Security Risk Assessment & Audit Report

of

Security Risk Assessment & Audit Services for LeaveHomeSafe Mobile App and related Support System (3.0)

Version 1.0
22 November 2021

Document Information

Project Name:	Security Risk Assessment & Audit Services for LeaveHomeSafe Mobile App and related Support System (3.0)		
Project Manager:	[redacted]	**Document Version No:**	1.0
Quality Review Method:	Independent Quality Review	**Document Version Date:**	22 November 2021

Distribution List

From	**Date**	
Contractor	22 November 2021	

To	**Action***	**Due Date**	
OGCIO	Review		
Contractor	Inform		

** Action Types: Approve, Review, Inform, File, Action Required, Attend Meeting, Other (please specify)*

Version History

Ver. No.	**Ver. Date**	**Description**	**Filename**
1.0	22 November 2021	Document creation	OGCIO LHS SRAA Report (3.0) v1.0.docx

Table of Contents

Abbreviation

The following abbreviations are commonly used in this document:

HKSARG	The Government of the Hong Kong Special Administrative Region
LHS	LeaveHomeSafe Mobile App and related Support System
IT	Information Technology
OGCIO	Office of the Government Chief Information Officer
SR	Security Regulations
SRA	Security Risk Assessment
SA	Security Audit

1. Introduction

The Contractor provided the following services for the Office of the Government Chief Officer ("OGCIO") of the Government of the Hong Kong Special Administrative Region ("HKSARG or the Government"):

(a) By evaluating the security risks of the LeaveHomeSafe ("LHS") Mobile App and related Support System ("the System") including planned enhancements, the Contractor identified and recommended safeguards with the aim of strengthening the security protection of the system and the related data to an acceptable level.

(b) A security audit has been carried out to determine the state of the existing protection and to verify whether the existing protection has been implemented effectively.

(c) A verification process has been carried out to review the security status of the System and data to ensure that all risks identified in the security risk assessment and security audit have been mitigated or reduced to an acceptable level.

The scope of the services covered the security areas and controls specified in the Baseline IT Security Policy (S17), in particular the 14 areas listed in section 2.1 of S17.

The purpose of this document is to formally present the findings and recommendations of the security assessment and audit activities to OGCIO.

2. Management Summary

The Contractor analysed the security risks of LHS based on the information collected in various activities – document review, user interviews, discussion sessions, questionnaires and vulnerability scans. Each identified threat was associated with a risk level derived based on the potential impacts and the likelihood of occurrences to LHS. For each threat, the Contractor provided recommendations to enhance the security of LHS and to mitigate the potential risk to LHS. The various risk levels are described as follows:

Risk level	Implication and recommendation
H (high)	Means critical impact and improvements should be made within a short time: high-priority items
M (medium)	Means moderate impact and improvements should be made within a reasonable time: medium-priority items.
L (low)	Means low impact and improvements should be made when resources are available: low-priority items.
Area of Improvement (AOI)	Does not impose immediate threats but implementation of such items will improve the environment. Implementation of these suggestions should be considered when resources are available.

In general, security controls are found properly in place to protect LHS, their data and related infrastructure, and the System are in compliance with the prevailing IT security regulations, security policies, standards, guidelines and procedures of the Government and OGCIO.

Nevertheless, 3 low risk items and 1 medium risk item were identified in the Security Risk Assessment (SRA) and Security Audit (SA). The tables below summarise the findings:

SRA Findings:

Systems	Risk Level			
	H (High)	**M (Medium)**	**L (Low)**	**AOI (Area of Improvement)**
Source Code Review	0	0	0	0
LHS Website Penetration Test	0	0	1	0
LHS Mobile App Penetration Test	0	1	1	0
Total	**0**	**1**	**2**	**0**

SA Findings:

Systems	Risk Level			
	H (High)	**M (Medium)**	**L (Low)**	**AOI (Area of Improvement)**
General Control Review	0	0	1	0
Total	**0**	**0**	**1**	**0**

3. Assessment Scope and Objectives

3.1 Assessment Scope

The scope of the services covered, but not limited to, those areas related to security management, access control security, data security, system security, application security, and network and communications security. The Contractor identified and recommended safeguards with the aim of strengthening the level of security protection of the System and the related data to an acceptable level.

3.2 Assessment Objectives

The project objectives of this work assignment were:

a. To evaluate the security risks of the LHS and the related data of OGCIO in relation to the use of information technology ("IT"), to identify and recommend safeguards with the aim of strengthening the security controls of the System and data to an acceptable level.

b. To evaluate the compliance with required security requirements and the effectiveness of security controls being implemented.

c. To carry out a verification check to review the security status of information system(s) and the related data to ensure that all identified risks have been mitigated or reduced to an acceptable level.

4. Security Risk Assessment Methodology

The IT security risk assessment methodology ensures that the qualitative approach to conduct a security risk assessment is based on logical analysis. The security risk assessment consisted of a number of smaller steps. The overall security risk assessment process is illustrated in a flow chart as follows:

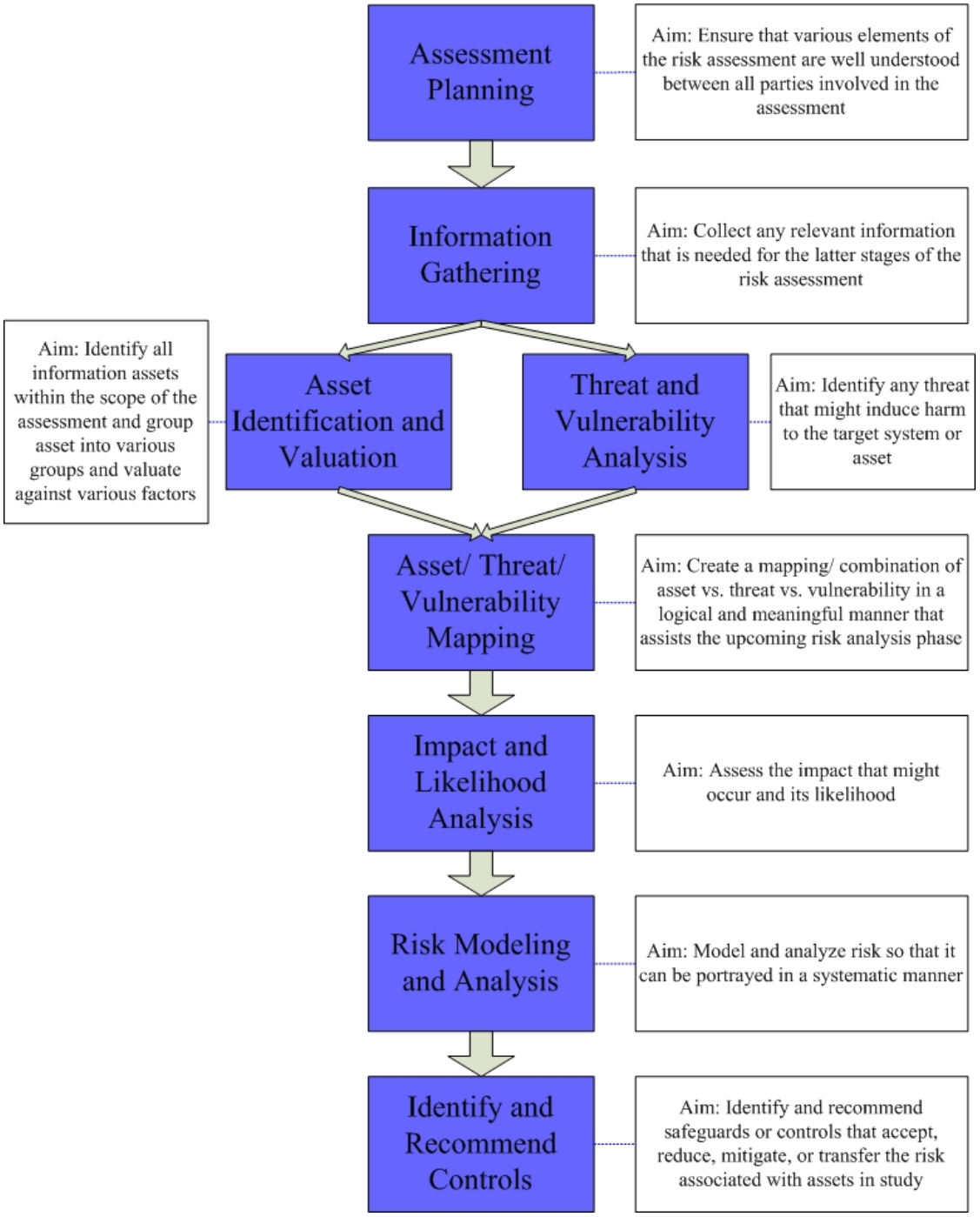

Figure 1. Methodology of security risk assessment service

4.1 Assessment Planning

The initial step of the security risk assessment was assessment planning. This step ensured that various elements of the security risk assessment were well understood among all parties. The Contractor collected, identified and defined elements such as background information, objectives, scope, roles and responsibilities, constraints and approach.

4.2 Information Gathering

In this step, the Contractor collected all relevant information that was needed for the subsequent stages of the security risk assessment. Information collected included:

- Security requirements
- Service requirements
- System documentation (e.g. system specifications, etc.)

The methods used for information gathering included:

- Discussions – to discuss the documents and design with the service provider to identify proposed security controls on the system, network, data and application.
- Document review – to review system documents.
- Questionnaires – to facilitate the purpose of understanding more about the current environment/ security practices and as part of the general control review
- penetration/scanning test (website and mobile app) and source code review– to scan the network, application and hosts by using OWASP Zed Attack Proxy ("ZAP"), Mobile Security Framework ("MobSF") and Fortify Audit Workbench for existing vulnerabilities, opened services, system configurations and source code to facilitate the risk analysis.

The following documents were assessed:

1. Technical Specification Document of LHS

4.3 Asset Identification and Valuation

All information assets within the scope of the assessment were identified.

The importance of the data security was classified into three classes: confidentiality, integrity and availability:

- **Confidentiality** – OGCIO should establish sufficient security controls to safeguard the information assets from being disclosed without proper authorisation.
- **Integrity** – OGCIO is involved in the processing of system data. The information assets must be well protected from unauthorised, unanticipated, or unintentional modification.
- **Availability** – The availability requirement of the system is defined per business users' requirements. High resilience of the application is needed.

This step grouped assets into various groups and valuated them against various factors:

- Value in terms of Confidentiality, Integrity, and Availability

4.4 Threat and Vulnerability Analysis

This step of the assessment identified any threat that might induce harm to the target system or asset. Examples of threats included misuse of computing resource, natural disaster, fraud, theft, cyber attacks or human errors.

In addition, the assessor would identify any vulnerability that would allow threat to occur within the scope of the assessment. Such vulnerability might be found using the information collected in previous stages. The vulnerability identified would also be measured by its exposure and accessibility. Examples of vulnerabilities included operating system loopholes, or flaws in operational practices.

4.5 Asset/Threat/Vulnerability Mapping

The identified vulnerabilities would be mapped to threats and assets within the scope of the assessment. The purpose was to create a mapping/combination of asset vs. threat vs. vulnerability in a logical and meaningful manner that assisted in the upcoming risk analysis step.

4.6 Impact and Likelihood Analysis

Provided with the identified threats and vulnerabilities to various assets, the assessor would assess the impact that might occur. Impact to a specific system or asset might include business loss, loss of goodwill or service level disruption. In addition, the likelihood of the occurrence of a threat was also assessed. In general, higher likelihood usually constituted more risks.

The Contractor analysed impacts to the assets based on the observed threats and vulnerabilities. For the observed material vulnerability, the team assessed its impact to the system, in particular the impact on the data confidentiality, by the potential damage should a security incident occur. Impacts to the information asset might include business service disruption, information leakage, unauthorised information alternation and loss of goodwill. The more severe damage it possibly induced, the greater the impact.

Likelihood was defined by the possibility that a particular security incident could occur. The higher possibility it associated with, the higher the likelihood. This was estimated by expert judgment.

The purpose of the security risk analysis in this stage was to understand the effectiveness of the planned technical security controls in protecting the data security. An assessment on general security risks of OGCIO users was not included in this stage[1]. Furthermore, the security assessment of the future operation security was not included in this stage.

4.7 Risk Modelling Analysis

In this step of the risk assessment, risk was modeled and analysed so that it can be portrayed in a systematic manner. A risk matrix technique was used so that risk can be portrayed for each threat.

1. Risk Rating

A value was assigned to each finding indicating the status of impact and likelihood. The risk level was the results of a combined risk assessment attributed from the potential impacts and the likelihood of occurrence of the finding according to the risk ranking matrix below:

[1]The assessment on the general security risks analysis of OGCIO was according to document review, site visits and discussions.

Risk		Likelihood		
		High 3	Medium 2	Low 1
Impact	High 3	**High 9**	**Medium 6**	**Low 3**
	Medium 2	**Medium 6**	**Medium 4**	**Low 2**
	Low 1	**Low 3**	**Low 2**	**AOI 1**

4.8 Identify and Recommend Controls

The last step of the risk assessment was for the assessor to identify and recommend safeguards or controls that accepted, mitigates, transferred, or eliminated the associated risk depending on the severity. The security improvements would be prioritized based on the severity of identified risks and the value of a specific asset. In achieving this, the assessor might also help to prioritize the controls based on severity of the risk.

5. Security Audit Methodology

The security requirements were defined based on the following inputs:

- Baseline IT Security Policy (S17)
- The HKSARG Interoperability Framework (S18)
- IT Security Guidelines (G3)
- OGCIO IT Security Policy (OITSP)
- Practice Guide for Security Risk Assessment & Audit
- Practice Guide for Penetration Testing
- Practice Guide for Information Security Incident Handling
- Practice Guide for Internet Gateway Security
- Practice Guide for Cloud Computing Security
- Practice Guide for Mobile Security
- Best Practices for Business Analyst
- Effective Systems Analysis and Design Guide
- Practice Guide for Agile Software Development
- Practice Guide for Scoping and Planning of Large-scale IT System Development Projects
- The Government Technology and System Architectures (GTSA) Framework
- Common Look and Feel Guidelines and Design Specifications
- Personal Data (Privacy) Ordinance (Cap 486)
- Six Data Protection Principles issued by the Office of the Privacy Commissioner for Personal Data ("PCPD")
- Code of Practice on the Identity Card Number and other Personal Identifiers issued by the Office of the PCPD
- IoT Security Best Practice Guidelines

5.1 Recommend Controls

For each identified risk and/or area of improvement, the Contractor recommended controls to improve the security level of the system. The recommendations were proposed to fit in OGCIO's IT environment, based on a cost-benefit analysis. Best practices in other government departments, commercial organisations, security guidelines and industry standards were referenced when the team proposed the suitable recommendations for the observed risks or areas of improvement.

According to the severity of the risk, a schedule to implement the recommendations to improve the security of the system is proposed. The risk classification and indicative implementation schedule are given below:

Table 1. Risk classification and indicative implementation schedule

Risk level	Implication and recommendation
H (high)	Means critical impact and improvements should be made immediately
M (medium)	Means moderate impact and improvements should be made within a short time
L (low)	Means low impact and improvements should be made within a reasonable time
AOI (area of improvement)	Does not impose immediate threats but implementation of such items will improve the environment. These enhancements should be implemented when resources are available.

The following security audit activities were performed during the security audit stage:

5.2 Audit Planning

A project schedule was prepared to outline the planning of the security audit.

5.3 Information Gathering

The major tasks performed in the information gathering included document review, site visits, source code review, system configuration reviews and discussions.

5.4 Control Review

The Contractor discussed the follow-up actions with OGCIO on the suggested security controls.

5.5 Audit Tests

The Contractor reviewed the modified technical security controls.

5.6 Audit Reporting

Each assessment finding in the Security Risk Assessment came with a corresponding recommendation. In the security audit stage, the Contractor reviewed the rectification status of the recommendations and discussed the current progress with OGCIO. The individual rectification status could be either:

- **Completed**: the status review found that the recommended safeguard was properly implemented or compensating controls were taken such that the risk was properly rectified.
- **In-Progress**: OGCIO was still implementing recommendations to rectify the risk. Possible reasons were procurement, extended construction work or testing work, as well as involvement of other government departments.
- **Acknowledged:** OGCIO had considered all options of the recommended safeguard and concluded that accepting the security risk was the best choice. Typical reasons for this status were relating to rectification cost/resource justification, or integration to environment(s) that could not be controlled by OGCIO, or risk accepted.

The project team then prepared the findings and analysis results during the security audit.

5.7 Clean Up and Follow Up

After the security audit and verification report were accepted, sensitive information was returned to OGCIO or destroyed. The Contractor used its own laptops to conduct the vulnerability test for the security risk assessment and security audit and no tool was required to be removed. The audit data including the test results such as vulnerability scan results, audit checklists were passed to OGCIO for retention. As there was no improvement needed to be made after the security audit, no follow up action would be required.

6. Security Risk Assessment and Audit Results

Security Risk Assessment (SRA) Findings:

6.1 Source Code Review Findings

There were no findings from the mobile app and website source code, the distribution of those items with corresponding improvement area was:

Risk Level	Number of corresponding risk level
H (High)	0
M (Medium)	0
L (Low)	0
Area of Improvement (AOI)	0
Total number of improvement proposed	**0**

6.2 Penetration/Scanning Test (Website) Findings

The Contractor observed 1 finding from the website, the distribution of those items with corresponding improvement area was:

Risk Level	Number of corresponding risk level
H (High)	0
M (Medium)	0
L (Low)	1
Area of Improvement (AOI)	0
Total number of improvement proposed	**1**

Findings:

Report Title	Risk Level	S17 Area	Findings Description	Recommendation
[redacted]				

6.3 Penetration / Scanning Test (Mobile App) Findings

The Contractor observed a total of 2 findings from the mobile app, the distribution of those items with corresponding improvement area was:

Risk Level	Number of corresponding risk level
H (High)	0
M (Medium)	1
L (Low)	1
Area of Improvement (AOI)	0
Total number of improvement proposed	**2**

Findings:

Report Title	Risk Level	S17 Area	Findings Description	Recommendation
[redacted]				

Security Audit (SA) Findings:

6.4 General Control Review Findings

There were 1 finding from general control review, the distribution of those items with corresponding improvement area was:

Risk Level	Number of corresponding risk level
H (High)	0
M (Medium)	0
L (Low)	1
Area of Improvement (AOI)	0
Total number of improvement proposed	**1**

Findings:

Report Title	Risk Level	S17 Area	Findings Description	Recommendation
[redacted]				

7. Follow-Up Actions

During the assessment, the Contractor analysed the security risks of the System based on the information collected in various activities – configuration review, vulnerability scanning, document review, web application scan and discussion sessions. Each identified threat was associated with a risk level derived based on the potential impacts and the likelihood of occurrences to OGCIO's LHS. For each threat, the Contractor provided recommendations to enhance the security of LHS and to mitigate the potential risk. OGCIO is encouraged to develop an implementation plan to follow up the remaining risk findings according to their priorities. By prioritising the completion of the remaining rectification works, OGCIO could efficiently enhance the information security of LHS.

Appendix I. References

This appendix presents the list of reference materials used in this engagement and the reference materials that OGCIO could refer to in implementing the security safeguards and/or understand this report.

Information Security Standards

- [S17] Baseline IT Security Policy
- The HKSARG Interoperability Framework (S18)
- [G3] IT Security Guidelines
- OGCIO IT Security Policy (OITSP)
- Practice Guide for Security Risk Assessment & Audit
- Practice Guide for Penetration Testing
- Practice Guide for Information Security Incident Handling
- Practice Guide for Internet Gateway Security
- Practice Guide for Cloud Computing Security
- Practice Guide for Mobile Security
- Best Practices for Business Analyst
- Effective Systems Analysis and Design Guide
- Practice Guide for Agile Software Development
- Practice Guide for Scoping and Planning of Large-scale IT System Development Projects
- The Government Technology and System Architectures (GTSA) Framework
- Common Look and Feel Guidelines and Design Specifications
- Personal Data (Privacy) Ordinance (Cap 486)
- Six Data Protection Principles issued by the Office of the PCPD
- Code of Practice on the Identity Card Number and other Personal Identifiers issued by the Office of the PCPD
- IoT Security Best Practice Guidelines

Application Development Guidelines

- SP800-64 Security Considerations in the System Development Life Cycle, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
- Projects/OWASP Development Guide/Releases/Guide 2.0, The Open Web Application Security Project
- Improving Web Application Security: Threats and Countermeasures, Microsoft Corporation http://msdn.microsoft.com/en-us/library/ff649874.aspx
- Security in Development: The IBM Secure Engineering Framework, IBM Corporation, http://www.redbooks.ibm.com/redpieces/pdfs/redp4641.pdf
- Building web application security into your development process: are your web applications vulnerable?

General Security Information

- CERT Coordination Center: A major reporting center for Internet security problems. http://www.cert.org/
- Common Vulnerabilities and Exposures Project: CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. http://www.cve.mitre.org/

- Security Focus: Security Focus is the most comprehensive and trusted source of security information on the Internet. Security Focus is a vendor-neutral site that provides objective, timely and comprehensive security information to all members of the security community, from end users, security hobbyists and network administrators to security consultants, IT Managers, CIOs and CSOs. http://www.securityfocus.com/
- Open Source Web Application Security Project: OWASP creates an open source community where people could advance their knowledge about web application and web services security issues by either contributing their knowledge to the education of others or by learning about the topic from documentation and software produced by the project. http://www.owasp.org/

~~ End of Security Risk Assessment and Audit Report ~~