MCB Arif Habib Savings and Investments Limited

IT Audit Report

Net Promoter Score Process

December 2021

Strictly Private and Confidential

pwc

A·F·FERGUSON&Co.

Limitations and Responsibility

This report has been issued by A. F. Ferguson & Co. solely for the use of MCB Arif Habib Savings and Investments Limited only (hereafter referred as 'MCBAH' or 'Company'), and, without our explicit written approval, these reports (or any part thereof) should not be disclosed to any third party. Without our explicit written approval, it is also not allowed to quote from our reports, regardless whether this is done with or without acknowledgement of its source. We explicitly mention that our reports are not intended and cannot be used in any legal proceedings.

Table of contents

1

Executive summary

Executive summary

Background

MCB Arif Habib Savings and Investments Limited is using Net Promoter Score (NPS) methodology in order to measure customer loyalty through feedbacks being received via Short Message Service (SMS).

This exercise is carried out on annual basis or when needed wherein an SMS on a pre-defined and approved template and scale is shared with existing customers of the entity with the help of a portal provided by Intellexal Solutions (Pvt.) Ltd. on a set criteria requiring them to rate the services of MCB Arif Habib being provided to them. The customers in return reply with the desired score through the SMS gateway and the results are then captured in the entity's database.

Scope of service

S. No.	In-scope System	Details
1.	**SMS Gateway**	Vendor based – Intellexal Solution (Pvt.) Ltd.
2.	**Core Database**	Oracle 12c Enterprise Edition Release 12.2.0.1.0

Approach and Methodology

Our approach for IT Audit is structured around five clearly defined phases. Key aspects of our approach are:

i. <u>Planning</u>

In this phase meetings were conducted with Mr. Moiz Ali (Head of Customer Services) and Mr. Shabbir Hussain (Head of Information Technology) to finalize a mutually agreeable project plan. Further, nature, timing and extent of our procedures were finalized.

ii. <u>Understanding of Controls</u>

During this phase, we have obtained the understanding of the Net Promoter Scoring (NPS) process, in-scope systems governance mechanism, operating units, business and IT setup and have gone through the available documentation to develop our understanding of in-scope database IT security controls.

iii. <u>Assessment of Suitability of Design of Controls</u>

In this phase, we have identified the controls implemented and have focused on suitability of design of controls to meet control objectives. To determine the suitability of design of controls, we have focused on the following:

Executive summary

Approach and Methodology (Cont'd)

iii. Assessment of Suitability of Design of Controls (Cont'd)

- Ability of the controls to prevent and detect errors.
- Ability of the controls to support information's Confidentiality, Availability and Integrity.

iv. Assessment of Operating Effectiveness of Controls

In this phase, tests of operating effectiveness of the controls with the objective that controls are placed in operation and are operating effectively within the review period have been conducted.

Test plans were prepared in this phase and accordingly procedures were executed. Results of our assessment and findings were discussed in detail with the management.

v. Completion and Reporting

The last phase of the project is engagement completion, draft report compilation and issuance of final report.

Meetings were held with the relevant management personnel at MCBAH to understand the internal controls environment related to Company. Information gathered in those meetings was corroborated through various review procedures, PwC's scripts were used to review databases and walkthroughs of NPS process were performed.

Risk Priority and Impact Assessment

The table below provides a definition of the risk priority used in our report

Risk Priority	Definition
High (H)	Finding is pervasive in nature and results in either significant non-compliance of the company's policies and procedures or exposes the MCBAH's information systems to internal or external threats which if exploited may compromise confidentiality, integrity or availability of information systems.
Medium (M)	Finding results in either non-compliance of the company's policies and procedures or exposes the MCBAH's information systems to internal or external threats which if exploited may affect confidentiality, integrity or availability of information.
Low (L)	Observation has secondary significance with suggested improvements to enhance the internal controls or efficiency.

Executive summary cont'd

Caveats

This report is intended for the benefit of the Company, its owners and management and is not planned or conducted in contemplation of reliance by any third party or with respect to any specific transaction. Therefore, items of possible interest to a third party may not be specifically addressed, or matters may exist that would be assessed differently by a third party, possibly in connection with a specific transaction. You may not authorize any third party to rely upon any of the deliverables without our prior written consent. For the avoidance of doubt, the provisions of this paragraph are expressly intended to preclude, among other things, all references to AFF or PwC in press releases, periodic filings with regulators, or communications with stakeholders without our prior written consent.

The work was rendered with an understanding that the management of the Company will indemnify and hold harmless M/s A. F. Ferguson & Co. (the Consultants), its partners, directors, agents and employees from, and against, any and all costs, expenses, losses, claims, demands, actions, suits or proceedings paid, incurred or suffered or made or initiated against them by any third party arising out of or in connection with the services. In addition, any liability of the Company shall not be a liability of the Consultants, its partners, directors, employees and agents. However, the liability of the Consultants for any loss or damage caused, as a result of negligent performance of the services or action thereto, shall be limited to and not exceed the amount of fee paid to us.

A.F.Ferguson & Co. does not provide the assurance on the reliability, integrity and accuracy of the results which were obtained historically pertaining to NPS Survey.

2

Detailed findings

2.1

NPS System Process Review

Finding 1.1

Results might comprise the responses received from unregistered customers / entities

Medium

Issue

It has been noted based on our review that when customers respond to the survey on a pre-defined scale through specified gateway then those results are directly captured in the Oracle 12c database which is the core database of the entity. There is no such restriction which disallows the response being received is only from the registered contact number of the customer. Response in any format can be received from any contact number depending on the literacy of the customer.

Risk

Responses being received from any individual / entity outside the registered customer portfolio can lead to

- Integrity of the results being compromised.
- Unrealistic results being portrayed to the managements

Recommendation

It is recommended that responses received from those customers should only be considered in the final result who are the registered contact of the entity.

Management response / action plan	Responsibility	Timelines
At the time of result compilation, we only used those responses whose numbers were in the initial list used to send out the SMS. .	Quality Assurance & Customer Service	N/A

Finding 1.2

Results may also comprise the responses received from employees and internal stakeholders

Medium

Issue

It has been noted based on our review that when customers respond to the survey on a pre-defined scale through specified gateway then those results are directly captured in the Oracle 12c database which is the core database of the entity.

There is no such restriction which disallows the response being received from employees and internal stakeholders. Responses of employees and internal stakeholders also form the final result statistics.

Risk

Responses being received from any employees and internal stakeholders can lead to

- Integrity of the results being compromised.
- Unrealistic results being portrayed to the managements

Recommendation

It is recommended that responses received from employees and internal stakeholders should not be considered in the final result.

Management response / action plan	*Responsibility*	*Timelines*
Noted. We will exclude employee accounts at the time of compiling NPS results.	Quality Assurance & Customer Service	Jan-2022

Finding 1.3

Manual intervention at the stage of results extraction

Medium

Issue

Marketing department or customer services and quality assurance department requests the IT department for the extraction of the responses received by the customers to assess and evaluate the results instead of directly being able to review and inspect the results through a set platform such as front-end dashboard.

Risk

Extraction of results with the help of external department such as IT runs at the risk of:

- Intentional or unintentional modification or falsification of the results.
- Integrity of the results being compromised

Recommendation

It is recommended that a front-end dashboard should be made available to the relevant user departments which should be integrated with the database in order to review and extract the desired reports comprising the responses received on real time basis.

Management response / action plan	Responsibility	Timelines
Noted. We have already planned to build real-time MIS and dashboards with systematic result compilation	Quality Assurance & Customer Service	Jan-2022

2.2

Technical Review

Finding 1.4

Improvement needed at the Database

Medium

Issue

Completeness, accuracy and validity of the information processed by the system and the security of the system are reliant on the level of strength and effectiveness of the access controls in place.

Further, passwords, act as a critical access control used to authenticate users and restrict access to database and sensitive data. No matter how strong the organization internal controls are, the role of strong password remains significant.

During the review of database (Oracle 12c) where results of NPS survey are fall, following issues identified:

1) 2 DB users ID were identified with default profile including 'SMS' and 'CRM' accounts. Further, parameters for the default profile are following:

User Name	Last Login	Profile
SMS	11/18/2021	DEFAULT
CRM	11/18/2021	DEFAULT
PROFILE: DEFAULT		
Parameter	**Settings Defined**	**Recommended Practice**
FAILED_LOGIN_ATTEMPTS	10	5 attempts
PASSWORD_LIFE_TIME	Unlimited	90 days
PASSWORD_REUSE_MAX:	Unlimited	10
PASSWORD_VERIFY_FUNCTION	Null	This is used to enable length and complexity

Risk

Default profiles are predefined set of controls which covers primary authentication and security mechanism including password parameters. Settings defined in these profiles are generally 'Unlimited' which can lead to unauthorised and misused of DB accounts.

Weakness in password standards may expose systems to be compromised by intruders and unauthorized internal users and can potentially lead to exposure of sensitive data and impact the integrity of data and information.

Finding 1.4
Improvement needed at the Database (Cont'd)

Medium

Issue

Further few more profiles were identified for DB Users where password parameters were not adequately configured including DBA profile allotted to database administer. Discrepancies of those profile are mentioned below: Further, completeness, accuracy and validity of the information processed by the system and the security of the system are reliant on the level of strength and effectiveness of the access controls in place.

PROFILE: MCBAH_USERS		
Parameter	Setting Defined	Recommended Practice
PASSWORD_REUSE_TIME	UNLIMITED	365 days
PASSWORD_REUSE_MAX	UNLIMITED	10
PASSWORD_VERIFY_FUNCTION	NULL	This is used to enable length and complexity
PROFILE: MCBAH_DBA		
Parameter	Settings Defined	Recommended Practice
PASSWORD_REUSE_TIME	UNLIMITED	365 days
PASSWORD_REUSE_MAX	UNLIMITED	10
PASSWORD_VERIFY_FUNCTION	Null	This is used to enable length and complexity

2) 1 database link was found during the period under review where approvals of DB link was not available for our review. Details of link is as follow:

DB Link	User	Host	Created
DBLINK.REGRESS.RDBMS.DEV.US.ORACLE.COM	PROXY_USER	mcbah0	30-Sep-18

Risk

Unauthorised and unprotected database link there is a risk if this database is compromised, any linked database might also be compromised via a database link.

Finding 1.4
Improvement needed at the Database (Cont'd)

Medium

Recommendation

It is recommended that management should consider implementing following:

1. Establishing appropriate user password profile with parameter settings as per the best practice. Also, a separate profile with stringent parameters should be created and allotted to database administrators. Super user / privileged accounts access should be documented with ownership and authorized by the management.
2. All unauthorized database links should be removed. Database link should be created only after formal approval and valid business justification. Record should be maintained, and appropriate monitoring should be performed.

Management response / action plan	*Responsibility*	*Timeline*
1. All these IDs were moved to Default profile for test purpose during the issue resolution phase. Later, these IDs are reverted back to approved profiles. Implemented Password policy as approved by Management and also recommend during previous audit for selected profiles. 2. "DBLINK.REGRESS.RDBMS.DEV.US.ORACLE.COM" is dropped now.	IT Department	1. Resolved 2. Resolved

Thankyou