Deloitte.

Deloitte Risk Advisory
Pty Ltd
ACN 611 748 184
Grosvenor Place
225 George Street
Sydney, NSW, 2000
Australia

Tel: +61 2 9322 7000
www.deloitte.com.au
www.deloitte.com.au

08/05/2023

Victor Giang
Bendigo and Adelaide Bank
Waterview Walk, Docklands, Melbourne, Victoria 3055

1 Letter of Engagement

This Letter of Engagement is issued under the terms and conditions of the Master Services Agreement between Bendigo and Adelaide Bank Limited (**BEN**) and Deloitte Touche Tohmatsu (**Service Provider**), as executed on 31 January 2023.

2 Structure and Interpretation

(a) This Letter of Engagement (the **EL** or **Letter of Engagement**) is incorporated into and is part of the Agreement. To the extent of any inconsistency or conflict between the terms of an executed Letter of Engagement and the terms of the Agreement, clause 1.3 (Precedence) of the Agreement will apply. An inconsistency or conflict will be considered to exist if, regardless of the purpose of the provision, the relevant subject matter or action to be taken is dealt with differently in both the Agreement and this Letter of Engagement.

(b) This EL incorporates by reference the following Schedules to this EL:

NA

(c) In this EL, unless the context requires otherwise, a reference in this EL simply to a “Schedule” is to be read as reference to a Schedule to this EL.

(d) Other than those terms defined below, all capitalised terms in this Letter of Engagement have the meanings given to them in the Agreement.

Deloitte.

NA

3 Type of Services

☒ Advisory Services
☐ IT Services
☐ Staff Augmentation Services

4 Scope of Services

This assessment will focus on the following GCP control validation and configuration review. Deloitte will:

- Conduct the GCP environment discovery
- Conduct the Cloud configuration audit that will compare the current configuration of the GCP environment against industry standards and best practices to provide a view on the security posture of the services being used, as well as overall environment using Bendigo provided tools (e.g. Prisma Cloud) assess the security configuration of the cloud environment.
- Build the extra security testing cases on top of the following controls validation and configuration review that were requested by BEN:
    - Firewall Rule Review
        - Ensure GCP destinations are only allowed to limited traffic sources with a business justification. Note: access to the technical details of all business exemptions will be required to complete this task
        - Ensure only limited SaaS Services like Power BI traffic is allowed to egress from GCP
        - Ensure limited Public Cloud traffic from VPC in AWS and Azure (Azure AD) is allowed to enter GCP via on-prem NGFW/Partner Interconnect
        - Ensure all traffic in to GCP via Cloud Interconnect is encrypted.
    - VPC Service control validation
        - Review VPC Service Control Policies
            - GCP VPC Service controls only allow on-prem networks to enter GCP Lakehouse from the Internet to consume Public facing Google APIs
        - Penetration Testing from the Internet to ensure public facing Google APIs are not accessible (Strictly NO LOAD TESTING/NO DDOS TESTING)
            - GCP Lakehouse public facing APIs should only be accessible from BEN on-prem networks
    - Access control validation
        - Positive testing to ensure only authorised AD users can access GCP Lakehouse resources. BEN is to provide an AD account that is authorised to access GCP Lakehouse resources. The pentesting team will also use a standard BEN AD account to authenticate to GCP Lakehouse resources to validate access controls to the resources.
        - Negative testing to ensure use of Google Cloud Identity, local accounts, Administrator accounts is prohibited except with Bendigo's prior approval.
        - Associated Services including (but not limited to) Power BI and Jupyter Notebooks to use BEN AD accounts and verified through positive and negative use cases

Deloitte.

        - IAM rules strictly only allow Predefined roles (in a limited capacity where the custom role cannot fulfill the requirement) and Custom roles. Basic roles are strictly prohibited
    - Date Security validation
        - Verify use of IAM policies for all access to GCP Cloud Storage Buckets and BigQuery
        - Verify use of BigQuery Policy Tags for all access Verify use of Azure AD integrated SSO for all access to GCP Cloud Storage Buckets and BigQuery. Note that this will require BEN to supply details of all mandatory & optional tags, and how they are to be used
        - Verify use of Azure AD integrated SSO for all access to Power BI SaaS
        - Verify use of GCP ACLs for all access to GCP Cloud Storage Buckets
        - Verify VPC Service Controls integration with Vertex AI
        - Verify Access Transparency is enabled on GCP Lakehouse Project

5 Term and timelines

5.1 Term of engagement

Commencement Date: 03/07/2023
Completion Date: 31/07/2023

5.2 Milestones and due dates

Report Delivery Due Date: 07/08/2023

6 Responsibilities

6.1 Responsibilities of the Service Provider

Providing onsite security testing service to identify security weaknesses within the above scope and provide an opportunity to achieve security in depth.

6.2 Responsibilities of BEN

1. In addition to the responsibilities set out in the attached Terms and Conditions, you acknowledge that Bendigo is, and will continue to be, solely responsible for:

    a) Among other things (a) making all management judgements and decisions and assuming all management responsibilities, (b) designating an individual, preferably within senior management, to be responsible for your decisions and to oversee the Services, (c) providing oversight of the Services and evaluating the adequacy and results of the Services, and (d) accepting responsibility for the actions, if any, to be taken arising from the results of the Services.

    b) Establishing and maintaining an effective system of internal control over its operations and financial reporting, including, without limitation, systems designed to achieve its control objectives and its compliance with

applicable laws and regulations, including, without limitation, monitoring ongoing activities.

c) Provision of Information and data.

d) Informing Deloitte in a timely manner of any need to change the testing schedule.

e) Obtaining authorisation from and notifying all third parties that may be directly affected by this engagement of Deloitte's activities and timings of such activities.

f) Taking the necessary precautionary steps to ensure that the security testing will not, or will not be likely to, interfere with the functioning or availability of your systems prior to the testing commencing. Such steps should include but may not be limited to:

a. Preparing backups of all data, configurations, programs, networks and systems which could be exposed to the penetration testing, to enable your staff to restore your systems to the state in which they were prior to the security testing.

b. Updating and patching systems in accordance with current manufacturer and vendor recommendations.

c. Having your key support staff available during the security testing.

2. In connection with the Services, Deloitte shall be entitled to rely on all decisions and approvals of Bendigo.

3. You warrant that the IP addresses and URLs provided by Bendigo to Deloitte for testing are owned and used exclusively by you.

4. You acknowledge that:

1. Our ability to perform the Services and to meet any reporting deadlines is dependent on you meeting your responsibilities, as well as you providing us with instructions and making timely decisions.

7 Regulatory compliance

NA

8 Assumptions

We will provide the Services on the following assumptions:

1. Our Services

a) Will be based purely on advisory and consulting in nature

b) Cannot be relied upon to disclose irregularities, including fraud, other illegal acts, or errors which may exist; however, we will inform you of any such matters as come to our attention in the performance of our Services

Deloitte.

c) Will be subject to the limitations inherent in any test of the vulnerability of networks and web-based applications set out below

2. Our testing is scheduled to be performed in accordance with the below timetable. If your systems are unavailable for testing during a scheduled testing period, testing for that period will not be performed. If you are aware of system downtime during a scheduled testing period (for example due to systems maintenance) you should notify us in advance to make alternative arrangements.

9 Fees

The fixed fee payable for the Services is $ 68,741 (excluding GST and Expenses). The estimated costs for each service are described in the table below:

Service	Effort Estimate (Man days)	Total (excl. GST)
GCP Security Testing (scope highlighted in section 4)	35 days	$ 68,741
Total (excl. GST)		**$ 68,741**

10 General manner of performance

To complete the specific tasks most effectively, the following information is required before starting each activity. Additional information may be required during the project execution, and Deloitte will contact your designated contact as soon as possible to facilitate the activities.

Activity	Information requirement for Bendigo
General Requirement	• Provide project manager and technical contact details (email and phone number). • For any assets hosted by a third party (i.e., Hosting/Cloud provider), Bendigo to raise the necessary third-party penetration testing and obtain approvals. • Provide GCP read admin access account (viewer)
Firewall Review	• Provide firewall rules via an API dump of the rules implemented on the actual firewall instances (i.e. not just documentation)

Deloitte.

VPC Service Validation – API Access Testing	• Provide POSTMAN collection, which should have
	  ○ API endpoint URL(s)
	  ○ API payload/query strings to construct valid API requests
	• user account(s) for authentication
	• Ensure the testing environment is provisioned with test data before testing commences.
	• Provide access to an in-house SME to answer any questions that may come up with the POSTMAN collection

Access Control Validation	• Provide positive and negative testing cases • Provide accounts associated with the positive and negative cases • Provide services associated with the positive and negative cases • Provide GCP Lakehouse - Personas – Data Domain - Confluence (bbl.int) document
Data Security validation	• Provide BigQuery data masking requirement details

11 [Service Levels – IT Services only]

NA

12 [Service Credits – IT Services only]

NA

13 Deliverables

(a) The Service Provider must provide each of the Deliverables identified on Table 1 – Deliverables by on or before the Due Date specified below. Each of the Deliverables is subject to Acceptance or Document Review (as applicable) by BEN.

(b) Deloitte will provide BEN with a report detailing the results of the testing performed. This report will include the following key sections:

- **Executive Summary**: Directed at executive management – A general overview of the security level of the systems tested,

including major vulnerabilities and areas where the general approach to security needs to be improved. We explain the implications of our findings within the business context of BEN and provide an overall rating of security within the environment tested.

- **Summary of Findings**: Directed at operational management – A more detailed breakdown on the vulnerabilities and weaknesses identified for each portion of the engagement. We provide an explanation on the finding, as well as the associated risk to your business.
- **Detailed findings**: Directed at operational management and technical staff – A detailed description of exposures and their context, together with supporting documentation. We assess the impact and associated business risk of each identified exposure and make prioritised technical recommendations to be implemented to address the identified exposures. The priorities and 'Detailed findings' section will also be supported by technical appendices where required.

No.	Deliverable	Description	Due Date	Acceptance / Document Review Criteria
1	Security Testing Report	A report detailing the results of the testing performed and the recommendations.	07/08/2023	BEN accepts the security assessment report.

Table 1 – Deliverables

14 Key Personnel

The Key Personnel identified in Table 2 - Key Personnel will deliver the Services identified in this Letter of Engagement.

Key Personnel	EL Position	Key Position?	Utilisation Commitment (% FTE)	Location
Ashish Mahajan	Engagement Partner	yes	3%	Sydney
Andy Yang	Engagement Director	yes	3%	Brisbane
David Mitchell	Engagement Lead	yes	42%	Melbourne
Akalanka Karunarathne	Pentester	yes	26%	Melbourne
Ali Muhammad	Pentester	Yes	26%	Melbourne

Table 2 - Key Personnel

15 Provision of BEN Supplied Items

Deloitte.

(a) BEN will provide the BEN Supplied Items set out in Table 3 - BEN Supplied Items to the Service Provider in accordance with the agreed requirements and timeframes for the purpose of the Service Provider performing the Services and providing the Deliverables.

(b) BEN will cease to supply BEN Supplied Items at the EL Completion Date, unless it is otherwise set out in Table 3 - BEN Supplied Items that BEN has agreed to continue to provide the item.

No.	Description	Specific Requirement *(e.g. software licence type and number of licences, etc.)*	Date Required *(# weeks from EL Commencement Date)*
1	Testing Requirement	Please refer to 10. 10 General manner of performance	03/07/2023

Table 3 - BEN Supplied Items

16 Access to BEN Premises and Systems

BEN will grant the Service Provider access to such parts of BEN Sites and BEN Environments identified in **Table 4 - BEN Premises and Systems** and in accordance with clause 5.4 (Access to BEN Premises and Systems) of the Agreement.

BEN Site or BEN Environment	Specific Requirement *(e.g. when access required, by whom, etc.)*	Conditions of Access
BEN Dockland Office	Provide the office and network access on 03/07/2023 by Victor Giang	NA

Table 4 - BEN Premises and Systems

17 Subcontracting

17.1 Approved Subcontractors

The following Service Provider Subcontractors are approved for this Letter of Engagement.

Subcontractors Name	Scope of Services	Products / Services Supplied	Location
NA			

Table 5 - Approved Subcontractors

18 Reporting

The final report will be delivered five (5) days after project completion.

19 BEN Group Members

Victor Giang

20 Governance

N/A

21 Background IPR

N/A

22 Intellectual Property Rights

N/A

Deloitte.

23 Security requirements

N/A

24 Insurance

As per the MSA

25 Staff Augmentation Services

The Provided Persons identified in Table 6 - Provided Person(s) will deliver the Staff Augmentation Services identified in this Letter of Engagement.

Name of Provided Person	Type of work arrangement
Ashish Mahajan	Part Time Person Time Allocation Percentage: 3 %
Andy Yang	Part Time Person Time Allocation Percentage: 3%
David Mitchell	Full Time Person Time Allocation Percentage: 42%
Akalanka Karunarathne	Full Time Person Time Allocation Percentage:26%
Ali Muhammad	Full Time Person Time Allocation Percentage: 26%

Table 6 - Provided Person(s)

26 Other matters

N/A

27 Special Conditions

Inherent Limitations

Security testing has a number of limitations that must be understood to ensure the correct interpretation of the results:

a) Testing is usually restricted to a number of discrete tests which are performed during a small window of time. Where possible, Deloitte will identify additional tests which could be performed, but will not perform these without agreement from you.

b) Penetration testing is often performed in isolation, with very little background information on the nature of the system or systems that are tested (also referred to as "blind" testing). In this case, the tester will make a number of attempts to obtain Information about the systems and any associated vulnerabilities.

This type of Information is usually cryptic and incomplete, requiring the tester to interpret the data available in order to state their findings. The results are therefore a skilled interpretation of incomplete Information and

Deloitte.

not a statement of fact. We cannot warrant that the Information obtained is accurate or complete. The tester's results should not be relied on in isolation but as an important and necessary factor in your overall assessment of your security measures and the Application's potential vulnerabilities.

c) Testing in live or production environments will require a modified approach and restriction of the use of tools or techniques that may cause an adverse impact to the environment. More restricted testing may result in gaps, or areas of the environment which cannot be properly evaluated.

d) The tester will be unaware of the composition of your network, and whilst this may increase the risk of damage to your software and data, this is an aspect of the testing.

e) We do not perform destructive tests during a penetration test; however, if we identify potential vulnerabilities to require such an attack and the nature of the vulnerability, we will inform you.

f) The Information obtained and the results provided are only current at the time of testing (results represent a snapshot in time). New vulnerabilities will arise continually. It is therefore critical that patches are kept current, and security audits and vulnerability tests are performed regularly.

g) We will assume that Information provided by you is complete and accurate and will not subject such Information to testing except as described in this engagement letter.

Impact of Testing

You acknowledge that our Work within the scope of this Agreement may cause disruption to your network, systems, and processes. We will make reasonable efforts to limit the impact of testing on your network, subject to which, you acknowledge and agree that we will not be responsible for network or other disruption from testing which falls within the scope of this Agreement.

You agree to defend, indemnify and hold harmless Deloitte, its partners, and employees from and against any and all third party costs, expenses, demands, actions, suits, or proceedings paid, incurred or suffered by or made or initiated against them or any third party arising out of or in connection with our Services.

Deloitte Standard Terms and Conditions.pdf

Deloitte.

Execution

Letter of Engagement
This Letter of Engagement is made pursuant to, and forms part of, the Agreement between BEN and the Service Provider dated 08/05/2023 and may, by agreement between the parties, be executed electronically using DocuSign.

Signed for and on behalf of **Bendigo and Adelaide Bank Limited** (ABN 11 068 049 178) by an authorised representative:

DocuSigned by:
Ollie Murphy
B50F94AC2B80467...
Signature of authorised representative

Position Practice Lead - Customer & Data

Print Name Ollie Murphy

Signed for and on behalf of **Deloitte Touche Tohmatsu** (ABN 74 490 121 060) by its authorised representative:

Ashish Mahajan DocuSigned by:
Ashish Mahajan
7B62F00671184F2...
Signature of Partner

Ashish Mahajan
Print Name