Omni Channel Business Platform Renewal

Request for Proposal

++
Disclaimer: This document contains confidential and proprietary information. This document may not be reproduced or transmitted to third-parties without the written consent of AEON Credit Service (Asia) Co., Ltd. (ACSA). You are permitted to use this document solely for the stated purpose of responding to ACSA in relation to the suitability of your solution to ACSA requirements. If you do not agree to these conditions please return or destroy all copies of this document and notify the ACSA Point of Contact.
++

DOCUMENTATION DESCRIPTION

Title	Omni Channel business Platform Renewal
Owner	ACSA - IT Division
Document Type	Request for Proposal
Issue Date	July 2025
Version	1.5
Confidentiality	High

REQUEST FOR CLARIFICATION

Your Requests for Clarification must be addressed to ACSA Point of Contact only. ACSA may submit additional questions or requests for clarification by email during the evaluation of your response. All requests shall be directed to your prime contact and shall come from the ACSA Point of Contact.

Name:	Mr. Dave Ng
Address:	20/F, Mira Place Tower A, 132 Nathan Road, Tsim Sha Tsui, Kowloon
City:	Hong Kong
Country:	Hong Kong SAR
Telephone:	+852 - 2239 9723
Email:	Dave.kcng@aeon.com.hk

Name:	Mr. Kelvin Kam
Address:	20/F, Mira Place Tower A, 132 Nathan Road, Tsim Sha Tsui, Kowloon
City:	Hong Kong
Country:	Hong Kong SAR
Telephone:	+852 - 2239 9754
Email:	kelvin.nhkam@aeon.com.hk

Table of Content

SECTION 1 INTRODUCTION

1.1 Introduction

This Request for Proposal (RFP) document is issued by AEON Credit Service (Asia) Company Limited (ACSA), to qualified vendor (hereafter referred to as “you”) to respond to ACSA’s potential requirements for the provision to ACSA of such service and system as set out in this RFP.

1.2 Company Background

ACSA, is a company incorporated in Hong Kong with limited liability, the shares of which are listed on the Stock Exchange (00900.HK).

ACSA is engaged in the consumer finance business, which includes the issuance of credit cards and the provision of personal loan financing and other consumer products, insurance broking and agency business and micro-finance business.

ACSA is also a subsidiary of AEON Financial Service Co., Ltd. ("AFS") and a member of the AEON Group. AFS is listed on the first section of the Tokyo Stock Exchange.

1.3 Purpose of the RFP

This Request for Proposal (RFP) is an invitation to vendors to submit a response for the Omni Channel business platform as outlined within this document. You should consider appropriate services so that you will be able to submit:

1. Responses for the provision of the Revamp Project or services necessary for ACSA based on the services that, in your opinion, are the most appropriate to comply with ACSA’s requirements for the System; and
2. Necessary relevant information.

ACSA may add to or remove any of its requirements from this RFP.

1.4 Principle Requirements

Current Challenges: AEON Credit Service Asia (ACSA) now using the WhatsApp platform is out of capability to perform broadcast promotion, lack of support, and the platform is not cost-effective.

In order to have better communication channel with customer ACSA is looking for a new platform that have the capability to extend to omnichannel solution.

Below are the key guidelines for the vendor in providing the solution:

1. Unified customer profile and interaction history
2. Real-time communication and notifications
3. AI-powered chatbots and automation

4. Analytics and reporting dashboard
5. Multilingual support
6. Role-based access control
7. Marketing message broadcast
8. Integrated Rich media messaging
9. Opt-in / Opt-out preference management
10. Multiple Number handling functionality
11. Channel-Specific QR code
12. Customer interaction queue management
13. Intelligent Agent Routing
14. Supervisor Mode

Below are the requirements of the platform capability

1. Modular Omnichannel Framework (extendable on communication channel)
2. Cloud-based or hybrid deployment
3. API availability for integration
4. Data Security and compliance (e.g PCIDSS is preferred)
5. Mobile responsiveness
6. AD Federation Support

Given the above situation, ACSA is looking for a Solution for revamping the existing omni channel platform. ACSA is open to different types of service arrangement, total solution or package you may propose ACSA, although package solution is preferable.

SECTION 2 INSTRUCTION TO SUPPLIERS

2.1 RFP Process and Project Timeline

The RFP process may be conducted in phases. Key activities and target completion dates are set out below. ACSA may change the phases and time-scales at its sole discretion.

Process/activity	Time-Scale
Clarification	16 Jul – 31 Jul 2025
Proposal Submission	1 Aug 2025
Vendor Demo Presentation	8 – 12 Aug 2025 (TBC)
Proposal Confirmation	Aug 2025 (TBC)
Contract Administration and Project Kickoff	Sep 2025 (TBC)
UAT Complete	Dec 2025 (TBC)
Pilot Run	Jan 2026 (TBC)
Production Launch	Jan 2026 (TBC)

ACSA reserves the right to discontinue the RFP process at any time, and makes no commitments, implied or otherwise, that this RFP process will result in a business transaction with one or more third parties.

2.2 Response

2.2.1 How to response

You should provide a thorough and complete response to each element of every section contained within this RFP. You should ensure that you understand all aspects of the RFP and all other related documents whether a statement of compliance is required or not. You should provide a full supporting explanation against every statement.

Where you are presented with a requirement or are asked to use a specific approach, you should not only state conformity, but also describe, where appropriate, how you intend to conform. Where a statement of non-conformity is provided, you should indicate your reasons and explain your proposed alternative. You should identify any material assumptions made in preparing your proposals in your response. The deferral of a response to a question or issue to the contract negotiation stage is not acceptable.

Where ACSA states a preference for a particular approach, you are encouraged, in addition, to propose an alternative solution, provided you demonstrate that such alternative has either no adverse impact or is more beneficial to ACSA.

2.2.2 Format

When completing this RFP, you should

- Provide a proposal in email in PDF/Word format with your responses to each item stated in Section 4, 5 & 6 and the detail of your proposed solution. A **compliance table** is required.

Your responses should be sent to the ACSA Point of Contact in printed copy with the filled out RFP attached.

2.2.3 Vendor Presentation Guidelines

Shortlisted vendor will be expected to present their responses in person at the ACSA offices at:

Address: 20/F, Mira Place Tower A, 132 Nathan Road, Tsim Sha Tsui, Kowloon, Hong Kong

Selected vendor will have two (2) hours in which to present their response. All presentation materials should be submitted before the presentation 1 week in advance. Each vendor will present their proposed solution; indicate their acceptance or deviation of ACSA's preferences. If the respondent determines that there is a better (more cost effective or significantly higher quality) solution, they are free to present that solution at this time as well as during the written response. However, the respondent must be prepared to indicate why the proposed solution is better and what, if any, benefits ACSA would enjoy as a result of accepting the solution. ACSA will not tolerate presentations that have negative content about the other respondents.

2.2.4 Demo Session

The vendor is expected to provide a Demo to ACSA according to the schedule. The scope will be provided by ACSA based on the high-level requirement of the Omni Channel Business Platform. Basic integration and setup are expected.

The demo session offers a valuable opportunity to explore the vendor's skills, creativity, and how well they align with ACSA's distinctive style and collaborative work ethic**.**

2.2.5 Commitments to the Response

The initial response to this RFP must be signed by a person in your organization with authority to commit to all information specified by you in your responses. Details of that person's position within your organization must be provided.

2.2.6 RFP Preparation Costs

You will assume all responsibilities and costs incurred in providing responses to this RFP and for providing any additional information (i.e. pre-requisite assets, tools) required by ACSA to facilitate the evaluation process and the RFP process generally. You will also assume all costs you incur during the process of contract development and negotiation.

2.3 *Confidentiality & Publicity*

2.3.1 *Confidentiality*

This RFP is confidential and the property of ACSA. You can disclose relevant parts of the RFP to partners and/or sub-contractors provided that the partners and/or sub-contractors first execute a non-disclosure agreement identical to the non-disclosure agreement signed by you. Distribution or sharing of this RFP by you with any other parties must be approved in writing by ACSA beforehand. You will continue to be bound by the non-disclosure agreement previously signed with ACSA.

2.3.2 *Publicity*

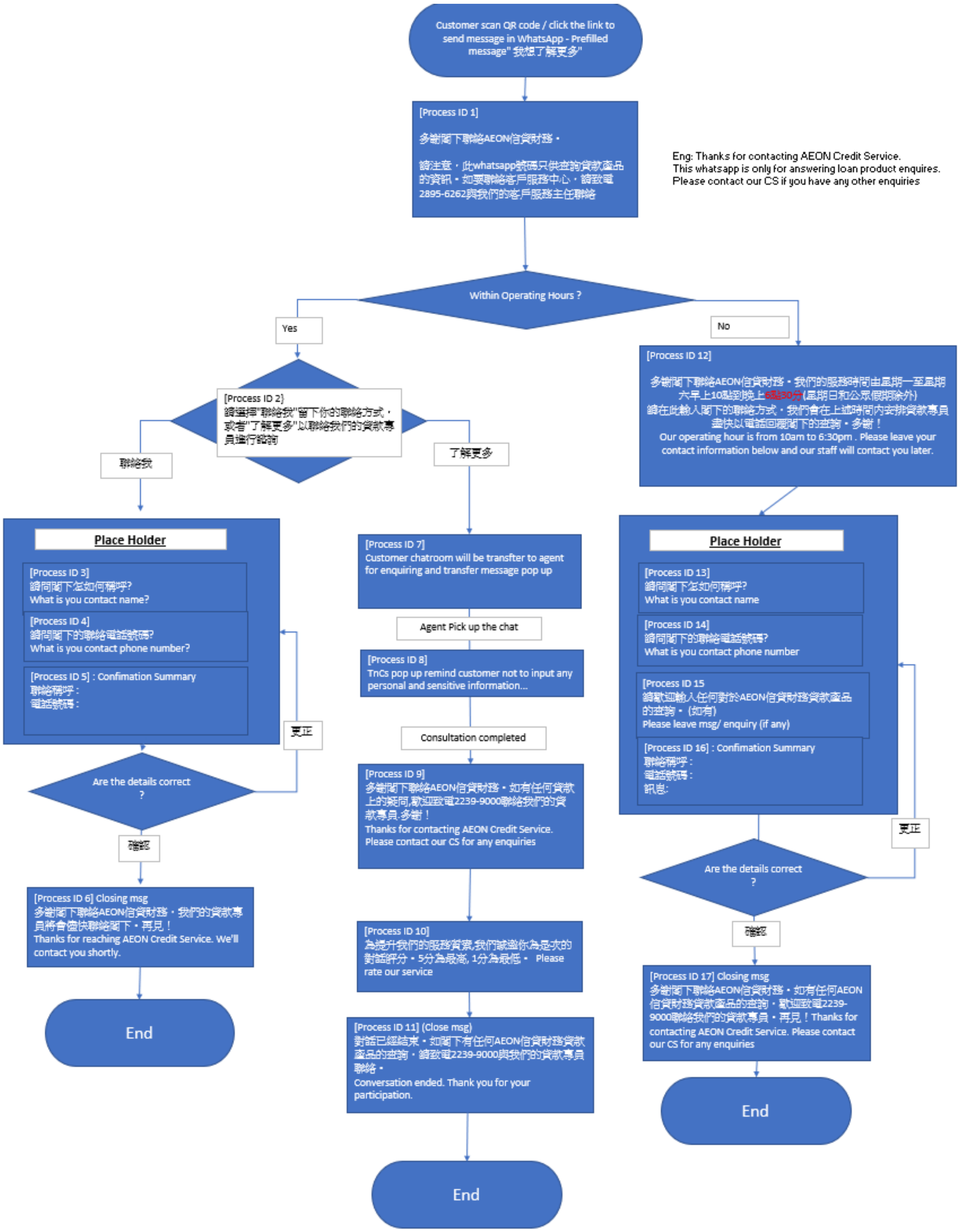
Publicity releases pertaining to the RFP, ACSA or to any of the ACSA businesses, products and/or services referenced in the RFP, will not be made without prior written approval from ACSA. No results of this RFP process are to be released without ACSA's prior written consent, and then only to designated individuals.

2.4 *Contractual Arrangements*

This RFP is not and should not be taken as intent to purchase goods or services. Rather, the vendor is being invited to submit a proposal at your own expense and volition. ACSA accepts no liability for time, property or material cost expended in the provision of a proposal. ACSA reserves the right to request you to comply to its terms and conditions if applicable.

SECTION 3 EXISTING WORKFLOW

3.1 Telemarketing Flow



Customer scan QR code / click the link to send message in WhatsApp - Prefilled message" 我想了解更多"

[Process ID 1]

多謝閣下聯絡AEON信貸財務。

請注意，此whatsapp號碼只供查詢貸款產品的資訊。如要聯絡客戶服務中心，請致電2895-6262與我們的客戶服務主任聯絡

Eng: Thanks for contacting AEON Credit Service.
This whatsapp is only for answering loan product enquires.
Please contact our CS if you have any other enquiries

[Process ID 2]
請選擇"聯絡我"留下你的聯絡方式，或者"了解更多"以聯絡我們的貸款專員進行諮詢

[Process ID 3]
請問閣下怎如何稱呼?
What is you contact name?

[Process ID 4]
請問閣下的聯絡電話號碼?
What is you contact phone number?

[Process ID 5] : Confimation Summary
聯絡稱呼：
電話號碼：

[Process ID 6] Closing msg
多謝閣下聯絡AEON信貸財務。我們的貸款專員將會儘快聯絡閣下。再見！
Thanks for reaching AEON Credit Service. We'll contact you shortly.

[Process ID 7]
Customer chatroom will be transfter to agent for enquiring and transfer message pop up

[Process ID 8]
TnCs pop up remind customer not to input any personal and sensitive information...

[Process ID 9]
多謝閣下聯絡AEON信貸財務。如有任何貸款上的疑問,歡迎致電2239-9000聯絡我們的貸款專員.多謝！
Thanks for contacting AEON Credit Service.
Please contact our CS for any enquiries

[Process ID 10]
為提升我們的服務質素,我們誠邀你為是次的對話評分。5分為最高, 1分為最低。 Please rate our service

[Process ID 11] (Close msg)
對話已經結束。如閣下有任何AEON信貸財務貸款產品的查詢，請致電2239-9000與我們的貸款專員聯絡。
Conversation ended. Thank you for your participation.

[Process ID 12]

多謝閣下聯絡AEON信貸財務。我們的服務時間由星期一至星期六早上10點到晚上6點30分(星期日和公眾假期除外)
請在此輸入閣下的聯絡方式，我們會在上述時間內安排貸款專員盡快以電話回覆閣下的查詢。多謝！
Our operating hour is from 10am to 6:30pm . Please leave your contact information below and our staff will contact you later.

[Process ID 13]
請問閣下怎如何稱呼?
What is you contact name

[Process ID 14]
請問閣下的聯絡電話號碼?
What is you contact phone number

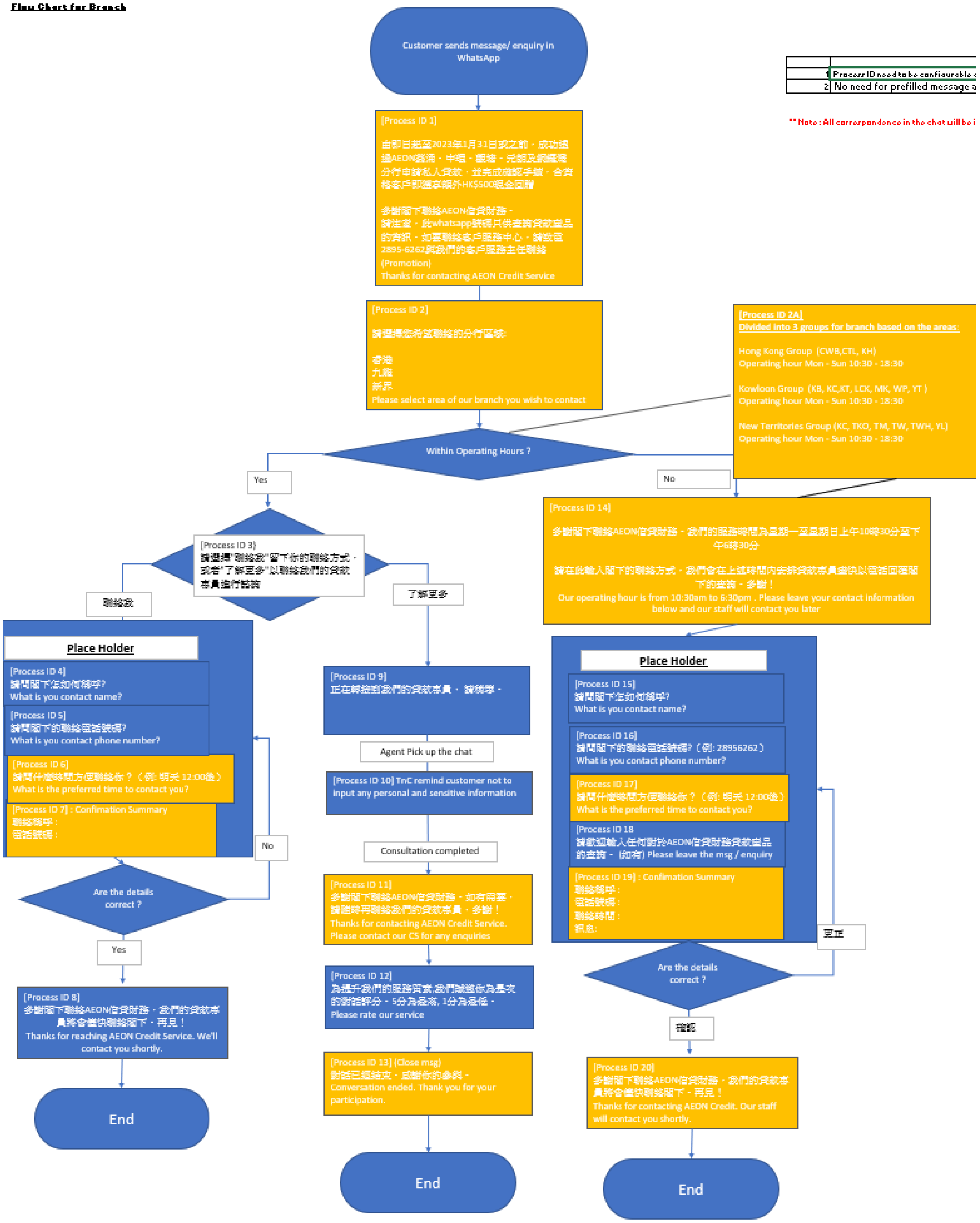
[Process ID 15
請歡迎輸入任何對於AEON信貸財務貸款產品的查詢。(如有)
Please leave msg/ enquiry (if any)

[Process ID 16] : Confimation Summary
聯絡稱呼：
電話號碼：
訊息:

[Process ID 17] Closing msg
多謝閣下聯絡AEON信貸財務。如有任何AEON信貸財務貸款產品的查詢，歡迎致電2239-9000聯絡我們的貸款專員。再見！Thanks for contacting AEON Credit Service. Please contact our CS for any enquiries

3.2 Branch Flow

Flow Chart for Branch



[Process ID 1]

由即日起至2023年1月31日或之前，成功透過AEON荃灣、中環、旺角、元朗及將軍澳分行申請私人貸款，並完成提款手續，合資格客戶即獲享額外HK$500現金回贈

多謝閣下聯絡AEON信貸財務。
請注意，此whatsapp號碼只供查詢貸款產品的資訊，如要聯絡客戶服務中心，請致電2895-6262與我們的客戶服務主任聯絡
(Promotion)
Thanks for contacting AEON Credit Service

[Process ID 2]

請選擇您希望聯絡的分行區域:

香港
九龍
新界
Please select area of our branch you wish to contact

[Process ID 2A]
Divided into 3 groups for branch based on the areas:

Hong Kong Group (CWB,CTL, KH)
Operating hour Mon - Sun 10:30 - 18:30

Kowloon Group (KB, KC,KT, LCK, MK, WP, YT)
Operating hour Mon - Sun 10:30 - 18:30

New Territories Group (KC, TKO, TM, TW, TWH, YL)
Operating hour Mon - Sun 10:30 - 18:30

[Process ID 3]
請選擇"聯絡我"留下你的聯絡方式，或者"了解更多"以聯絡我們的貸款專員進行諮詢

[Process ID 4]
請問閣下怎如何稱呼?
What is you contact name?

[Process ID 5]
請問閣下的聯絡電話號碼?
What is you contact phone number?

[Process ID 6]
請問什麼時間方便聯絡你？（例: 明天 12:00後）
What is the preferred time to contact you?

[Process ID 7] : Confimation Summary
聯絡稱呼 :
電話號碼 :

[Process ID 8]
多謝閣下聯絡AEON信貸財務，我們的貸款專員將會儘快聯絡閣下，再見！
Thanks for reaching AEON Credit Service. We'll contact you shortly.

[Process ID 9]
正在轉接到我們的貸款專員， 請稍候。

[Process ID 10] TnC remind customer not to input any personal and sensitive information

[Process ID 11]
多謝閣下聯絡AEON信貸財務，如有需要，請隨時再聯絡我們的貸款專員，多謝！
Thanks for contacting AEON Credit Service.
Please contact our CS for any enquiries

[Process ID 12]
為提升我們的服務質素,我們誠邀你為是次的對話評分，5分為最高, 1分為最低。
Please rate our service

[Process ID 13] (Close msg)
對話已經結束，感謝你的參與。
Conversation ended. Thank you for your participation.

[Process ID 14]

多謝閣下聯絡AEON信貸財務，我們的服務時間為星期一至星期日上午10時30分至下午6時30分

請在此輸入閣下的聯絡方式，我們會在上述時間內安排貸款專員盡快以電話回覆閣下的查詢，多謝！
Our operating hour is from 10:30am to 6:30pm . Please leave your contact information below and our staff will contact you later

[Process ID 15]
請問閣下怎如何稱呼?
What is you contact name?

[Process ID 16]
請問閣下的聯絡電話號碼?（例: 28956262）
What is you contact phone number?

[Process ID 17]
請問什麼時間方便聯絡你？（例: 明天 12:00後）
What is the preferred time to contact you?

[Process ID 18
請歡迎輸入任何關於AEON信貸財務貸款產品的查詢。 (如有) Please leave the msg / enquiry

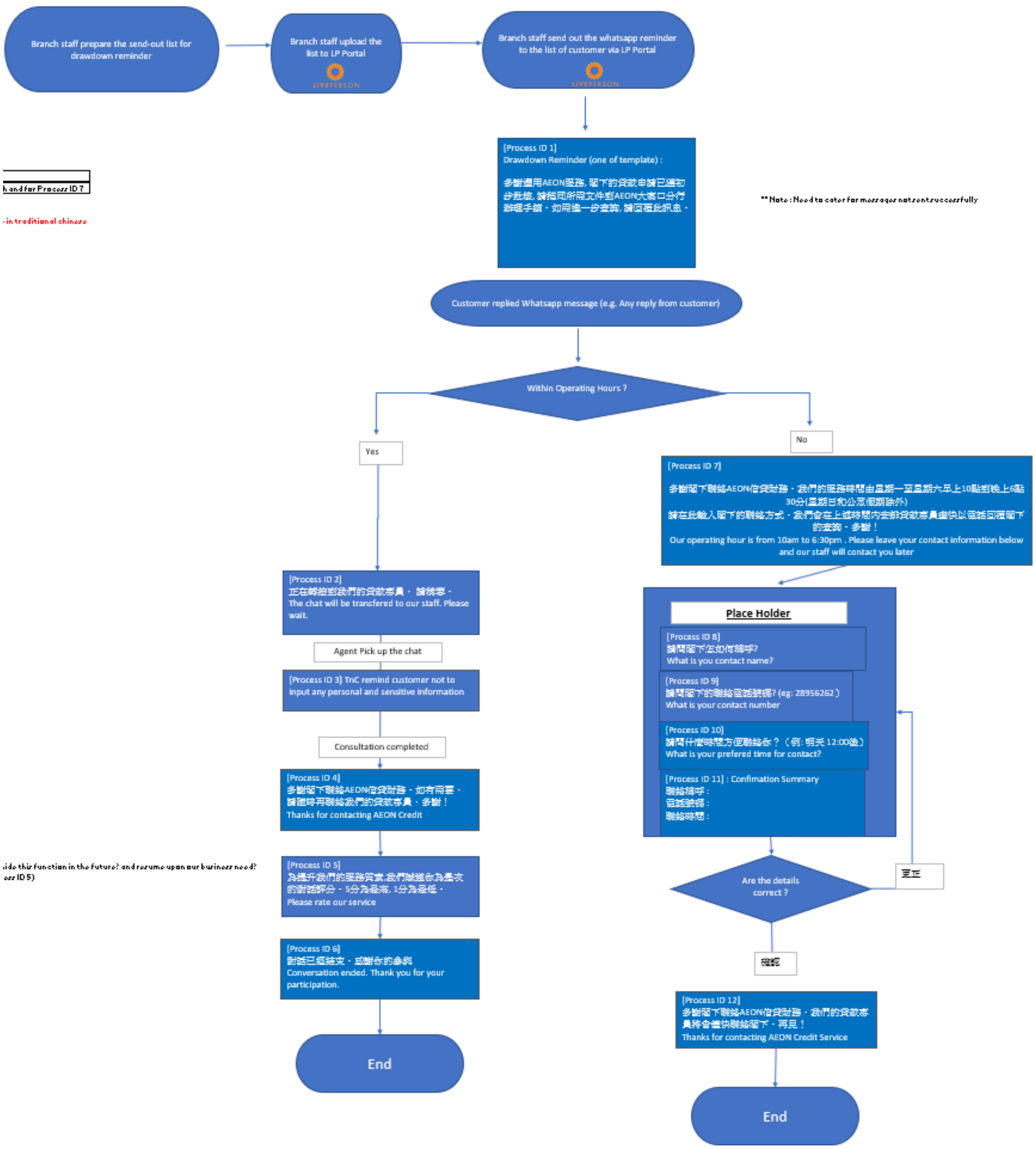
[Process ID 19] : Confimation Summary
聯絡稱呼 :
電話號碼 :
聯絡時間 :
訊息:

[Process ID 20]
多謝閣下聯絡AEON信貸財務，我們的貸款專員將會儘快聯絡閣下，再見！
Thanks for contacting AEON Credit. Our staff will contact you shortly.

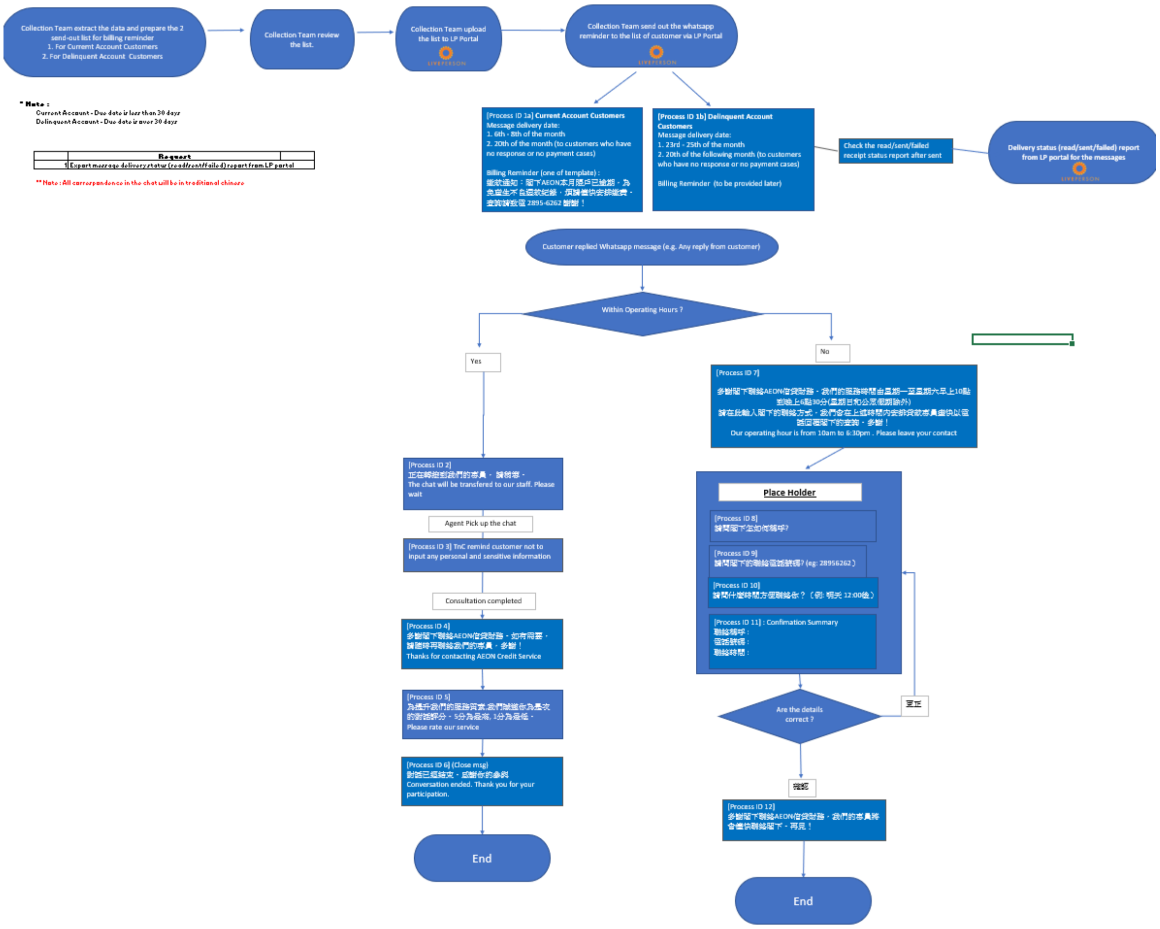
1	Process ID need to be configurable c
2	No need for prefilled message a

** Note : All correspondence in the chat will be i

3.3 Loan Drawdown Reminder Flow


Branch staff prepare the send-out list for drawdown reminder
Branch staff upload the list to LP Portal
LIVEPERSON
Branch staff send out the whatsapp reminder to the list of customer via LP Portal
LIVEPERSON
[Process ID 1]
Drawdown Reminder (one of template) :
多謝選用AEON服務, 閣下的貸款申請已經初步批核, 請攜同所需文件到AEON大客口分行辦理手續。如需進一步查詢, 請回覆此訊息。
h and for Process ID 7
· in traditional chinese
** Note : Need to cater for messages not sent successfully
Customer replied Whatsapp message (e.g. Any reply from customer)
Within Operating Hours ?
Yes
No
[Process ID 7]
多謝閣下聯絡AEON信貸財務。我們的服務時間由星期一至星期六早上10點到晚上6點30分(星期日和公眾假期除外)
請在此輸入閣下的聯絡方式，我們會在上述時間內安排貸款專員盡快以電話回覆閣下的查詢。多謝！
Our operating hour is from 10am to 6:30pm . Please leave your contact information below and our staff will contact you later
[Process ID 2]
正在轉接到我們的貸款專員， 請稍等。
The chat will be transfered to our staff. Please wait.
Agent Pick up the chat
[Process ID 3] TnC remind customer not to input any personal and sensitive information
Consultation completed
[Process ID 4]
多謝閣下聯絡AEON信貸財務，如有需要，請隨時再聯絡我們的貸款專員，多謝！
Thanks for contacting AEON Credit
ide this function in the future? and resume upon our business need?
ess ID 5)
[Process ID 5]
為提升我們的服務質素,我們誠邀你為是次的對話評分。5分為最高, 1分為最低。
Please rate our service
[Process ID 6]
對話已經結束。感謝你的參與
Conversation ended. Thank you for your participation.
End
Place Holder
[Process ID 8]
請問閣下怎如何稱呼?
What is you contact name?
[Process ID 9]
請問閣下的聯絡電話號碼? (eg: 28956262）
What is your contact number
[Process ID 10]
請問什麼時間方便聯絡你？（例: 明天 12:00後）
What is your prefered time for contact?
[Process ID 11] : Confimation Summary
聯絡稱呼：
電話號碼：
聯絡時間：
Are the details correct ?
更正
確認
[Process ID 12]
多謝閣下聯絡AEON信貸財務，我們的貸款專員將會盡快聯絡閣下，再見！
Thanks for contacting AEON Credit Service
End

3.4 Collection Flow



Collection Team extract the data and prepare the 2 send-out list for billing reminder
1. For Curremt Account Customers
2. For Delinquent Account Customers

Collection Team review the list.

Collection Team upload the list to LP Portal

Collection Team send out the whatsapp reminder to the list of customer via LP Portal

* Note :
Current Account - Due date is less than 30 days
Delinquent Account - Due date is over 30 days

	Request	
1	Export message delivery status (read/sent/failed) report from LP portal	

** Note : All correspondence in the chat will be in traditional chinese

[Process ID 1a] **Current Account Customers**
Message delivery date:
1. 6th - 8th of the month
2. 20th of the month (to customers who have no response or no payment cases)

Billing Reminder (one of template) :
繳款通知：閣下AEON本月賬戶已逾期，為免產生不良還款紀錄，煩請儘快安排繳費。查詢請致電 2895-6262 謝謝！

[Process ID 1b] Delinquent Account Customers
Message delivery date:
1. 23rd - 25th of the month
2. 20th of the following month (to customers who have no response or no payment cases)

Billing Reminder (to be provided later)

Check the read/sent/failed receipt status report after sent

Delivery status (read/sent/failed) report from LP portal for the messages

Customer replied Whatsapp message (e.g. Any reply from customer)

Within Operating Hours ?

Yes

[Process ID 2]
正在轉接到我們的專員， 請稍等。
The chat will be transfered to our staff. Please wait

Agent Pick up the chat

[Process ID 3] TnC remind customer not to input any personal and sensitive information

Consultation completed

[Process ID 4]
多謝閣下聯絡AEON信貸財務，如有需要，請隨時再聯絡我們的專員，多謝！
Thanks for contacting AEON Credit Service

[Process ID 5]
為提升我們的服務質素,我們誠邀你為是次的對話評分，5分為最高, 1分為最低。
Please rate our service

[Process ID 6] (Close msg)
對話已經結束，感謝你的參與
Conversation ended. Thank you for your participation.

End

No

[Process ID 7]

多謝閣下聯絡AEON信貸財務，我們的服務時間由星期一至星期六早上10點至晚上6點30分(星期日和公眾假期除外)
請在此輸入閣下的聯絡方式，我們會在上述時間內安排貸款專員盡快以電話回覆閣下的查詢，多謝！
Our operating hour is from 10am to 6:30pm . Please leave your contact

Place Holder

[Process ID 8]
請問閣下怎如何稱呼?

[Process ID 9]
請問閣下的聯絡電話號碼? (eg: 28956262）

[Process ID 10]
請問什麼時間方便聯絡你？（例: 明天 12:00後）

[Process ID 11] : Confimation Summary
聯絡稱呼：
電話號碼：
聯絡時間：

Are the details correct ?

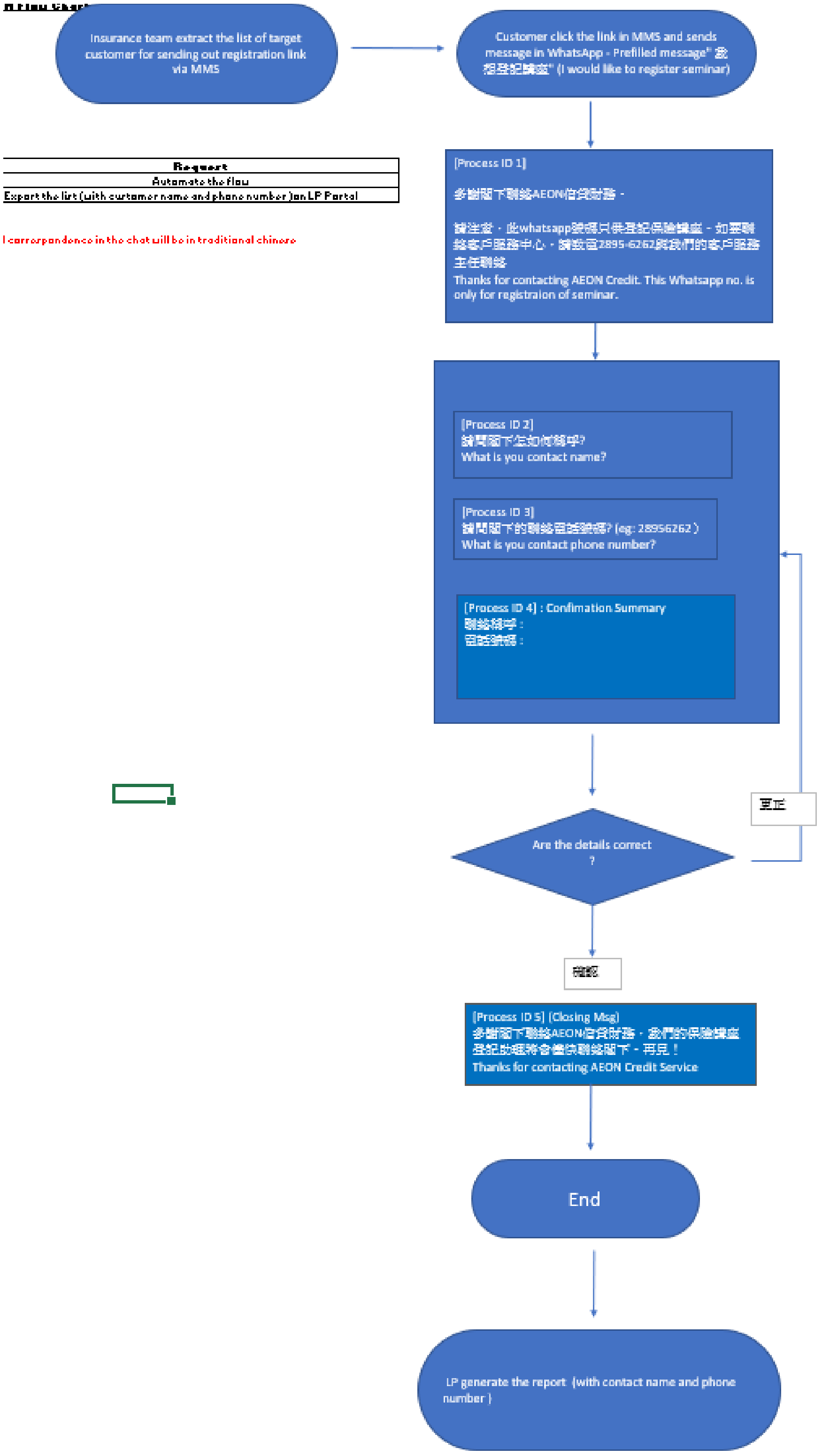
更正

確認

[Process ID 12]
多謝閣下聯絡AEON信貸財務，我們的專員將會儘快聯絡閣下，再見！

End

3.5 Seminar Registration Flow



Insurance team extract the list of target customer for sending out registration link via MMS

Customer click the link in MMS and sends message in WhatsApp - Prefilled message" 我想登記講座" (I would like to register seminar)

[Process ID 1]

多謝閣下聯絡AEON信貸財務。

請注意，此whatsapp號碼只供登記保險講座。如需聯絡客戶服務中心，請致電2895-6262與我們的客戶服務主任聯絡

Thanks for contacting AEON Credit. This Whatsapp no. is only for registraion of seminar.

[Process ID 2]
請問閣下應如何稱呼?
What is you contact name?

[Process ID 3]
請問閣下的聯絡電話號碼? (eg: 28956262）
What is you contact phone number?

[Process ID 4] : Confimation Summary
聯絡稱呼：
電話號碼：

Are the details correct ?

[Process ID 5] (Closing Msg)
多謝閣下聯絡AEON信貸財務，我們的保險講座登記助理將會儘快聯絡閣下。再見！
Thanks for contacting AEON Credit Service

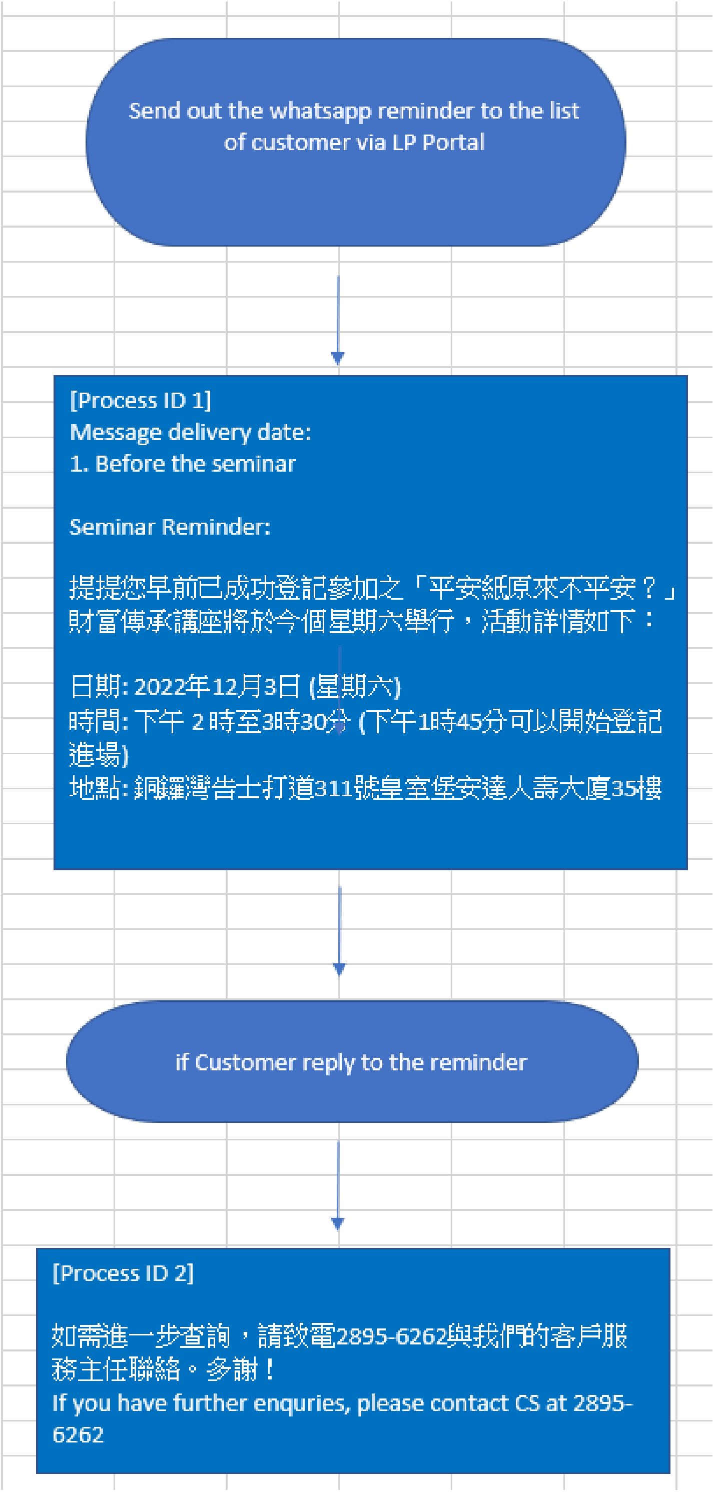
End

LP generate the report (with contact name and phone number)

Request
Automate the flow
Export the list (with customer name and phone number)on LP Portal

l correspondence in the chat will be in traditional chinese

3.6 Seminar Reminder Flow



Send out the whatsapp reminder to the list of customer via LP Portal

[Process ID 1]
Message delivery date:
1. Before the seminar

Seminar Reminder:

提提您早前已成功登記參加之「平安紙原來不平安？」財富傳承講座將於今個星期六舉行，活動詳情如下：

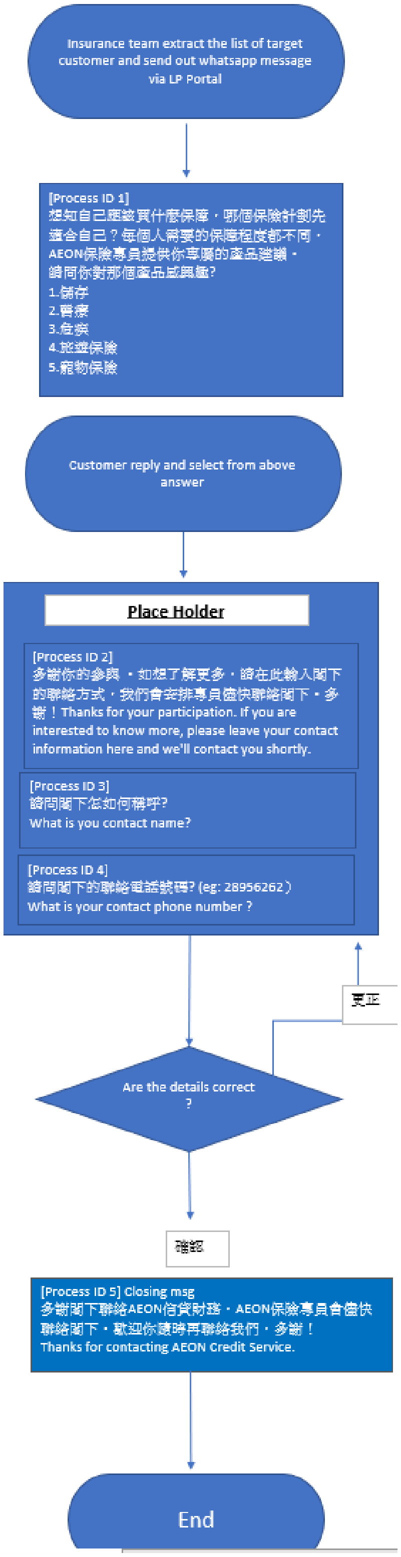
日期: 2022年12月3日 (星期六)
時間: 下午 2 時至3時30分 (下午1時45分可以開始登記進場)
地點: 銅鑼灣告士打道311號皇室堡安達人壽大廈35樓

if Customer reply to the reminder

[Process ID 2]

如需進一步查詢，請致電2895-6262與我們的客戶服務主任聯絡。多謝！
If you have further enquries, please contact CS at 2895-6262

3.7 *Insurance Questionnaire Flow*



Insurance team extract the list of target customer and send out whatsapp message via LP Portal

[Process ID 1]
想知自己應該買什麼保障・哪個保險計劃先適合自己？每個人需要的保障程度都不同・AEON保險專員提供你專屬的產品建議・
請問你對那個產品感興趣?
1.儲存
2.醫療
3.危疾
4.旅遊保險
5.寵物保險

Customer reply and select from above answer

[Process ID 2]
多謝你的參與 ・如想了解更多・請在此輸入閣下的聯絡方式・我們會安排專員儘快聯絡閣下・多謝！Thanks for your participation. If you are interested to know more, please leave your contact information here and we'll contact you shortly.

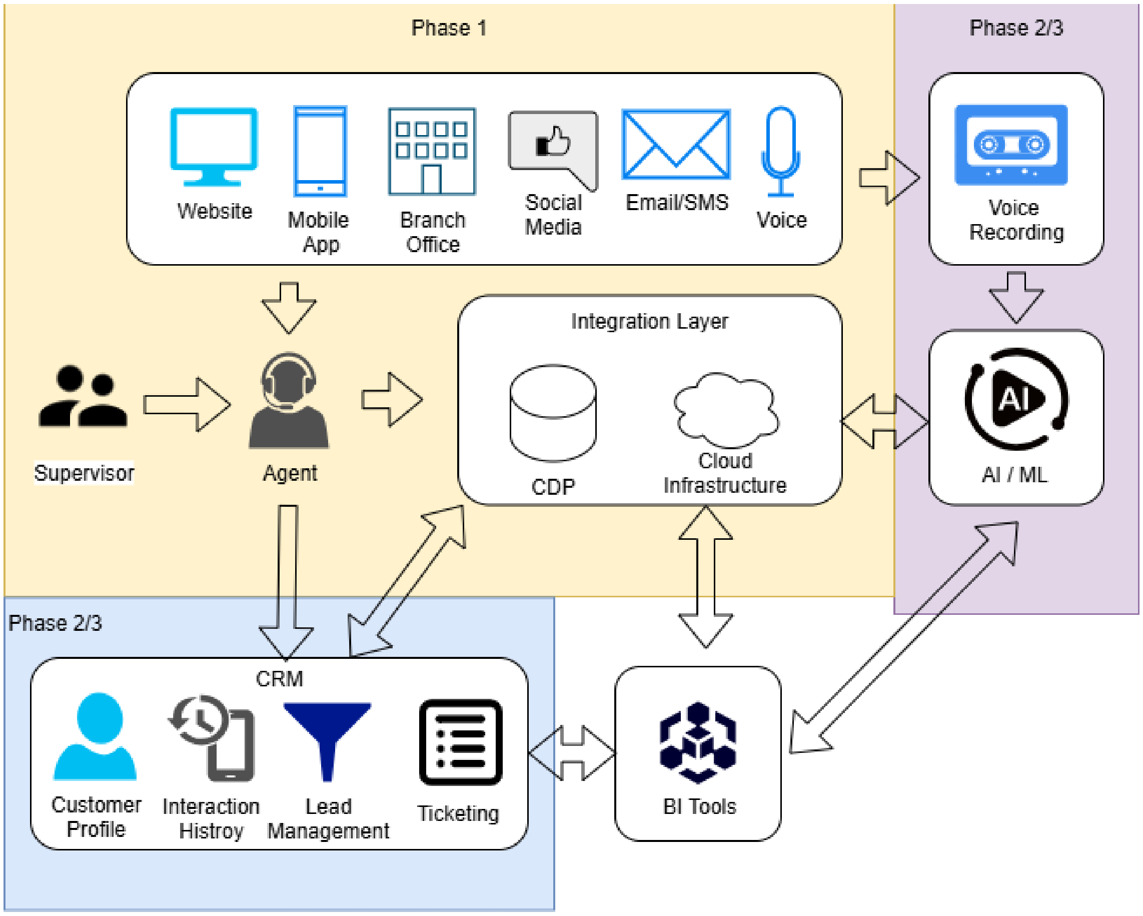
[Process ID 3]
請問閣下怎如何稱呼?
What is you contact name?

[Process ID 4]
請問閣下的聯絡電話號碼? (eg: 28956262）
What is your contact phone number ?

[Process ID 5] Closing msg
多謝閣下聯絡AEON信貸財務・AEON保險專員會儘快聯絡閣下・歡迎你隨時再聯絡我們・多謝！
Thanks for contacting AEON Credit Service.

SECTION 4 DETAILS OF PROJECT REQUIREMENTS

4.1 Expected New Environment



The diagram provided represents a comprehensive roadmap of the omni-channel CRM system, illustrating all essential components required for a modern, integrated customer engagement platform. Vendors are expected to propose and include all necessary modules and capabilities to support a fully functional omni-channel environment.

ACSA will implement the system in phased onboarding, and awarding one phase of the project does not guarantee entitlement to subsequent phases. Therefore, vendors must ensure that their solutions are modular and interoperable, with robust API integration capabilities to seamlessly connect with other components and systems across different phases.

4.2 Functional Requirement Description

You are required to response the requirements for Judgement Workflow based on the below format:

RQ#	Function	Fully Comply (F) / Can be customized (C)/ Not included (N)	Response Details

Req. No.	Title	Description	Mandatory / Optional	Workflow
BRQ1	Channel integration	Seamless transition between: -Mobile apps -Web portals -Chatbots and virtual assistants	Mandatory	
BRQ2	Channel integration	- Supports RESTful API integration with custom-built CRM systems, enabling secure data exchange and real-time synchronization of customer records and workflows. - Facilitates API-based connectivity with proprietary Core Systems, ensuring interoperability through standardized protocols (e.g., REST, SOAP) and robust authentication mechanisms.	Mandatory	
BRQ3	Real-Time Communication	Instant messaging and notifications across channels Support and not limited to -WhatsApp -WeChat -Instagram -Facebook message -Chatbot -Mobile app	Mandatory	
BRQ4	Real-Time Communication	Support alerts on -SMS -email -push notifications (if applicable) -in-app alerts (if applicable)	Mandatory	
BRQ5	Real-Time Communication	Capability to integrate live chatbot to webpage/mobile app	Mandatory	
BRQ6	Real-Time Communication	Promotional message blasting across different channels	Mandatory	
BRQ7	Personalization Engine	Dynamic content delivery tailored to user segments	Mandatory	

Req. No.	Title	Description	Mandatory / Optional	Workflow
BRQ8	Personalization Engine	AI-driven chatbot that will automatic suggest related answer or predefined prompt.	Mandatory	
BRQ9	Personalization Engine	Multi-media support on message	Mandatory	
BRQ10	Unified Customer profile	Centralized customer chat history across all channels	Mandatory	
BRQ11	Security & Compliance	Implementation of Multi-Factor Authentication (MFA) on administrator web console, leveraging protocols such as TOTP, SMS, and biometric verification for enhanced security.	Mandatory	
BRQ12	Security & Compliance	End-to-end encryption and secure APIs	Mandatory	
BRQ13	Security & Compliance	Compliance with financial regulations E.g. HKMA, PCIDSS	Mandatory	
BRQ14	Chat Management	Unified chat history view Unified chat windows for multiple phone numbers	Mandatory	
BRQ15	Chat Management	Cross-channel chat initiation and tracking	Mandatory	
BRQ16	Chat Management	Chat Queue management and chat assign function	Mandatory	

Req. No.	Title	Description	Mandatory / Optional	Workflow
BRQ17	Chat Management	Multiple contact number for separate team and product		
BRQ18	Analytics & Reporting	Cross-channel performance dashboard -including Active/pending chats -agent availability	Mandatory	
BRQ19	Analytics & Reporting	Customer journey mapping and funnel analysis	Mandatory	
BRQ20	Scalability & Flexibility	Modular architecture to support new channels	Mandatory	
BRQ21	Scalability & Flexibility	Cloud-native infrastructure / On-premises solution	Optional	
BRQ22	Scalability & Flexibility	API-first design for third-party integrations	Mandatory	

4.3 Non-Functional Requirement Description

You are required to response the requirements for System, Infrastructure and Operation based on the list below:

Ref#	Control	Control can be implemented Control can be partially implemented Control cannot be implemented Control not applicable Others-please specify	Remark

Ref	Category	Control	Requirement	Expected Proof	Layer
1	Account Management	Enforce a Role-based Access Control	Enforces a **role-based access control** policy over defined subjects and objects to restrict information system access to authorized users. The application should clearly define different type of user roles and responsibilities with following principles 1. Segregation of duties (addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion) 2. Least privilege (allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions) The defined **roles and rights matrix** MUST be prepared by project requestor, reviewed and approved by project manager and business unit leader	To provide the roles and rights matrix, or user access matrix (UAM) in both application and infrastructure layer	**Application, Administration Portal-if any, OS, Database,** Network Device, Management Portal for Internal-if any,

Ref	Category	Control	Requirement	Expected Proof	Layer
2	Account Management	Enfore Unique Account to Provide Individual Accountability	Each user MUST use **unique** account (same as [PCI 8.1.1]). [PCI 8.5] Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components. In case group account will be used for non-administrative activities, an individual owner must be able to be assigned to the group account, usage history (user/ operation contents) shall be specified. [ACSA Requirement] Procedures for approval of granting ID/account and privileged rights shall be defined. User ID must be individually requested for approval to allow the employee to use the systems.	To provide **designed method** and **implementation evidence** for account uniqueness in both application and infrastructure layer, otherwise provide justification. To provide account management **procedure** and record in both application and infrastructure layer	**Application, Administration Portal-if any, OS, Database,** Network Device, Management Portal for Internal-if any,
3	Account Management	Function to Support Identity Lifecycle Management	The application must support identity / user lifecycle management function (e.g., provisioning / create user, de-provisioning/ delete / remove / disable user and role-change / update user) (same as [PCI 8.1.2])	To provide **designed method** and **implementation evidence** of account / identity lifecycle management function in application layer.	**Application, Administration Portal-if any,**
4	Account Management	Capability to Manage Privileged Account	[ACSA Requirement] All Application, Operating Systems (OS), Network Devices and Databases administration / privileged account / password should be kept and managed via CyberArk or equivalent solution, where applicable.	Privileged account should be managed by **ACSA's CyberArk**, vendor shall provide the account list to ACSA for central management. Otherwise, provide justification to ACSA on any constraint or limitation.	**Application, Administration Portal-if any, OS, Database,** Network Device, Management Portal for Internal-if any,
6	Account Management	Remove or Avoid Default Password	[PCI 2.1] Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. [ACSA Requirement] This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.). If wireless connection used in the solution:	To provide the set of default / development credentials (usage component, ID, password) .	**Application, Administration Portal-if any, OS, Database,** Network Device, Manageme

Ref	Category	Control	Requirement	Expected Proof	Layer
			- [PCI 2.1.1] For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.		nt Portal for Internal-if any, **Cloud,**
7	Access Control	Account Expiration	[PCI 8.1.4] Remove/disable inactive user accounts within 90 days. [ACSA Requirement] Access right deletion shall be done in a quick manner as soon as it becomes unnecessary. The solution should be technically support the expiration setup or account disable automatically.	To provide **defined policy / configuration** of automatic account expiration in both application layer and infrastructure layer. Otherwise, provide justification to ACSA on any constraint or limitation.	**Application, Administration Portal-if any, OS, Database,** Network Device, Management Portal for Internal-if any,
8	Access Control	Unused Account Revoke	[PCI 8.1.3] Immediately revoke access for any terminated users. - at least within six months of termination - for both local and remote access - the ID need to be deactivated or removed from the access list [ACSA Requirement] Access right deletion shall be done in a quick manner as soon as it becomes unnecessary. The solution should be technically support detect and remove unused account after certain period automatically.	To provide account management **procedure** (e.g., account valid period/condition) **for removing** unused account in both application layer and infrastructure layer	**Application, Administration Portal-if any, OS, Database,** Network Device, Management Portal for Internal-if any,
9	Access Control	User List Report Generation	The application MUST support: - regularly generation of user access right list and change history for responsible personnel review	Design the function of regularly generation of user access right list (able to map to UAM) and change history for supporting account review. To provide the: **- report samples** and **- usage procedures** of schedule job setup / function	**Application, Administration Portal-if any,**

Ref	Category	Control	Requirement	Expected Proof	Layer
10	Access Control	Access Right Review Process	Establish **access right review** process. Proper actions must be taken for inappropriate, unauthorized or suspicious access rights in order to ensure access control security is maintained over time.	N/A. Account review handled by ACSA infrastructure team	**Application, Administration Portal-if any, OS, Database,** Network Device, Management Portal for Internal-if any,
12	Access Control	Authentication - Infrastructure Level	**Multi-Factor Authentication (MFA)** with other communication channels such as text message to mobile phone or email shall be implemented, such as (same as [PCI 8.2]): Optionally, in addition to basic authentication by ID and password, physical or logical security tokens, smart cards, certificates, etc., authentication shall be implemented. [PCI 8.6] Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. [PCI 8.3.1] Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	Infrastructure should **integrate with MFA**. Utilise ACSA current solution (NetIQ). Otherwise, provide justification to ACSA on any constraint or limitation.	**OS,** Management Portal for Internal-if any,
13	Access Control	Authentication for High Risk Transaction	For Internet banking, require 2FA at least once to authenticate customers' identity for each login session before performing high-risk transactions. High-risk transactions should cover, at least, high-risk funds transfers, which include: (i) funds transfers to third-party payees that have not been registered by the customers; (ii) bill payments to merchants that have been classified by ACSA as high-risk merchants but where the payees have not been registered by the customers; and (iii) transactions that effectively allow online transfers of customers' eligible monetary or non-monetary benefits or interests (e.g. credit card rewards points), directly or through conversion/redemption (including via ACSA's corporate websites), to third parties that have not been registered by the customers.	**Screenshot** of implemented extra authentication page and **description** of authentication logic for high risk transaction in application layer. The threshold of high risk transaction should be confirmed with project owner. If not applicable, please provide justification	**Application, Administration Portal-if any,**

Re f	Category	Control	Requirement	Expected Proof	Layer
17	Access Control	Anti-Brute Force - Infrastructure Level	**Anti-brute force** mechanism to protect against unauthorized access, using (same as [PCI 8.1.6] [PCI 8.1.7]): - Captcha, OR - Follow ACSA AD setting: 1. Account lockout duration: 30 minutes 2. Account lockout threshold: 5 invalid logon attempts 3. Reset account lockout counter after: 30 minutes [PCI 8.1.6] Limit repeated access attempts by locking out the user ID after not more than six attempts. [PCI 8.1.7] Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	Apply ACSA SSO or AD authentication to follow ACSA AD account management. Otherwise to provide the configuration / policy (follow ACSA AD setting) of anti-brute force protection in infrastructure layer or provide justification to ACSA on any constraint or limitation.	**OS, Database,** Network Device, Management Portal for Internal-if any,
18	Access Control	Previous Logon Notification	The information system **notifies** the user, upon successful logon (access) to the system, of the date and time of the last logon (access).	**Screenshot** of notification for previous logon history in application landing page.	**Application, Administration Portal-if any,**
19	Access Control	Dual Control	Enforces **dual authorization** mechanisms (require the approval of two authorized individuals in order to execute) for highly impactful actions (subject to evaluation of the application functions during design phase)	**Screenshot** of implemented dual control method for highly impact action in application layer. The threshold of highly impact action should be confirmed with project owner. If not applicable, please provide justification	**Application, Administration Portal-if any,**

Ref	Category	Control	Requirement	Expected Proof	Layer
20	Access Control	Restrict Access to Database	[PCI 8.7] All access to any database containing **Regular data / cardholder data** (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	Completed ACSA Special Privilege **request form** for limiting access to database .	**Database,**
21	Access Control	Prepare for Production	[PCI 6.3.1] Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	**Set/list** of test and/or custom application data, file path, testing account.	**Application, Administration Portal-if any,**
22	Remote Access	Remote Access to Application	**Restrict access to administrative portal** to internal network only. Otherwise Multi-Factor Authentication (MFA) and / or IP whitelisting MUST be implemented for user access the administrative portal / with administrative right from outside of ACSA trusted network.	**Screenshot proof** of not accessible from external network. Otherwise provide screenshot of MFA / IP whitelisting implemented.	**Application, Administration Portal-if any,** Management Portal for Internal-if any,
23	Remote Access	Remote Access / External Connection to Infrastructure	[ACSA Requirement] Remote connection to ACSA Infrastructure MUST use authorised secure remote access channel, such as: - ACSA VPN and allocated jumphost - AWS workspace and allocated jumphost - Site-to-site VPN and allocated jumphost - Leased line and allocated jumphost - Other remote access channel (e.g., Webex, TeamViewer, Anydesk, etc.) MUST go through special request and approval procedure Note: The request for remote access is via email and ACSA will manually configure the setting. VPN access will be logged. Utilise CyberArk (or equivalent solution if the application is hosted outside ACSA's infrastructure) for managing remote access with administrative privilege from external network (same as [PCI 8.1.5]), - enable screen recording and/or keyboard recording for monitoring in use - enabled only during the time period needed and disabled when not in use. - utilise CyberArk ACL to control user's access to necessary resource only - [PCI 8.3.2] Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network. When the system hosted in outside of ACSA but need to communicate with ACSA Office or IT network environment, all connections MUST be listed out and utilise secured manner, reviewed and approved.	Completed operation **request form** (ask ACSA Infrastructure team) for establish remote connection with ACSA infrastructure.	**OS, Database,** Network Device, Management Portal for Internal-if any,

Ref	Category	Control	Requirement	Expected Proof	Layer
24	Remote Access	Remote Access - Unique Credential per Entity	[PCI 8.5.1] Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as password/phrase) for each customer. Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.	Vendors **acknowledge**: We will not use ACSA provided / ACSA's credential in other customers' / entities' IT environment.	**OS, Database,** Network Device, Management Portal for Internal-if any,
25	Password Management	Password Storage - Application Level	For mobile application or thick client application, credentials should not be stored on the device, otherwise, it MUST be hashed and MUST be prohibited to use for accessing server side application.	**Screenshot** of secure storage of application credentials in database or other location.	**Application, Administration Portal-if any,**
27	Password Management	Password Policy - Infrastructure Level	**Password complexity** is configurable or support setting as below (same as [PCI 8.2.3] [PCI 8.2.4] [PCI 8.2.5]): - Require a minimum password length of 8 characters - Require 4 times password histories (i.e. users cannot set the same password as any of the last three) - Require password complexity contains 3 out of the following types: lowercase letters, uppercase letters, number and symbols - Require password must be forced to change at least every 30 days, including administrative and general user account, or at least password is able to be changed - Do not use the same password to access multiple systems/devices.	To provide screenshot or evidence of the **configuration or policy** setting of password requirement in infrastructure layer.	**OS, Database,** Network Device, Management Portal for Internal-if any,
28	Password Management	Password Transmission and Storage	[PCI 2.3] Encrypt all non-console administrative access using strong cryptography. [ACSA Requirement] Passwords shall be encrypted when transmitting over an un-trusted communication network. Passwords shall always be well protected by using strong cryptography, render all authentication credentials **unreadable during transmission and storage** on all system components. (same as [PCI 8.2.1]) - Vendor shall adopt secured authentication method for password transmission, such as HTTPS and SSH, instead of HTTP or Telnet. The encryption level could be considered as listed below: Level 1 - TLS at least v1.2 Level 2 - Client side symmetrical encryption Level 3 - Client side asymmetrical encryption with nonce - Storage: Passwords/phrases should be stored in unreadable format (e.g., hashed or encrypted)	**Screenshot** of authentication process showing password is encrypted (e.g., encrypt in password field level or in network traffic level) .	**Application, Administration Portal-if any, Network, OS, Database,** Network Device,
29	Password Management	Password Mask	Password must be masked with star (*) while user entering	**Screenshot** of password mask while user entering password in login page	**Application, Administration Portal-if any,**

Ref	Category	Control	Requirement	Expected Proof	Layer
31	Session Management	Session Time Out	Session time-out must be implemented to reasonable time duration for inactive session (e.g., 15 minutes idle time) [ACSA Requirement] [PCI 8.1.8] If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Provide **screenshot or evidence** on the session **setting** in application and infrastructure level. Otherwise, provide justification on exemption.	**Application, Administration Portal-if any, OS, Database,** Network Device, Management Portal for Internal-if any,
32	Session Management	Re-authenticate After Session Timeout	Users must be re-authenticated after the session timeout. [PCI 8.1.8] If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**Screenshot** of re-authentication page or setting and **description** of re-authentication scenario. Otherwise, provide justification on exemption.	**Application, Administration Portal-if any, OS, Database,** Network Device, Management Portal for Internal-if any,
33	Session Management	Session Renew	Session token for authentication must be renewed. Reference : https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#renew-the-session-id-after-any-privilege-level-change	**Demo** of session is renewed when user log out and login to the application again, or provide the **snippet of source code** evidence with description or **pentest report** should include verification of session management security.	**Application, Administration Portal-if any,**
34	Session Management	User Log Out	Session must be terminated when user manually log out of the application	**Demo** of session token terminated when user log out and logout, or provide the **snippet of source code** evidence with description or **pentest report** should include verification of session management security.	**Application, Administration Portal-if any,**

Ref	Category	Control	Requirement	Expected Proof	Layer
35	Session Management	Concurrent Session Control	Limits the number of concurrent sessions for each user to single session only, unless obtain approval to multiple limited session	**Screenshot or demo** of concurrent login notification, or restriction setting (e.g., user can only open one session), or provide the **snippet of source code** evidence with description or **pentest report** should include verification of session management security.	**Application, Administration Portal- if any,**
36	Media Protection	Mobile Device Management (MDM)	[ACSA Requirement] If the mobile application is for ACSA internal staff or authorised third party usage, it can only be used in mobile device managed by ACSA MDM profile or devices with equivalent controls. MDM should support below controls: a) Hard disk / device encryption b) Authentication and screen lock after certain period of idle c) Root detection d) Certificate Management e) Detect unnecessary applications (and inform to device management person in charge) and delete remotely f) Detect necessary applications deleted and install them as mandatory More detailed requirements please refer to IT Security Standard - 8.1 Terminal and Device Management	Provide **screenshot or evidence** on applied ACSA MDM solution to follow ACSA mobile device management. Otherwise to provide the configuration / policy (follow ACSA MDM setting) or provide justification to ACSA on any constraint or limitation.	**Application,**
37	Media Protection	Terminal Protection	In case terminal or device (components required for supporting the solution's function. Vendor's own facilities is not included) need to be used outside of ACSA office environment, follow ACSA's requirement to apply necessary security measures, such as: - ID and smart card or biometric authentication - Location identification function - Privacy filter If the terminal or device will be used by customer, more controls need to be applied, such as: - Anti-shoplifting labels / RFID - Asset management label - Screen saver or lock screen More detailed requirements please refer to IT Security Standard - 8.2 Terminal and Device Management	**Photo** of applied physical protection on terminals	N/A

Re f	Category	Control	Requirement	Expected Proof	Layer
38	Media Protection	Web Application in Device	[ACSA Requirement] For web browser or applications developed that are used on the devices, below items shall be considered to prevent customer information leakage from cache memories left in the devices. Web Browser: - Thorough instruction shall be provided for users to log out after usage. - Thorough instruction shall be provide for users to clear cache memories after usage or it should be considered to use browser with easy cache clear functions or implement add-ons for easy cache clear functions. Applications Allow Customized Development: - Functions to clear the entered values or cache after application usage shall be developed as a part of application functions.	**Demo** of removing cache after user logout or **pentest report** should include verification of cache deletion.	**Application,**
39	Media Protection	Root Detection - Mobile Application	The mobile application MUST implement **Root Detection** mechanism to prevent or notify user the usage of insecure mobile devices. For protecting the mobile application from manipulation by attacker, utilise **application protector**, such as AppGuard or equivalent solution to perform root detection, executable file encryption, application package integrity checking, server authentication, etc.	Follow ACSA requirement to implement **mobile app security protection tool** (e.g., AppGuard)**. Or Pentest report or Screenshot** of root detection result showed in jail-break device running the application or **snippet of source code** with description	**Application,**
40	Media Protection	Certificate Pinning - Mobile Application	The mobile application MUST implement **Certificate Pinning** to ensure the application can only communicate with trusted server	**Pentest report or Screenshot** of mobile application cannot communicate with server when the server is not directly connected (e.g., there is a proxy in the middle)	**Application,**
41	Input Validation	Auto-Completion	[Headquarter Requirement] For all user input field, disable "**auto-complete**" and "**autofill**" functions and prohibit enabling these functions in order to prevent the sensitive information, such as userid, password and card numbers, being automatically stored and visible to unauthorized users.	**Provide screenshot or evidence** that the application does not generate any cached data or cookies to client-side. Otherwise, provide justification on exemption.	**Application, Administration Portal-if any,**
42	Integrity	Code Obfuscation - Mobile Application	For mobile application or thick client application which will be installed / used by customer or external parties, adopt code obfuscation to increase the code reading difficulty and reduce the risk of arbitrary code modification and recompiling.	**Pentest report or Screenshot** of showing code is obfuscated. For mobile application	**Application, Administration Portal-if any,**

Ref	Category	Control	Requirement	Expected Proof	Layer
				development, use app-shielding solution e.g. AppGuard, Promon Shield. For vendor packaged mobile application, provide security proof or pentest report to prove that code obfuscation has been applied.	
43	Integrity	Message Integrity	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified (subject to evaluation on business requirement and regulatory requirement in design phase), and appropriate control identified (e.g. digital signatures, key-hash message authentication code, authentication protocols and tamper-detection) and implemented refer to industry secure standard (e.g., SHA-256 and above) [ACSA Requirement] Network line/packet encryption or digital signature shall be implemented for communication or sending/receiving information that shall be protected from information leakage or falsification. When a digital signature is used to protect from falsification, means for verifying digital signature shall be shared with the users to the extent possible.	**Screenshot** of message checksum appended with message with description of the hashing algorithm	**Application,**
44	Integrity	Unauthorized Modification Detection (Change Detection)	[PCI 11.5] Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. - [PCI 11.5.1] Implement a process to respond to any alerts generated by the change-detection solution.	Provide screenshot or evidence on applied **ACSA FIM** to detect system changes on critical files. Otherwise, provide justification to ACSA on any constraint or limitation.	**OS,**
45	Legal & Compliance	Notification to Internet Banking Customer	To facilitate customers' timely detection of unauthorized transactions that may arise as a result of fraudulent activities related to e-banking channels, notify customers immediately via an effective channel (e.g., SMS, email, etc.) once the customers initiate transactions that are considered as of higher risk. Vendor shall obtain confirmation from project owner or user department on the mechanism details, such us scenario of "higher risk", which channel to notify user is acceptable, etc.	**Screenshot** of customer notification on high risk transaction initiation. The threshold of high risk transaction should be confirmed with project owner. If not applicable, please provide justification	**Application,**

Ref	Category	Control	Requirement	Expected Proof	Layer
46	Legal & Compliance	Use Notification	Displays to users the notification message before granting access to the system that provides privacy and security notices policies, regulations, standards, and guidance End user is responsible for following the guidance and does not misuse data or function provided by the system.	**Screenshot** of notification to users when login to the application The notification message could be customised to suit the purpose of reminding end user's responsibility. Whenever the nofication could not be displayed and the system contains sensitive or critical information, provide justification to ACSA security team for any technical constraints.	**Application, Administration Portal-if any, OS, Database,** Network Device, Management Portal for Internal-if any,
47	Audit & Logging	Audit Trial Type of Activity	[PCI 10.1] Implement audit trails to link all access to system components to each individual user. [PCI 10.2] Implement automated audit trails for all system components to reconstruct the following events: - [PCI 10.2.1] All individual user accesses to cardholder data - [PCI 10.2.2] All actions taken by any individual with root or administrative privileges - [PCI 10.2.3] Access to all audit trails -[PCI 10.2.4] Invalid logical access attempts - [PCI 10.2.5] Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges - [PCI 10.2.6] Initialization, stopping, or pausing of the audit logs - [PCI 10.2.7] Creation and deletion of system-level objects	Used AD authentication: follow ACSA procedure Non-AD authentication: follow left PCI requirement to implement in application and infrastructure layer.	Whole
48	Audit & Logging	Audit Trial Entries	[PCI 10.3] Record at least the following audit trail entries for all system components for each event: - [PCI 10.3.1] User identification - [PCI 10.3.2] Type of event - [PCI 10.3.3] Date and time - [PCI 10.3.4] Success or failure indication -[PCI 10.3.5] Origination of event - [PCI 10.3.6] Identity or name of affected data, system component, or resource.	List of attribute to be logged for each audit trail entry	Whole

Re f	Category	Control	Requirement	Expected Proof	Layer
49	Audit & Logging	Centralised Logging	[ACSA Requirement] All system / event log must distribute to ACSA central logger (SIEM). Follow ACSA SOC technical requirement to conduct the log integration (same as PCI 10.5.3] [PCI 10.5.4]). Countermeasures for acquired log alteration shall be taken. (e.g. Strict access control for log servers, Log writing to the wright once media.) If the system is PCI-DSS in-scope system, please notify the central logger service provider for dedicated log management. Note: Application level log is currently not required to be sent to ACSA centralised logging server. Note to ACSA: ACSA shall provide the log server protocol to vendor for integration.	Windows, Linux, network and security device type information would be centralised. Detailed integration specification please consult ACSA infrastructure and operation team.	Whole
50	Audit & Logging	Trusted Time Sync	[ACSA Requirement] Ensure correctness of time stamps on all log files and audit trails, all the production servers' system clock should configured to synchronize daily with ACSA time server. [PCI 10.4] Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. - [PCI 10.4.1] Critical systems have the correct and consistent time. - [PCI 10.4.2] Time data is protected. - [PCI 10.4.3] Time settings are received from industry-accepted time sources.	**Screenshot** of timeserver configuration for all hosts	**OS,**
51	Audit & Logging	Log Protection	Logs stored inside solution should be well protected from destruction/deletion/modification. Limit viewing of audit trails to those with a job-related need. In addition, please consider: • Masking sensitive data (e.g., PCI-DSS related data, Personal Identifiable Information, account credential, session token, etc.) in log • Web Crawler rejection [PCI 10.5] Secure audit trails so they cannot be altered. - [PCI 10.5.1] Limit viewing of audit trails to those with a job-related need. - [PCI 10.5.2] Protect audit trail files from unauthorized modifications. - [PCI 10.5.5] Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	1. **List of log** storage location/path and **Configuration or setting** of log data/system access restriction and storage protection - For infrastructure log (either on-premise or cloud environment), restrict the system level access by firewall rules and authentication - For external facing web application, if the log file is stored inside a	**Application, Administration Portal- if any, OS, Database,**

Ref	Category	Control	Requirement	Expected Proof	Layer
				folder, restrict access to the log data/folder/web path to trusted IP or user account. 2. Provide a **list** of log attribute and log sample, and indicate whether the potential sensitive data is logged and masked	
52	Audit & Logging	Log Review	[PCI 10.6] Review logs and security events for all system components to identify anomalies or suspicious activity. - [PCI 10.6.1] Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). - [PCI 10.6.2] Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment. - [PCI 10.6.3] Follow up exceptions and anomalies identified during the review process.	**Provide a list of logs with categories and instructions** for IT BAU to review.	N/A
53	Audit & Logging	Log Retention	[PCI 10.7] Retain audit trail history for **at least one year**, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). [ACSA Requirement] - All log records in scope should be kept online at least 3 months for immediate analysis. - After the 3 months, log records can be stored off-line. - The log records which are older than 2 years can be purged.	Provide evidence on forwarding the event logs to the ACSA log servers. For other system / application logs which do not forward to the ACSA log servers, provide evidence on the log retention period configuration. Otherwise, provide justification on exemption.	N/A

Ref	Category	Control	Requirement	Expected Proof	Layer
54	Network Protection	Network Architecture Design	Vendor shall provide the network architecture design following below requirement: 1. The network architecture **design** for the solution should follow below ACSA network domains defined with respect to their security trust levels, including: - Demilitarised Zone (DMZ) - Application Server Zone - Database Server Zone - Core Server Zone - Development Zone Vendor may indicate in the design diagram, all components will be fall into which zone above. - A server with user data stored should not be placed in DMZ. Based on the level of confidentiality of information stored, a separate network segment with additional security measure can be implemented to control data access. - A public facing server should be placed in DMZ and should communicate with internal servers through firewall protection. Authentication and data protection controls should be established to safeguard the confidentiality and integrity of data passing over public networks. - Direct communication between the Internet and internal network should be prohibited and safe connection to the Internet shall be performed via proxy server in DMZ. **2. Firewall** should be used to restrict the communication to necessary minimum, security assessment should be performed on any connection request across different network zones,	**Network diagram and firewall rule** showing the solution's hosting systems mapped to ACSA defined different network zone.	Network,
55	Network Protection	Protect from Public Access	[PCI 1.3] Prohibit direct public access between the Internet and any system component in the cardholder data environment: - [PCI 1.3.1] Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. - [PCI 1.3.2] Limit inbound Internet traffic to IP addresses within the DMZ. - [PCI 1.3.3] Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.) - [PCI 1.3.4] Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. - [PCI 1.3.5] Permit only “established” connections into the network. - [PCI 1.3.6] Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. - [PCI 1.3.7] Do not disclose private IP addresses and routing information to unauthorized parties.	**Network diagram** and **review result** of applied firewall rules or ACL to limit external access.	Network,

Ref	Category	Control	Requirement	Expected Proof	Layer
56	Network Protection	Protect from Untrusted Network	[PCI 1.2] Build firewall and router configurations that restrict connections between untrusted networks and any system components in the current solution / cardholder data environment - [PCI 1.2.1] Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. - [PCI 1.2.2] Secure and synchronize router configuration files. - [PCI 1.2.3] Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment. [ACSA Requirement] Firewall, router and so forth shall be installed at the network border to limit any unnecessary communication: - Only necessary port and protocol for inbound/ outbound connection should be opened across network zones of different security trust levels. Any unnecessary connection shall be refused by default. - Measures such as NAT and so forth shall be implemented to prevent from disclosing internal network address. For outsourced network service, review any necessary change to the current service scope and conditions. Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced. (The security mechanisms, service level and mgmt. requirements and so forth can be defined either by ACSA or by service supplier.)	**Network diagram** and **review result** of applied firewall rules or ACL between trusted and untrusted network	Network Device,
57	Network Protection	Network Separation	1. Production environment MUST be separated from development / testing environment - [PCI 6.4.1] Separate development/test environments from production environments, and enforce the separation with access controls. - [PCI 6.4.2] Separation of duties between development/test and production environments 2. HA and DR machine should not be used for development / testing / UAT machine which according to year 2014 Japan head office instruction.	**Network diagram and firewall rule** showing network separation between different purpose	Network,

Ref	Category	Control	Requirement	Expected Proof	Layer
58	Network Protection	Firewall and Router Configuration	[PCI 1.1] Establish and implement firewall and router configuration standards: - [PCI 1.1.1] A formal process for approving and testing all network connections and changes to the firewall and router configurations - [PCI 1.1.2] Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks - [PCI 1.1.3] Current diagram that shows all cardholder data flows across systems and networks - [PCI 1.1.4] Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone - [PCI 1.1.5] Description of groups, roles, and responsibilities for management of network components - [PCI 1.1.6] Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. - [PCI 1.1.7] Requirement to review firewall and router rule sets at least every six months	Configuration **guideline**, **record** of applying settings accordingly and review **result** for firewall and router configuration If the service provider has independent assessment report or certified by PCI-DSS, ISO27001, ISO27002, SOC2, etc., this control could be considered as implemented by the service provider and verified by their auditor. Otherwise, the service provider shall provide confirmation of the control existing and obtain ACSA security team's approval	Network Device,
59	Network Protection	Control on Portable Devices for Accessing Server / Internal Network	[PCI 1.4] Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices. [ACSA Requirement] Protection need to be implemented on devices has remote access to internal data: 1) Log-in authentication not only with a password but also with smart card or biometric authentication (2) Downloaded data from the internal network shall be automatically deleted from a hard disk when session is disconnected. (3) In case downloaded data can be saved in a hard disk, the hard disk shall be encrypted to prevent information from being leaked due to device theft. (4) Personal firewall shall be installed and activated or anti-virus software with similar functions shall be implemented and activated. (5) A thin client device shall be considered.	**Screenshot** of firewall setting on portal devices, MDM solution or network proxy to protect the portal device from internal attack.	Network,

Ref	Category	Control	Requirement	Expected Proof	Layer
60	Network Protection	Network Communication Authentication	Connection between hosts should be **authenticated** (e.g., API or port level connection).	**List** of APIs or port level communication and **authentication setting**	Network,
61	Network Protection	Monitor for Malicious Call-back	[ACSA Requirement] A system shall be installed for monitoring and interrupting any improper communication transmitted between a malicious program intruding into the internal network and an attacker's external server (C&C server), the solution's network should be managed by the network protection mechanism.	Install or integrate with ACSA malware detection (e.g., Fireeye NX, Trend Micro HIPS, CheckPoint IPS) solution. Otherwise, provide justification to ACSA on any constraint or limitation.	Network,
62	Network Protection	Anti-DDoS Attack	[ACSA Requirement] Below countermeasures against DDoS attack shall be implemented. (1) Systems to detect DDoS attack shall be implemented. (2) Functions or services for automatic access filtering, blocking or distributing shall be implemented.	- For mission critical customer facing service hosting in ACSA on premise, utilise ACSA's external network line with Anti-DDoS feature. - For cloud solution, deploy/enable Anti-DDoS solution in cloud environment. Otherwise, provide justification to ACSA on any constraint or limitation.	Network,
63	Data Protection	Data In Transit Encryption over Untrusted Network and between Internal Systems	- Identify the communication channel between **external systems / SaaS** components and encrypt the data from end-to-end for all communication channels. - Implement network level encryption or use secured protocol for communications **between internal system** interfaces, e.g., TLS, SFTP, to protect all communication [PCI 4.1] Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	**List** of all system and network communication channels and whether used encrypted protocol	Network,

Ref	Category	Control	Requirement	Expected Proof	Layer
64	Data Protection	Data in Transit over Wireless Network	[PCI 4.1.1] Ensure **wireless** networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	If wireless network is utilised, deploy secure transmission solution (e.g., authentication and encryption by Certificate Authority solution and PKI mechanism) between device and server. Otherwise, provide justification to ACSA on any constraint or limitation.	Network,
65	Data Protection	Data in Transit for PAN	[PCI 4.2] Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	Vendors acknowledge: No unprotected PAN will be transmitted by end-user messaging technologies	**Application, Administration Portal- if any, Network,**
66	Data Protection	Data Mask for PAN	[PCI 3.3] Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN. [PCI 3.4] Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures.	**List** of user interfaces with PAN displayed (with remark if full PAN is displayed) and **screenshot** of showing PAN masked on unnecessary user interfaces. **1. List** of PAN storage locations (server, directory/folder, file name/database, field/column). 2. **Screenshot** of the stored PAN or unreadable format of the encrypted file with PAN data. 3. State what encryption/hashing algorithm is used and provide screenshot or the encryption keys to prove the	**Application, Administration Portal- if any, OS, Database,**

Ref	Category	Control	Requirement	Expected Proof	Layer
				encryption/hashing algorithm used.	
68	Data Protection	Data at Rest Encryption	**Regular data, PCI-DSS related data and any other personal data** of the solution be encrypted at rest (e.g., data field encryption, database encryption, hard disk encryption) The encryption algorithm must comply with ACSA's encryption standard	**Screenshot** of 1) data query result in database showing the data is encrypted and 2) encryption setting enabled for all data storage device (e.g., database and SAN) with 3) encryption algorithm information.	**OS, Database,**
69	Data Protection	PCI - Sensitive Authentication Data Storage	[PCI 3.2] Do not store sensitive authentication data (e.g. CVV, PIN) after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3: - [PCI 3.2.1] Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. - [PCI 3.2.2] Do not store the card verification code or value (three-digit or	**Provide the application design (including data flow document) to prove that no sensitive authentication data is stored after authorization.** **Otherwise to provide the justification to**	**Database,**

Re f	Category	Control	Requirement	Expected Proof	Layer
			four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization. -[PCI 3.2.3] Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	**ACSA on any constraint or limitation and provide screenshot** of encryption setting enabled for all storage of authentication data with encryption algorithm information.	
70	Data Protection	Disk Encryption, if any	[PCI 3.4.1] If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	Provide the screenshot of credentials used for disk encryption to prove that they are not local accounts or default accounts of the operating system or appliance.	**OS,**
71	Data Protection	Archive/Backup Data Encryption	The archived or backup data must be encrypted to protect the confidentiality of the data	**Screenshot** of encryption setting enabled for all data backup storage device with encryption algorithm information.	**Database,**
72	Data Protection	Data / File Transfer into external media	[ACSA Requirement] In case data / file will be transferred into **external media** (Floppy, CD/DVD, and other external storage devices) based on requests submitted by users for both internal and external parties, the relevant Information Security Officer is responsible to ensure the data handling is comply with DSG and ISS; where applicable, follow **CRM-ISM-001 Security Manual for Data Transfer into External Storage Media**. For AS400 related files, there are two kinds of AS400 File Transfer files. Development team should develop the corresponding program according to the following procedure for file transfer action (Case reference refer to "**AEON-SYSOPS-STG-297 V2.0 Section 3.7**) Note: Backup tape is not managed under this control. Note: This control applies to external storage device which will be used outside of ACSA	Completed **request form** for data transfer to external media	N/A
73	Data Protection	Data Mask for Testing	Mask, redact or obfuscate Restricted / Confidential / PCI-DSS data of the solution (in digital/physical format) for testing purposes or any other non-production use. - Real personal information shall not be used for any testing purpose - Production data / data base shall not be used for any testing purpose. When it is required to test on production real data, Head of IT Division's approval is required. And in such case, personal data items must be removed / masked. Production data usage (purpose, person in charge, date of copy, data date, deletion evidence, etc.) shall be recorded. [PCI 6.4.3] Production data (live PANs) are not used for testing or development	**Do not** use production data for testing purpose. Otherwise, where necessary, provide **justification** to ACSA and get approval from IT division head before proceed.	**Database,**

Re f	Category	Control	Requirement	Expected Proof	Layer
				In general, provide the masking methodology and design, and show the production data is masked for testing usage. **Screenshot** of applied security control for non-production system storing production data, when the production could not be masked and stored in non-production environment	
74	Data Protection	Test Data Protection	[ACSA Requirement] Test data shall be selected carefully, protected and controlled. Consideration points on System Test are: - Testing environment shall be prepared to avoid any affection to the running production environment - Test data shall be similar to the production real data as much as possible - Test data and result shall be retained at least two years after test completion date	**Description** of testing data preparation method and **screenshot** of testing data storage setting	**Application, Administration Portal-if any, OS, Database,**
75	Data Protection	Test Data Removal	[PCI 6.4.4] Removal of test data and accounts from system components before the system becomes active / goes into production.	**List** of test data location, test account. **Screenshot** or **request form** (ACSA Operation Job Request Form) showing test data removing task completed	**Application, Administration Portal-if any, OS, Database,**
76	Data Protection	Data Retention	For Financial system (agreed upon ACSA's criteria, please consult ACSA), data MUST be kept at least 7 years for legal compliance requirement.	**Screenshot** of data storage setting and infrastructure design for supporting the storage volume.	Whole

Ref	Category	Control	Requirement	Expected Proof	Layer
77	Data Protection	Email System Usage	[ACSA requirement] When the project is associated to E-mail system, a solution to provide E-mail archiving function to keep mail contents including attachment files as well as basic information such as sender and time for **5 years** is required. Follow AEON-SYS-013 IT Security Standard. (Check with IT - Infrastructure and Operation when there is a need to communicate with web free email, or any other exception is necessary)	**Screenshot** of storage setting for 5 years email data archive and **list** of what attributes would be stored.	**Application, Administration Portal- if any, OS,**
78	Cryptography	Encryption Algorithm Standard	Encryption scheme that has encryption algorithm and key length with sufficient strength as industry standard shall be adopted. Information on algorithm compromise and safety assurance is collected to determine whether encryption algorithm should be upgraded or not. Strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.) should be considered. Apply strong cryptography according to PCI DSS requirement, latest as below AES – 128 bits or higher. TDES/TDEA – triple-length keys. RSA – 2048 bits or higher. ECC – 224 bits or higher.	**List** of items utilised encryption (e.g., data storage, data-in-transit) and used encryption algorithm	Whole
79	Cryptography	Cryptographic Architecture Description & Key Management	[PCI 3.5] Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse [PCI 3.5.1] Additional requirement: Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management [PCI 3.5.2] Restrict access to cryptographic keys to the fewest number of custodians necessary. [PCI 3.5.3] Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method [PCI 3.5.4] Store cryptographic keys in the fewest possible locations. [PCI 3.6] Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: - [PCI 3.6.1] Generation of strong cryptographic keys - [PCI 3.6.2] Secure cryptographic key distribution - [PCI 3.6.3] Secure cryptographic key storage - [PCI 3.6.4] Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). - [PCI 3.6.5] Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are	**Documentation** of cryptographic architecture and **list** of key storage location **Procedure documentation** of key management	N/A

Ref	Category	Control	Requirement	Expected Proof	Layer
			suspected of being compromised. - [PCI 3.6.6] If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. - [PCI 3.6.7] Prevention of unauthorized substitution of cryptographic keys. - [PCI 3.6.8] Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. **HSM configuration must follow industry best practice or vendor's suggestion. Access to HSM must be restricted to minimum and necessary users.**		
80	Cryptography	Certificate Management	Define and implement secure certificate management mechanism for handling purchasing, deploying, renewing, and replacing certificates on respective endpoints (which could be an application, a server, a device – or any other network component). For solution host in ACSA's environment, vendor shall provide the requirement details to ACSA on certificate usage, indicate the location where need to use certificate.	**1. Procedure** of certificate management 2. **List** of certificates and their usage (i.e. certicate inventory)	**Application, Administration Portal-if any, OS, Database,** Network Device, Management Portal for Internal-if any,
81	Configuration Management	Utility Program	[ACSA Requirement] Utility program (requirement administrative privilege) overriding ACSA existing systems values shall not be used or exceptional approval must be obtained from ACSA's IT	Provide **requirement and justification** for any updating on existing system values and obtain the department head of ACSA IT Infrastructure and Operation's **approval**	**OS,**
82	Configuration Management	Configuration Standards	[PCI 2.2] Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).	**List** of defined configuration standard for all relevant OS. For well-known OS such Windows Server, Red Hat, follow the ACSA hardening template. For vendor-tailor-made OS or proprietary system, such as HSM products, SSO appliance, provide the hardening guide from the manufacturer.	**OS, Database,** Network Device,

Ref	Category	Control	Requirement	Expected Proof	Layer
83	Configuration Management	System Hardening	[ACSA Requirement] System hardening be performed for all servers/databases/devices used in the solution according to the ACSA hardening guides, or industry best practice: - [PCI 2.2.1] Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component. - [PCI 2.2.2] Enable only necessary services, protocols, daemons, etc., as required for the function of the system. - [PCI 2.2.3] Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. - [PCI 2.2.4] Configure system security parameters to prevent misuse. - [PCI 2.2.5] Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. [ACSA Requirement] - Hardening should be completed before software/application installation & development - A hardening report to show the hardening results. - A workflow control for testing the hardened containers in testing environment and deploy to production after verifications - The hardening process should meet latest PCIDSS requirement - The process should cover all components in the system. Provide reasons and official supporting documents for excluding any components in the proposed solution	**For PCI compliant projects, provide the evidence to fulfil PCI 2.2.1.** Comply with ACSA hardening compliance check result. For vendor-tailor-made OS or proprietary system, such as HSM products, SSO appliance, provide the hardened configuration file as an evidenace.	**OS, Database,** Network Device,
84	Configuration Management	Installation of Software	[ACSA Requirement] Any installation of software on existing systems / golden image need to apply for approval with comply with AEON-SYS-005 IT Management Detail Regulation – Information System Operation: 11. Hardware, Software and Network Administration	**Request form** (ACSA Operation Job Request Form) for installation of software on existing systems / golden image	**OS, Database,** Network Device,
85	System Protection	Restrict Access to Source Code	[ACSA Requirement] Source code should be maintained in secured repositories to enable proper security oversight and controls. Access to source code and associated items (such as system designs and specifications) should be controlled to limit access based on job function. Developers should not have the ability to deploy code to production systems directly.	Provide User Access Matrix (**UAM)** for source code access control.	N/A
86	System Protection	Protection from Malware	[ACSA Requirement] [PCI 5.1] Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). - [PCI 5.1.1] Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. - [PCI 5.1.2] For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. - [PCI 5.2] Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7. - [PCI 5.3] Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Integrate with ACSA **anti-virus solution (Trend Micro). Or Report / result** of anti-virus deployment status and **operating procedure** for the anti-virus procedure (if not managed by ACSA)	**OS, Network**

Ref	Category	Control	Requirement	Expected Proof	Layer
			[PCI 11.4] Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.		
87	System Protection	Vulnerability / Patch Management	[PCI 6.1] Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. [ACSA Requirement] 1. Reliable third party providers (CERT organization in each country such as JPCERT/CC, US-CERT, HKCERT and so forth) shall be designated as sources to collect vulnerability information. 2. An intrinsic nature, a severity level and an impact of collected vulnerability shall be assessed and action policies shall be implemented, such as whether a patch is applied or not and when it is applied. 3. For core systems and public servers, operations of applying security patches shall be recorded. A list (or database) of security patches application status shall be created for review. [PCI 6.2] Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. Provide the system patching details which cover the workflow, procedures & ongoing patching arrangement for the docker/container platform. The plan should at least cover the following: - Regular patch review report which identify the patch level and patch recommendation list - Automate the patch deployment process - Patch will deploy in SIT/UAT environment for verification before production deployment - Conduct a systematic post production review - Provide system patching report for successful/failure/pending cases - The system must apply latest patch before production rollout - Follow ACSA Patch Management Procedure - Patch status should be visible. Patch deployment should be automated.	**Documented procedure** of vulnerability management and **sample** of patching result Provide the evidence that the manufacturer of the system or platform chosen in the project has not yet announced an End-of-support / End-of-life schedule. for regular patching the OS/firmware of the system or platform chosen in the project that is not Windows or Red Hat: Include in the SOW: 1. Regular patching should be 4 times per year; 2. Hardening scan will be performed 1 – 2 times per year Include in the SOW unlimited fix or patch for vulnerabilities finding based on below target periods: 1. Critical severity within 2 weeks; 2. High severity with 1 month; 3. Medium and	**OS, Database,** Network Device,

Re f	Category	Control	Requirement	Expected Proof	Layer
				low severity within 3 months Expect vulnerability fix schedule subject to security incidents or alerts from manufacturers or public sources finding.	
88	System Protection	Regular Patch Release	[ACSA Requirement] The solution MUST support regular patch / version update to remediate identified bugs and vulnerabilities and deploy the patch according to ACSA's patching arrangement. 1) For in-house development or outsourcing development, ensure the development team is continuously optimise the solution and release security patches timely 2) For COTS, customised package and SaaS product, ensure the vendor will regularly release patches Follow ACSA SLA ITD	Vendor acknowledge: vendor will release patch for identify vulnerability in solution. Otherwise, provide justification to ACSA on any constraint or limitation.	Whole

Ref	Category	Control	Requirement	Expected Proof	Layer
89	System Protection	Shared Hosting Providers	[PCI 2.6] Shared hosting providers must protect each entity's hosted environment and cardholder data. [PCI A1.1] Ensure that each entity only runs processes that have access to that entity's cardholder data environment. [PCI A1.2] Restrict each entity's access and privileges to its own cardholder data environment only. [PCI A1.3] Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10. [PCI A1.4] Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider. Remark: This is intended for hosting providers that provide shared hosting environments for multiple clients on the same server. When all data is on the same server and under control of a single environment, often the settings on these shared servers are not manageable by individual clients.	**Vendor acknowledge:** ACSA environment is separated from other tenants. Otherwise, provide justifications for exemptions.	Whole
92	Physical Security	Equipment Sitting and protection	[ACSA Requirement] For system sit in ACSA data center or IT environment, the equipment setup and maintenance MUST follow ACSA IT regulation and complete required information documentation. - Newly move-in equipment shall be sited in appropriate security zone based on the level of importance of information and business requirement. - IT Core Systems shall be all placed within datacenter or server rooms, following the equipment sitting and protection control. - Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. - Cables for equipment shall be placed under raised floor. In case where raised floor is not available, preventive measures shall be taken for power cables and communication cables. *It is recommended to retain system aging within 5 years. [ACSA Requirement] Data center capacity evaluation is required whenever plan for physical machine or IT equipment installation, it ensure the capacity in data center can meet the new system specification.	For hardware installation, inform ACSA network team on rack space, device size (**depth***width*height), max power consumption, number of the power socket, type of the power socket, number of the network port, KVM facility and SAN storage adoption before start any installation work. Provide hardware serial number and model to System Planning and Control department for SAP input.	Physical,

Ref	Category	Control	Requirement	Expected Proof	Layer
93	Physical Security	Physical Access Control	[PCI 9.1] Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. • access is controlled with badge readers or other devices including authorized badges and lock and key. • a system administrator's attempt to log into consoles for randomly selected systems in the cardholder data environment and they should be "locked" to prevent unauthorized use. [PCI 9.3] Control physical access for onsite personnel to sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. [PCI 9.4] Implement procedures to identify and authorize visitors. Procedures should include the following: - [PCI 9.4.1] Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained. - [PCI 9.4.2] Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel. - [PCI 9.4.3] Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration. - [PCI 9.4.4] A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	If using ACSA data center, person enter the data center shall obtain **ACSA's approval.** If using vendor's data center, vendor shall provide **policy, procedure, request form and approval record** to proof physical access control is restricted	Physical,
94	Physical Security	Access Monitor	[PCI 9.1.1] Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	If using ACSA data center, all area is already covered by CCTV. If using vendor's data center, vendor shall provide **photo** evidence showing the hardware is monitored by CCTV	Physical,
95	Physical Security	Protect Devices	[PCI 9.1.2] Implement physical and/or logical controls to restrict access to publicly accessible network jacks. [PCI 9.1.3] Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	Independence audit **report** or **certificate** (e.g., ISO27001) to ensure the necessary controls are in-place for data center security management.	Physical,

Re f	Category	Control	Requirement	Expected Proof	Layer
96	Physical Security	Distinguish Visitor	[PCI 9.2] Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	Independence audit **report** or **certificate** (e.g., ISO27001) to ensure the necessary controls are in-place for data center security management.	Physical,
97	Physical Security	Protect Media	[PCI 9.5] Physically secure all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes). [PCI 9.5.1] Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	Independence audit **report** or **certificate** (e.g., ISO27001) to ensure the necessary controls are in-place for data center security management.	Physical,

Ref	Category	Control	Requirement	Expected Proof	Layer
98	Physical Security	Distribution of Media Protection	[PCI 9.6] Maintain strict control over the internal or external distribution of any kind of media, including the following: - [PCI 9.6.1] Classify media so the sensitivity of the data can be determined - [PCI 9.6.2] Send the media by secured courier or other delivery method that can be accurately tracked. - [PCI 9.6.3] Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	Independence audit **report** or **certificate** (e.g., ISO27001) to ensure the necessary controls are in-place for data center security management.	Physical,
99	Physical Security	Labelling of information	[ACSA Requirement] Information Asset shall be labelled with the classification defined in Information Security Standard (refer to definitions in item 4.1.3).	Vendor provide hardware serial number and model to ACSA System Planning and Control for SAP input	Physical,
100	Physical Security	Media Inventory	[PCI 9.7] Maintain strict control over the storage and accessibility of media. [PCI 9.7.1] Properly maintain inventory logs of all media and conduct media inventories at least annually.	Independence audit **report** or **certificate** (e.g., ISO27001) to ensure the necessary controls are in-place for data center security management.	Physical,
101	Physical Security	Physical media transfer	In case Media contains personal data would be transferred during the project (same as [PCI 9.6]): 1. In order to reduce the risk of personal data being stolen or lost, select the most reliable delivery Company as delivery agent. 2. Specify the value of content, e.g. by declaring that it is confidential. 3. Any documents or physical media transported off site for disposal should be kept in locked containers until the media is destroyed. 4. Management approval for such transfer must be obtained	**N/A. Handled by ACSA corresponding department**	Physical,

Ref	Category	Control	Requirement	Expected Proof	Layer
102	Physical Security	Destroy Media / Data Disposal	[PCI 9.8] Destroy media when it is no longer needed for business or legal reasons as follows: - [PCI 9.8.1] Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. - [PCI 9.8.2] Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. [ACSA Requirement] In principle, prohibit taking out equipment such as servers, terminals, network devices, etc. from the office to the outside by repair etc. (In principle, on-site maintenance contracts should be placed instead of send-back maintenance contracts.) [ACSA Requirement] In the case of repairing equipment with replacing parts, disposing procedure of failed parts storing important information (hard disk, memory, etc.) should be conform to the disposal procedure described in Article 64 of this standard. (It should be specified in the maintenance contract that the own company reserves ownership of the failed parts replaced.) [ACSA Requirement] For AIS system related, System Planning and Control Department ("SPC") is required to log the necessary information provided by AIS IT Department for any IT asset in AIS that are going to be disposed. ACSA also has the right to perform disposal at any circumstance, for the procedure of ACSA disposal, please refer to the document “Computer Equipment and Data Media Disposal”	**N/A. Handled by ACSA corresponding department**	Physical,

Ref	Category	Control	Requirement	Expected Proof	Layer
103	Physical Security	Protect Card Reading Device	[PCI 9.9] Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. - [PCI 9.9.1] Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification. - [PCI 9.9.2] Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). - [PCI 9.9.3] Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	**List** of card reading device inventory information, including applied physical security protection, **scheduled** maintenance checking arrangement	Physical,
104	Maintenance	Application Healthy Monitoring and Notification	Ensure regular health check scheduled and performed for ensuring the application is functioning as expected, the interfaces between different components or between different systems are exchanging correct information. Monitoring event or alert message through email or SMS send to systems operations department immediately whenever abnormal activities occur. [ACSA Requirement] Provide application healthiness monitoring: 1. Monitor the application and process healthiness such as transaction round trip time and API healthiness status (successful connection to other sub-system/interfaces); check # of sub-sys 2. Error Rate Report and alert for the system failure in each type of transaction (e.g. User failure log-in / More on customer experience) , performance of normal transaction. 3. Define the high-frequency customer activities and alert 4. Measurement of application healthiness with reports measured against baseline. Reports can be shared among IT and business team. 5. Application performance such as response time, 6. Resources monitoring for critical service and provide immediate alert during abnormal circumstance	Show that the design document has included application monitoring tools (e.g. Dynatrace, New Relic) for services facing to customers. For example, mobile application, public web application. Provide the URL or portal link for application healthy monitoring	Whole

Ref	Category	Control	Requirement	Expected Proof	Layer
			7. Batch Job performance Report and alert 8. Provide application performance report For those classified as core systems or customer facing services must be setup and monitoring by system proactive manner.	dashboard and list of monitored attributes.	
105	Maintenance	Infrastructure Healthy Monitoring and Notification	[ACSA Requirement] The system capacity should be closely monitored so System Operations could get **sufficient alert** (example: Email, SMS, LED tower signal, beacon, audible alarms, etc.) no matter failure or success in the system. Provide the **system monitoring** arrangement which cover the following 1. The utilization of system resources (CPU, RAM, network utilization, etc.) down to container level - using PRTG or alternative solution 2. The storage space consumption 3. Database performance and utilization 4. Abnormal system utilization and alert 5. Regular resources utilization report 6. Recommendation for resource reassignment to enhance application performance and cost saving 7. Areas that cannot monitor [PCI 10.8] Additional Requirement: Implement a process for the **timely detection and reporting** of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	**Provide the interfaces of the servers, appliances or platforms used in the project for ACSA monitoring tools and Security Operation Center (SOC) to perform the infrastructure health monitoring and notification.**	**OS, Database, Network**
106	Maintenance	Change Control / Change Management	[PCI 6.4.5] Change control procedures must include the following: - [PCI 6.4.5.1] Documentation of impact. - [PCI 6.4.5.2] Documented change approval by authorized parties. - [PCI 6.4.5.3] Functionality testing to verify that the change does not adversely impact the security of the system. - [PCI 6.4.5.4] Back-out procedures. [PCI 6.4.6] Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	Follow ACSA change management procedure	Whole
107	Maintenance	Maintenance Plan	Provide the ongoing maintenance & support plan which cover the following - Define the frequency of regular planned maintenance - The downtime required and the service impact for regular maintenance - The procedures for shutting down and bringing up the service/application - The health check procedures after maintenance - All maintenance job must obtain operation team approval before proceed	**Procedure** of ongoing maintenance and support plan	N/A

Re f	Category	Control	Requirement	Expected Proof	Layer
108	Security Validation	Wireless Access Point Testing	[PCI 11.1] Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. - [PCI 11.1.1] Maintain an inventory of authorized wireless access points including a documented business justification. - [PCI 11.1.2] Implement incident response procedures in the event unauthorized wireless access points are detected.	**For Wireless access point solution project, provide the testing report** for wireless access point, testing method, testing scope, identified issues and remediation verification result for all identified issues. In general, provide the inventory of wireless access points to ACSA for vulnerability scan.	Network,
109	Security Validation	Vulnerability Scanning	[PCI 11.2] Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). - [PCI 11.2.1] Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel. - [PCI 11.2.2] Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. - [PCI 11.2.3] Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. [ACSA Requirement] External vulnerability scanning shall be performed at least once in a year.	**Provide the inventory of items to ACSA for vulnerability scan.** **Provide the testing report** for network scanning, scanning method, scanning scope, identified issues and remediation verification result for all identified issues.	**OS, Database,** Network Device,
110	Security Validation	Application Security Testing - Code Review	For web applications, smartphone/mobile application, thick client applications which are available for public, security **code scanning MUST be conducted** before and after production launch. If there are any reported security flaws, the vendor is responsible to fix the issues.) [PCI 6.3.2] Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release.	**Provide the development guide including the code security review or scan, review method and scanning scope.** **Provide the evidenace that the code security or scan has been completed, such as identified issues, remediation records.**	**Application, Administration Portal- if any,**

Ref	Category	Control	Requirement	Expected Proof	Layer
111	Security Validation	Application Security Testing - Penetration Testing	For web applications, smartphone/mobile application, thick client applications which are available for public, end-to-end penetration testing (such as web / mobile / thick client application testing, network penetration test, configuration review, wireless penetration test) MUST be conducted before and after production launch. If there are any reported security flaws, the vendor is responsible to fix the issues.) [PCI 11.3] Implement a methodology for penetration testing (details please refer to PCI 11.3): - [PCI 11.3.1] Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). - [PCI 11.3.2] Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification - [PCI 11.3.3] Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. - [PCI 11.3.4] If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. - [PCI 11.3.4.1] Additional Requirement: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. [ACSA Requirement] - An external penetration test shall be performed at least once in a year. - In addition to the above, vulnerability scanning and penetration test from internal network shall be considered. - Vulnerability verification shall be conducted by a third party (e.g. professional security vendor)	**Testing report** for application penetration testing, review method, scanning scope, identified issues and remediation verification result for all identified issues. For PCI compliant projects, both external and internal penetration tests must be included. Otherwise, external penetration test is compulsory to include.	**Application, Administration Portal-if any, OS, Network,** Management Portal for Internal-if any,

Ref	Category	Control	Requirement	Expected Proof	Layer
112	Security Validation	Public-facing Web Applications On-going Vulnerability Monitoring	[PCI 6.6] For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	**For cloud project implementation , provide the design document to use WAF for public facing web applications.** **For on-premises project, provide the design document to use ACSA's WAF for public facing web applications. Otherwise, provide justifications for using a separate WAF.** **The followings apply to Infrastructure or Security projects only:** **- Provide the procedures in operation and maintenance manual** for on-going application vulnerability monitor, identification and remediation.	**Application, Administration Portal- if any,**
113	Security Validation	Secure Development	[PCI 6.5] Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines. - [PCI 6.5.1] Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. - [PCI 6.5.2] Buffer overflows - [PCI 6.5.3] Insecure cryptographic storage - [PCI 6.5.4] Insecure communications - [PCI 6.5.5] Improper error handling - [PCI 6.5.6] All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). - [PCI 6.5.7] Cross-site scripting (XSS) - [PCI 6.5.8] Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). - [PCI 6.5.9] Cross-site request forgery (CSRF) - [PCI 6.5.10] Broken authentication and session management.	Documented **coding practice** or followed **guideline** by application developers	Whole

Ref	Category	Control	Requirement	Expected Proof	Layer
115	System Protection	Countermeasures for Web Application Vulnerability	[ACSA Requirement] For web application, a **web application firewall (WAF)** shall be implemented to address vulnerability of a Web application that has access from the Internet and deals with inputting/outputting of confidential information. Settings of WAF shall be continuously maintained to protect from new threats or vulnerabilities. [ACSA Requirement] TLS Implementation MUST be implemented to enhance web security.	**Request form (ACSA Job Request Form) or confirmation** of WAF setup	**Application, Administration Portal- if any,**
116	System Protection	System Inventory	[PCI 2.4] Maintain an inventory of system components that are in scope for the current solution / PCI DSS. [ACSA Requirement] All system assets including hardware, OS, software, network equipment and so forth shall be managed with System Asset Management List.	Fill up ACSA provided **inventory template.**	**OS, Database,** Network Device,
117	Supplier Management	Information Security in Supplier Relationships	[PCI 12.9] Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement. [ACSA Note] Vendor shall provide such acknowledge in writing to ACSA.	Only apply to the project or solution that the vendor or service provider will process and store cardholder data in their own platforms: - Vendor acknowledges in writing that they are responsible for the security of cardholder data.	Whole
118	Incident Response	Incident Response Plan and Support Model	[PCI 10.8.1] Additional Requirement: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls Establish incident (both operation and security type) response plan, define escalation path, timely update responsible party's contact. Ensure identified incident is properly managed, suspicious security incident should be reported to ACSA IT Security team and CSIRT team for further investigation. In case the system is hosted in vendor's environment, vendor shall integrate with ACSA's incident ticketing system for centralised incident management, or manage the incident internally and regularly report to ACSA CSIRT team for information. The plan should at least cover: - Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents. - Information security incidents shall be responded to in accordance with	ACSA has infrastructure or operational **incident response plan** with defined role and responsibility, but vendor also needs to provide the focal point and SLA to support ACSA on incidents.	Whole

Ref	Category	Control	Requirement	Expected Proof	Layer
			the documented procedures. - Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents. - The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.		
119	Contingency Planning	Data Backup	Ensure data backup mechanism is in-place. The backup data should be well protected and encrypted. Backup data should only access by authorized personnel only when needed. A procedure MUST be in place to ensure back-up media is **restorable** with data and configuration integrity check when needed. The backup should include both data and configurations to ensure restore back of the entire system.	Implementation should follow ACSA's backup policy. - Provide the **data location or guideline** for ACSA to create backup scheduled jobs accordingly**.** **- Provide the restoration test** report or evidence. Otherwise, provide justifications for exemption approval.	**Database,**
120	Contingency Planning	Resilience Mechanism	Establish resilience mechanism, such as failsafe, load balancing, hot swap, implemented to achieve resilience requirements in normal and adverse situations for ensuring the delivery of critical services under all operating states (e.g., under duress / attack, during recovery, normal operation) The designed resilience mechanism should be tested before launching into production. [ACSA Requirement] For the systems that require high availability, redundancy of network provided by telecom carriers and redundancy of network lines and devices of the company LAN shall be in place, depending on the level of required availability. Network redundancy shall be designed with below consideration. - For the redundancy of network provided by telecom carriers, usage of network from multiple telecom carriers shall be considered. - For usage of network from multiple telecom carriers, it shall be ensured that there is no physical network overlapping with leased lines. - Usage of network devices with redundant adapters and power supplies shall be considered. - At least 2 data backup copies in separate locations.	**Infrastructure design document** indicate the resilience mechanism. Otherwise, provide justifications for exemption approval.	Whole

Ref	Category	Control	Requirement	Expected Proof	Layer
121	Contingency Planning	Service Level Objective (SLO)	Service Level Objective (SLO) – Define system availability indictors (RTO and RPO) for system HA, DR, hardware failure or network outage scenarios. Those requirements are based on user requirement to setup and state in this NFR for service owner confirmation. Systems operations department have the right to comment the designed SLO whether feasible and properly ask for additional resource to achieve the SLO. Systems operations department has a systems support level table which simplify the service category to different support tiers, it is easy for job requester to decide what they need and assist system division for future review and reporting purpose.	**Documented** RTO, RPO and planned method for achieving the SLO. ACSA person in charge of the project would arrange discussions with business units/stakeholders to define the RTO and RPO.	Whole

Ref	Category	Control	Requirement	Expected Proof	Layer
122	Contingency Planning	Disaster Recovery Planning	Establish disaster recovery (DR) plan with detailed procedures for the application / solution. The plan shall be developed to accommodate main cases, such as unexpected disasters, system failures, and cyber-attacks, which may have a significant impact on system service continuity. The DR plan should be reviewed and agreed by relevant parties (e.g., User Department and ACSA Infrastructure team) and the DR plan must fulfil the service continuity requirement (e.g., RTO/RPO/availability time) for this the application.	**Documented** disaster recovery plan (e.g. with the failover and failback procedures, and test plan)	Whole
123	Contingency Planning	Disaster Recovery Planning Drill Test	The disaster recovery (DR) plan MUST be tested and approved by responsible parties (e.g., User Department and ACSA Infrastructure team) at least once a year 1) Document any identified discrepancy between designed procedures and actual performance 2) Update the procedure and obtain related parties (e.g., application manager) approval	**Provide the SOW to show that DR drill standby support is included, also mentioning that vendor will troubleshoot and fix any issues related to the supported system or service that failed to perform the DR drill.**	Whole

Ref	Category	Control	Requirement	Expected Proof	Layer
124	Contingency Planning	Business Continuity Planning	Work with related User Department to establish Business continuity plan (BCP) with detailed procedures for the provided service. The plan shall be developed to accommodate main cases, such as unexpected disasters, system failures, and cyber-attacks, data center out-of-service, network failure, short of staff, which may have a significant impact on system service continuity. Ensure the business service could be maintained in case there is no HA and DR available on the solution. BIA analysis should be conducted to define the system priority and resource allocation during emergency situation.	**ACSA should review and update the** business continuity plan which related to the solution when needed.	Whole
125	Contingency Planning	Business Continuity Planning Drill Test	Business continuity plan tested and approved by responsible parties (e.g., User Department and ACSA Infrastructure team) at least once a year 1) Document any identified discrepancy between designed procedures and actual performance 3) Update the procedure and obtain related parties (e.g., application manager) approval	**Report** of business continuity test result or feasibility analysis of the plan. Otherwise, provide justifications for exemption approval.	Whole
126	Infrastructure and Capacity	Prefer VM Infrastructure	[ACSA Requirement] Hosting new system on VM infrastructure as possible to increased operational efficiency and flexibility. (Only for on-premises solution.)	**Infrastructure design document** with indication of hardware planning	**OS,**
127	Infrastructure and Capacity	Single brand of Server Product	[ACSA Requirement] To efficiency to execute system management and maintenance, it **recommends** to select single brand of server product (etc. HPE server product) (Only for on-premises solution.)	**Infrastructure design document** with indication of hardware planning	**OS,**
128	Infrastructure and Capacity	Software license	[ACSA Requirement] Check and procure sufficient software license, network software license (etc. VPN, encryption software) for the project. For the handling of software asset in ACSA's environment, please follow ACSA's requirement	**Infrastructure design document** with indication of software license list	Whole

Ref	Category	Control	Requirement	Expected Proof	Layer
129	Infrastructure and Capacity	Leverage ACSA Backup Solution	[ACSA Requirement for on-premises system/service] Leverage existing NetBackup system for system data backup, unless the special reason or hardware limitation, avoid to setup standalone backup device. Following NetBackup general backup policy to perform system backup, specification requirement if any special request. Estimate the backup tape utilization for the project period and reserve budget to purchase backup tape after implementation.	**Integrate** with ACSA NetBackup system. Otherwise, provide justification to ACSA on any constraint or limitation.	Whole
130	Infrastructure and Capacity	New System Utilisation Rate	[ACSA Requirement] Following system resource utilization standard (CPU < 60%, Storage < 65% in average) as the new system basis specification requirement.	**Report** of summarised resource utilization rate for all systems	Whole
131	Infrastructure and Capacity	Synchronise Deployment between Different Environment	[ACSA Requirement] Program deployment is expected to be synchronised on stand-by machine, backup machine, HA and DR system if they are applicable. The change result check should be conducted to ensure the deployed solution version is consistent across all environment.	**Screenshot** proof the change applied to source system (e.g., production) is synchronised to target system (e.g., HA, DR)	Whole
132	Application Design Principle	User Friendly Interface	[ACSA Requirement] Provide sufficient user function and interfaces to avoid any end user operation issue which result to create data patching and operation job request, those user interface are expected design as GUI (Window) or menu driven (AS400, AIX, Unix and Linux). Command line execution is not encouraged adopting for user or system operation's daily operation job. [ACSA Requirement] Data patching must not be treated as the procedure or solution to handle any job which without system function support. Data patching basically is prohibited except system incident, job request or human error scenario. If application has limitation which finally cannot provide user interface, corresponding user procedure should be created and provide to user review and confirmation. [ACSA Requirement] Adopting user self-service to improve customer and end user experience, it also can achieve the goal for fast deliver result. System job run as automation to reduce human intervention save operational manpower. * The design principle should be adopted in all applicable components. Where the principle could not be followed, please provide list of not applicable components and justification for such design.	**List of functions**, if any, which could not be provided with user interface. Provide justification to ACSA on any constraint or limitation for such implementation.	**Application, Administration Portal- if any,**

Ref	Category	Control	Requirement	Expected Proof	Layer
133	Application Design Principle	Extendable Change on Application	[ACSA Requirement] For future enhancement purpose, the application changes should be extendable and configurable. *The design principle should be adopted in all applicable components. Where the principle could not be followed, please provide list of not applicable components and justification for such design.	**Provide the high-level design for future system/application extension approach.**	Whole
134	Application Design Principle	File & Data Housekeeping Automation	[ACSA Requirement] For any newly created file in the job request, the file housekeeping and reorganization must be taken care, especially the file size grow rapidly in a short period. This file housekeeping and reorganization can be handled by the program automatically (e.g. by setting the parameter such as period range to purge). In case the file cannot be reorganized during the online period (e.g. file is locked all the time during the online period), inform responsible team to perform in maintenance time. System health level should be maintained with average of the system storage below 65% utilization criteria. Log cleanup (keep 3 months), log archiving , file re-organization, report cleanup procedure must be setup and execute regularly, typically they run as automatically, only manually execute is allow after get systems operations department consent. Data destruction is feasible upon ACSA request and data destruction procedures MUST include logging details of the destruction (i.e., date/time stamp, method of destruction). Data deletion followed by media disposal requires dedicated software to prevent data from being restored and the deletion evidence shall be recorded.	**List of scheduled job** for performing file and data housekeeping. For data level, confirm with business owner for the data required to be deleted regularly or on request.	Whole

4.4 Project Management Service Requirements

Vendor is expected to assign a Project Manager to monitor the delivery and implementation of the stated project for ACSA. The Project Manager is responsible for the followings:

a. Act as the primary project manager and focal point of contact.

b. A clear project team structure diagram

c. Clear project assumptions, your responsibility and ACSA 's responsibility

d. Project risk matrix and corresponding action to minimize risk

e. Manage subcontractors and ensure delivery of the following

    i. Delivery items as defined

    ii. Meet schedule

    iii. Deliverables must meet defined quality

    iv. Define and maintain change control management

f. Develop and maintain the master project schedule ("Master Project Schedule") on these infrastructure implementation services which identifies and assigns tasks to both the supplier and ACSA project participants, identifies major milestones for the efforts of the project team, identifies estimated dates on which they occur and indicates critical path for the overall project.

g. Measure, track and evaluate progress against the Master Project schedule and specific project schedules.

h. Resolve deviations from the project schedule with the supplier and ACSA's project manager.

i. Review project tasks, schedules and resources and make changes or additions, as appropriate.

j. Implement the Project Change Control Procedure ("PCR") in conjunction with the supplier and ACSA's Project Manager(s);

k. Provide the Project Escalation Procedures.

l. Participate in regular scheduled weekly meetings with the supplier and ACSA to discuss the status of the Implementation and prepare the Project Status Report.

4.5 Support Service Scheme

1. The proposal should describe the detail of the ongoing support service~~,~~ including telephone/email/on-site response time and business/non-business hour support to cover 24 hrs operation

2. Vendor should state the details of support service provided, the baselines of support service are:

    - Support service should include, but not limit to, major/minor patching (security, software, etc), application/software/hardware troubleshoot etc.

- Phone, email, remote and onsite support services
- Health check (every month) to the whole solution should be provided to ensure the stability of the system. Health check report should be submitted after every health check

3. The proposal should contain the service scope of System Integration Testing (if any), User acceptance Testing deployment, Soft launch deployment (if any), Production deployment and Production support.
4. The proposal should provide all proposed software(s) lifecycle information list (i.e. OS, Server OS etc.)
    - Provide the end of support date
    - All program / software and or it related license minimum lifecycle not less than 5 years
5. In future, in case of any end-of-support announcement by the original manufacturer of the product, tenderer needs to inform ACSA within one month after the announcement.

4.6 BCP Development Service Requirements

Supplier is expected to assist ACSA develop its business continuity plan (“Business Continuity Plan” or “BCP”) for the Production IT infrastructure. Detailed scope of the Services is as follows:

a. Assist ACSA to establish disaster recovery strategy and organization:
    1. Define disaster definition, business continuity plan scope and assumption in the context of your IT organization
    2. Define roles and responsibilities of each team.

b. Develop pre-disaster planning activities list.

c. Develop procedures for disaster notification.

d. Develop authorization and declaration procedures.

e. Develop a plan and procedures for invoking and executing the BCP.

f. Identify contact points for all disaster recovery team members, vendors, services vendors, suppliers, and emergency services.

g. Develop guidelines to implement process to return to permanent site or a re-constructed new primary site, including:
    1. Repair facility or new construction.
    2. Replace or relocate hardware.
    3. Recall of information to the permanent site.
    4. Perform data integrity checking after returning to the permanent site.

5. Continuity of normal business environment.

h. Develop maintenance schedule of the plan.

SECTION 5 PRICING AND COST STRUCTURE

5.1 General Costing Information

1. The proposal should clearly state or define the cost for initial setup
2. The proposal should state clearly on cost and it supported requirement(s) or function(s).
3. The proposal should clearly state and define the projected cost for ongoing maintenance fee. All cost should show clearly the breakdown for each item (esp. the maintenance cost breakdown)
4. The proposal should show clearly the one time investment cost and maintenance fee for the next 5 years.
5. The proposal should clearly state or define the cost for expected upgrade for long term operation.
6. The proposal should clearly state or define the lifetime of the investment for technology upgrades
7. The proposal should clearly state or define the license fee
8. The proposal should clearly state or define 3rd party license fee involved in the project.
9. The proposal should provide 5 years Total cost of ownership (TCO) for this project. Calculation and assumption should be stated clearly.
10. The proposal should separate the years spending cost (Owned & Rental) into One-off and On-going.

Please follow the below format the cost proposal:

	One-off			On-going				
	Items	Vendor / System Team	Estimate Cost	Year 1	Year 2	Year 3	Year 4	Year 5
HW			0	0	0	0	0	0
SW			0	0	0	0	0	0
Services								
	Total							

11. The proposal should provide the estimated operation cost from 5th year.
12. The proposal should clearly state that no additional cost for ACSA if the project is delayed.
13. Provide cost breakdown for new features.

SECTION 6 EXECUTION

6.1 Document Deliverables

Below listed item should be treated as project deliverables. If there are any extra documents required in the project, vendor should suggest to ACSA in the proposal with reasons and benefits.

1. System Requirement Specification
2. Functional Design Specification
3. Technical Design Specification
4. Test Plan, Test Scripts and Test Result for Unit Test
5. Test Plan, Test Scripts and Test Result for Stress Test
6. Test Plan, Test Scripts and Test Result for System Integration Test
7. Test Plan, Test Scripts and Test Result for Regression Test
8. User Manual
9. System Administration Manual
10. Migration Plan
11. Rollout & Cutover Plan
12. Source Code and related objects/APIs
13. Business Continuity Plan
14. Operation Manual

6.2 High Level Milestones

Please outline the major activities required during execution. Attach your proposed execution plan, including an estimate of ACSA's headcount, resource set and time required for execution of your proposed solution.

Your response should include the High Level Milestones Schedule in the following format:

Milestones	Responsibility	Timeframe

6.3 Payment Milestones

Payment Milestone	Software[2]	Services[3]
Signing of agreement / quotation	50%	20%

Delivery of Infrastructure Development	10%	10%
Delivery of Application Development	10%	10%
Completion of User Acceptance Test (UAT)	10%	20%
Production Rollout	15%	20%
After nursing period	5%	20%

** Note :

1. The above payment terms can still be changed as long as it is reasonably agreed by the Project team (IT and business staff) and Project Sponsor (related Division Head from IT and/or Business).

2. The above mentioned "Software" means standard package or application (i.e. Win OS license, SQLCAL or Netbackup etc.).

3. The above mentioned "Service" means System Integration ("SI") service (i.e. System develop/ implementation by ACSS, CSI or other system customization by vendor(s) for ACSA etc.).

6.4 Implementation Risks

Please provide your assessment of the risks to ACSA associated with implementing your proposed services.

6.5 Implementation Service Management

1. If you have any methodology for managing IT infrastructure & operations, please elaborate. Please include information about how operation status will be disseminated, service review process, problem escalation procedures and the management of risks throughout the service period.

2. ACSA recognizes that your proposed solution will include involvement of multiple vendors, however ACSA requires you to be the Primary Vendor to control and account for the performance and delivery of its subcontracting partners. If applicable, describe the process by which you would manage subcontracting partners.

3. You should be agreeable to work with any other vendor(s) that ACSA may select to implement new systems in the future.

6.6 Service Level Agreement

Please provide the SLA for the proposed solution. In case of quality downgrade, schedule delay due to implementer faults and errors or poor project management, etc. ACSA reserves the right to charge according to the SLA provided by the proposed vendor.

Consider providing a quality baseline such as

1. System and solution availability

2. Mean time between failures (MTBF), Mean time to repair (MTTR) and Recovery Time Objective (RTO).

3. Functions and features do not meet with the proposal

In case of problem occurs, ACSA will treat as system or application fault or malfunction if proposed solution cannot provide the following proof or evidence

1. Application healthiness report
2. Hardware healthiness report
3. Network abnormal behavior
4. System and application log
5. Maintenance service
6. Service hour coverage

6.7 Penalty Scheme

The proposal should state the penalty scheme in case of project delay, system failure and unhandled exceptional scenario. The vendor should also define system failure definition and service unavailable definition in the scheme.

Sample scheme:
System Down due to system failure, then deduct maintenance fee as penalty.
<Deduction> = <Monthly Maintenance Fee> * (<Number of days of system down>/30)

6.8 Ongoing Maintenance Support

For ongoing support, clearly provide the following

1. Scope
2. Schedule / Service Hour Coverage
3. Vendor responsibility
4. ACSA responsibility
5. Quality baseline
6. Early termination criteria by ACSA (In case vendor cannot meet quality baseline)

SECTION 7 ACCEPTANCE CRITERIA

All proposals will be evaluated base on cost and aesthetics. We will reserve the right not to explain to proposal senders the reason why their offers were not chosen. However, below consideration may apply for vendor selection:

1. Management Commitment
   - The quality of the vendor’s proposed management and technical personnel to be assigned in the event of an Agreement, and vendor’s commitment to maintaining key personnel on the engagement.
   - Vendor’s credibility and approach to developing and maintaining a good business relationship with ACSA.
2. Local Resources
   - Vendor’s resources should be able to support onsite services as ACSA environment may not support remote access.
3. Flexibility of Business Arrangements
   - The vendor’s ability and willingness to propose terms that are appropriate to the dynamic and competitive environment in which ACSA operates, and provide ACSA with maximum flexibility in terms of the Services provided and the fees charged.
   - ACSA expects vendor to adjust to changes in technology, size or volume of the Services, and overall business requirements of ACSA during the course of any agreement.
4. Work Approach
   - The degree to which the vendor’s proposal satisfies or exceeds the ACSA requirements, the completeness of the Services, and the quality of the proposed solution to provide consistently high quality Service for ACSA.
   - The vendor’s willingness to advance concrete solutions in its response, not defer matters to later stages, and to complete negotiations on a timely basis in accordance with ACSA’s schedule.
5. Technical Competence and Experience in Providing Comparable Services
   - The vendor’s specific Technical Competence, experience and demonstrated ability in providing the Services to other companies on a scale and at a level of complexity comparable to the Services described in this RFP.

ACSA reserves the right to reject all responses, to accept one which is not at the lowest cost or one which provides a lesser or larger range of services than indicated in this RFP.

SECTION 8 GEOGRAPHIC SCOPE

The rights, duties, and obligations of each party are valid in both Hong Kong and PRC expect that all licenses are valid as specifically granted.

******* End of Document *******