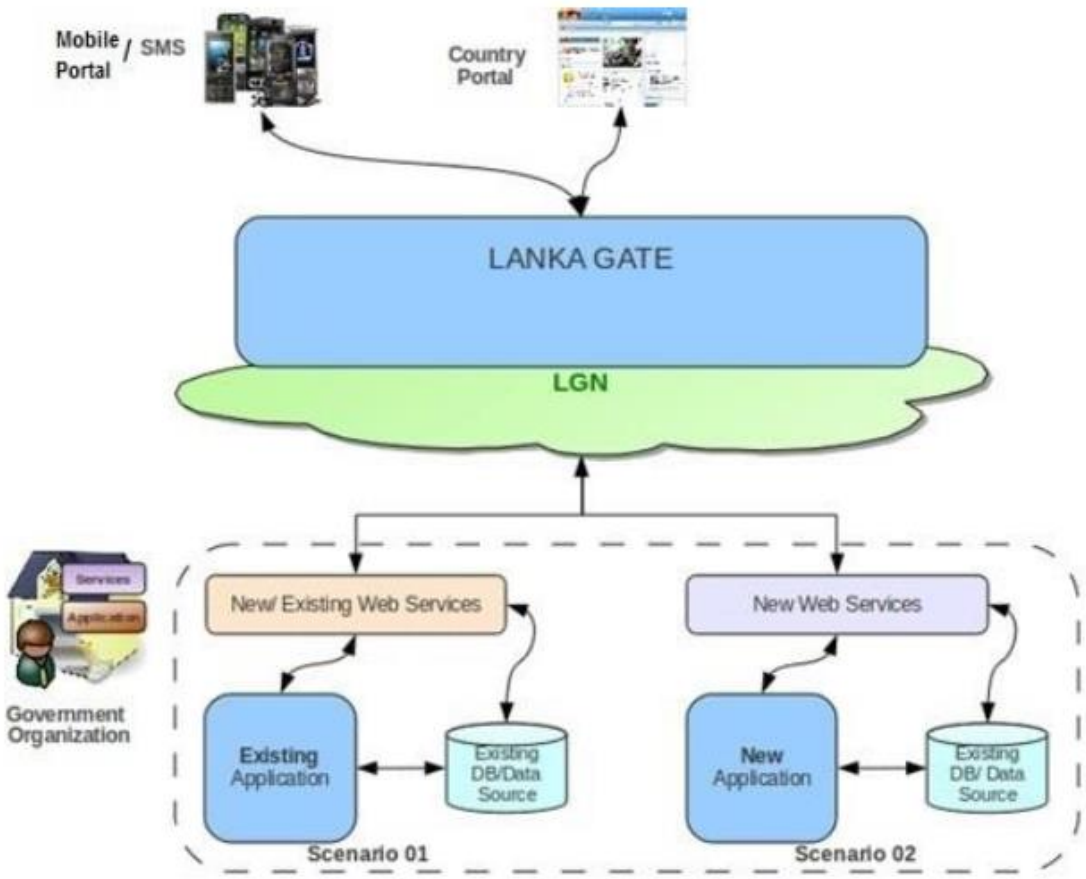


Figure 2: Developing eServices to Lanka Gate

Scenario 2: This is where SOME changes required. If the department only has a data source such as a spreadsheet, it is required to write a new application allowing the data source to be connected to the newly written web services. Otherwise, if the existing DB needs cannot be used directly to a web service, again a new application should be written to bridge the DB with web services. This complexity of this newly created application will depend on the complexity of other back office applications within the department. A proper Business Process Modeling (BPM) tool can be leveraged to ease this task depending on this complexity.

However, irrespective of the DB or the data source, it is required to write new web services to expose the back office systems to the Lanka Gate.

Certain eServices may allow the citizens to save information into the new systems, and these systems would require a database for persistence of this information. In addition, certain services may require a citizen to make payments – and these would be facilitated via the mobile or on-line payment gateways, or any existing payment mechanisms used by the department – such as via direct payment to a bank. Thus, the back-end support systems would need the ability to interact with the payment gateways and any direct interfaces to bank payment information, to ensure proper payments have been made.

In addition, some of these new systems may require an internal web based system to query information on these new eServices, as well as generate reports etc. To support these use cases, an internal web based application may need to be developed, supporting role based access for use by the internal departmental staff. As an example, if a citizen applies for some facility and electronically submits a set of documents, and makes a payment, the citizen should be able to visit the department with the relevant reference numbers, and a staff officer would then be able to verify the authenticity of the supporting documents, and confirm the payment, so that the facility could then be made available to the citizen with a shorter processing time. In addition, some of these eServices may allow a citizen to schedule such a visit to the department – to ensure expected levels of service. Hence, such a scenario would require the back end systemto perform a simple scheduling of the applicants to the department depending on certain variables.

Developing Web Applications for Lanka Gate eServices

For any eService, a simple web application should be developed and these web applications must be able to access via country portal as well as independently via the respective department's web site. The web applications must be able to support English, Sinhalese and Tamil. If the eService is a simple query (e.g. status check), the web application would be able to call into the existing web services or a new web service developed to cater to the use case in question.

Developing SMS Services for Lanka Gate eServices

If the query service in question, is also offered over SMS, the SMS gateway would be able to invoke this same web service, and respond back to the user with the results. Some eServices may allow the user to subscribe to certain events (e.g. change of status, delay of an application etc), at which point, the system should push SMS updated back to the user via the SMS gateway – if the user has specified a mobile number, and requested SMS notifications. When a new SMS is received by the SMS gateway, it will be routed to a REST service of the target department, and each department will then have to implement the SMS request processing logic, and optionally response where applicable.

[ANNEX 5]

SERVICE LEVEL AGREEMENT *for* SUPPORT AND MAINTENANCE SERVICES

I. Introduction

The aim of this agreement is to provide a basis for close co-operation between the Service Provider (name of the company) and Client (ICTA) for support and maintenance services to be provided by the Provider, thereby ensuring a timely and efficient support service is available. The objectives of this agreement are detailed below point (ii).

This agreement is contingent upon each party knowing and fulfilling their responsibilities and generating an environment conducive to the achievement and maintenance of targeted service levels.

II. Objectives of Service Level Agreements

- To create an environment conducive to a co-operative relationship between Client, Service Provider and Client's representatives (government organizations) to ensure the effective support of all end users.
- To define the commencement of the agreement, its initial term and the provision for reviews.
- To define in detail, the service to be delivered by each party and the level of service expected, thereby reducing the risk of misunderstandings.
- To institute a formal system of objective service level monitoring ensuring that reviews of the agreement is based on factual data.
- To provide a common understanding of service requirements/capabilities and of the principals involved in the measurement of service levels.
- To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

III. Principal Period of Support (PPS) Requirements

The Principal Period of Support (PPS) is considered as follows;

PPS category	Duration	Applicability
PPS	From 08:00 AM to 07:00 PM Monday to Sunday.	For the essential component applications and online service platform related departments.

Service Provider MUST assure System Support and Maintenance Services during the above stipulated times.

IV. On-Call Services Requirements

Provider MUST make at least ONE qualified personnel available to the Client by telephone and email for the reporting and resolution of non-conformities or other issues, defects or problems. Dedicated telephone numbers and emails should be available for reporting issues. Client will nominate the personnel who are authorized to report non-conformities or other problems with the system from the departments. Reporting of non-conformities includes requests by the Client to apply critical software updates or patches.

Table-1 shows the response priority assigned to faults according to the perceived importance of the reported situation and the required initial telephone response times for the individual priority ratings. All times indicated represent telephone response time during specified PPSs. The indicated telephone response time represents the maximum delay between a fault/request being reported and a Provider's representative contacting the Client by telephone. The purpose of this telephone contact is to notify the Client of the receipt of the fault/request and provide the Client with details of the proposed action to be taken in respect of the particular fault/request.

	Business Critical	**Non-Business Critical**
Fatal	30 minutes	45 minutes
Impaired	45 minutes	90 minutes

Table-1: Response Priority

Note:
Fatal - Total system inoperability
Impaired - Partial system inoperability
Business Critical - Unable to perform core business functions
Non-Business Critical - Able to perform limited core business functions

Provider notification can occur outside PPS time, and thus the response may occur after the next PPS begins. Furthermore, "Time to Arrive On-Site (Table-3)" starts from PPS starting time and "Time to Resolve the Problem" is PPS time starting from the actual time of arrival on site.

V. Problem Resolution and Penalties

If problems have not been corrected within two (2) hours of the initial contact, the Provider shall send qualified maintenance personnel to the respective Client's site to take necessary actions to correct the issue reported (defect, problem or non-conformity).

If faults are not corrected within the time limits specified in the Table-2, the Client shall be entitled to a penalty payment for each hour that the Consultant fails to resolve the fault. Maximum ceiling of penalty for a given month is 10% of the invoice amount for the month.

	Business Critical	**Non-Business Critical**
Fatal	1 Hours LKR 60,000.00	2 Hours LKR 30,000.00
Impaired	2 Hours LKR 40,000.00	5 Hours LKR 20,000.00

Table-2: Resolution Time and Penalties

The time to arrive on-site is specified in the Table-3.

	Business Critical	**Non-Business Critical**
Fatal	2 Hours	3 Hours
Impaired	3 Hours	5 Hours

Table-3: Time to arrive on-site

VI. Service Level Monitoring

The success of Service Level Agreements depends fundamentally on the ability to meet agreed service levels and effective measuring of performance, comprehensively and accurately so that reliable information is available for both parties in agreement. Thereby a clear understanding and effective communication can be maintained between the provider and customer.

Service factors must be meaningful, measurable and monitored constantly. Actual levels of service are to be compared with agreed target levels on a regular basis by both Client and Provider. In the event of a discrepancy between actual and targeted service levels both Client and Provider are expected to identify and resolve the reason(s) for any discrepancies in close co-operation.

Compliance to SLA will be monitored via:

a. Completion of deliverables as per agreed time lines;
b. Accuracy, completeness and quality of the deliverable;
c. Issues resolution within the agreed upon time;
d. On call support within agreed upon time;

Service level monitoring will be mainly performed by Client. Provider may also monitor the level of compliance, for possible improvements. Reports will be produced as and when required and forwarded to the necessary parties.