

---

# Schedule 1 Statement of Work (pro-forma)

This Statement of Work is made on the 6th day of December 2023.

This Statement of Work (**SOW**) is made by and between UniSuper Management Pty Ltd (ABN 91 006 961 799) (**UniSuper**) and Deloitte Risk Advisory Pty Ltd (ACN 76 611 748 184) (**Contractor**) pursuant to the Master Services Agreement between the parties dated 13 October 2020 (**Agreement**), the terms of which govern, and are incorporated by reference into, this SOW.

## 1 PROJECT SUMMARY

UniSuper has a requirement to conduct HAAS Penetration Testing. The following test cases have been provided to the contractor.

### Component 1: External Penetration Testing of GCVE

Conduct an unauthenticated external penetration test on the UniSuper Google Cloud VMware Engine (GCVE) cloud environments. The purpose is to identify potential security vulnerabilities, assess the resilience of the infrastructure to external threats, and improve the overall security posture of our cloud deployment.

#### External Network Discovery:

- Conduct unauthenticated external network discovery to identify publicly accessible assets.
- Enumerate exposed services, open ports, and potential entry points.

#### Vulnerability Scanning:

- Perform unauthenticated vulnerability scanning on external-facing systems.
- Identify and prioritise vulnerabilities based on severity and potential impact.

#### Network Security Review:

- Evaluate the effectiveness of network security controls, including firewalls and network segmentation.
- Identify misconfigurations that could lead to unauthorised access.

#### Identity and Access Management (IAM) Assessment:

- Assess the effectiveness of IAM policies for externally exposed services.
- Identify misconfigurations or unnecessary permissions.
- Provide recommendations for improving access controls.

#### Google Cloud VMware Engine Security:

- Identify and address potential vulnerabilities or misconfigurations related to the VMware environment.

#### Data Storage Security:

- Identify potential data exposure risks and recommend mitigations.

#### Cloud Function and Serverless Security:

- Evaluate the security of serverless functions and cloud-based services accessible from the external network.
- Identify and address any security vulnerabilities or misconfigurations.

### Component 2: Assumed Breach Penetration Testing

The primary objective of this engagement is to simulate an assumed breach scenario by conducting a penetration test on our Google Cloud Platform (GCP) and Google Cloud VMware Engine (GCVE) cloud environments. The purpose is to assess the security resilience of the infrastructure when an attacker has gained low-privileged access and to

identify potential vulnerabilities that could lead to unauthorised lateral movement and exploitation.

**Lateral Movement Assessment:**

- Assess the security controls in place to prevent and detect lateral movement within the environment.
- Attempt to escalate privileges within the cloud environment using the low-privileged access.

**Vulnerability Scanning from Low-Privileged Accounts:**

- Perform vulnerability scanning and enumeration activities from the perspective of a low-privileged user.
- Identify potential vulnerabilities and weaknesses that can be exploited from a compromised account.

**Web Application Testing with Low-Privileged Access:**

- Assess the security of web applications accessible to a low-privileged user.
- Attempt to exploit vulnerabilities within web applications to escalate privileges or gain unauthorised access.

**Network Security Review:**

- Evaluate the effectiveness of network security controls, including firewalls and segmentation, in preventing lateral movement.
- Identify misconfigurations or weaknesses that could be exploited by an attacker with low-privileged access.

**Identity and Access Management (IAM) Assessment:**

- Assess the effectiveness of IAM policies and configurations from the perspective of a low-privileged user.
- Identify misconfigurations or unnecessary permissions that could facilitate further exploitation.

**Google Cloud VMware Engine Security:**

- Evaluate the security configurations of the Google Cloud VMware Engine deployment with a focus on assumed breach scenarios.
- Identify and address potential vulnerabilities or misconfigurations related to the VMware environment.

**Data Storage and Exfiltration Attempt:**

- Assess the security of data storage solutions accessible to a low-privileged user.
- Simulate data exfiltration attempts to identify potential weaknesses in data protection.

**Firewall Rule Validation:**

- Assess the effectiveness of the firewall configuration
- Assess the effectiveness of the firewall ruleset

We propose to allocate senior testers to UniSuper to assist with the above activities.

**2**

**TERM**

The term of this SOW commences during the week starting the 4<sup>th</sup> of December 2023 until the 25<sup>th</sup> of January 2024.

### 3 SERVICES

3.1 Using the following services, the contractor will address the test cases highlighted in the Project Summary above. Senior testers will be made available to support the following activities for UniSuper:

#### 3.1.1 Component 1

| Testing type                 | Details  | Effort (days) |
|------------------------------|--|---------------|
| External Penetration Testing | Unauthenticated time box web penetration testing of the GCP internet facing instances (up to 50 IPs) | 5 days        |

#### 3.1.2 Component 2

| Testing type                       | Details   | Effort (days) |
|------------------------------------|---|---------------|
| Assumed Breach Penetration Testing | Time box security assessment simulating a threat actor with low privileged access to the GCP environment. | 5 days        |
|                                    | Firewall rule validation  | 3 days        |

### 4 SPECIFICATION

N/A

### 5 OUT OF SCOPE

N/A

### 6 ASSUMPTIONS AND LIMITATIONS

The services and timelines provided in this SOW are based on the following assumptions and dependencies:

1. All information provided by UniSuper is true, correct, complete, and not misleading.
2. UniSuper will provide access to relevant systems and evidence on the commencement of the engagement.
3. Relevant UniSuper staff and stakeholders will be available for consultation during the project timeframe.
4. UniSuper will nominate a point of contact for matters relating to this engagement, including scheduling of meetings, information gathering, directing, arbitrating, and escalating engagement priorities
5. Deloitte has a flexible workplace policy. We expect our staff will work remotely. Should our staff require travel to UniSuper premises, we will work with you to arrange this.

6. Deloitte personnel proposed are available at the time of submission. If availability changes, team composition will be discussed and agreed with you.

## **7 ACCEPTANCE PLAN**

Acceptance of the final Penetration Testing Report

## **8 DELIVERABLES AND MILESTONES (TIME REQUIREMENTS)**

Penetration Testing Report

## **9 SERVICE LEVELS AND SERVICE LEVEL REBATES**

### **Service Levels**

Not applicable

### **Service Level Rebates**

Not applicable

## **10 NOTICES; PROGRESS REPORTS AND MEETINGS**

### **Operational Managers; Notices**

#### **Contractor**

|                   |  |
|-------------------|--|
| Address:          | 477 Collins Street, Melbourne, Vic, 3000 |
| Email:            | ogreiter@deloitte.com.au                 |
| Contract Manager: | Oliver Greiter                           |

#### **UniSuper**

|                   |   |
|-------------------|---|
| Address:          | 385 Bourke Street, Melbourne, Victoria 3000 |
| Email:            | Wasi.Rizvi@unisuper.com.au                  |
| Contract Manager: | Wasi Rizvi                                  |

### **Progress Reports & Meetings**

- N/A

## **11 RESPONSIBILITIES**

### **Contractor responsibilities**

No additional responsibilities other than those already noted in this document and Master Services Agreement.

## UniSuper responsibilities

In addition to any obligations in the Agreement, UniSuper will also do the following:

- Providing facilities/ virtual access for the testers, including sufficient system and network access
- Provide information related to in-scope test target, including IP ranges to target as part of the firewall ruleset validation exercise.
- Provide a single point of contact (a Team Lead or equivalent) for coordinating and allocating tasks.

## Third-party responsibilities (if applicable)

Not applicable

## 12 SERVICE FEE AND MILESTONE PAYMENTS

To be charged on a time and materials basis. The MSA day rate for a Specialist Manager is \$2,562, and the MSA day rate for a Senior Analyst is \$1,934. However, these services will be delivered at a discounted day rate of \$1850 for all grades.

For an estimated 13 business days effort across the agreed term, the estimated cost of services is **\$24,050 (excluding GST)**.

Services to be invoiced with the delivery of the penetration testing report.

## 13 PERSONNEL AND PROBITY

### Nominated Personnel

The Contractor's nominated key Personnel providing the Services under this SOW are:

| Title/Role              | Name           |
|-------------------------|----------------|
| Engagement Partner      | Oliver Greiter |
| Project Director        | Arman Kurt     |
| Senior Security Testers | Various        |

## 14 SECURITY REQUIREMENTS AND OTHER DIRECTIONS

### Security Requirements

#### Penetration Testing Terms and Conditions

This letter and our standard terms and conditions (the "Terms") set out the basis on which we will provide our Services to you. Where an inconsistency arises between this letter and the Terms, the terms set out in the letter will prevail.

#### 14.1 Assumptions

We will provide the Services on the following assumptions:

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

- 14.2 Our testing is scheduled to be performed in accordance with the above 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.

- 14.3 Inherent Limitations - Penetration 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) Vulnerability 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 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 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 vulnerability 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.

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.

#### 14.4 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.

#### Directions

- Not applicable
- 15 **DISCLOSED THIRD PARTY MATERIAL**
- Not applicable

## EXECUTION

**Executed** as an agreement

**Executed** by **UniSuper Management Pty Ltd**  
(ABN 91 006 961 799) by its authorised  
representative:

)  
)  
)  
)

.....  
Authorised representative

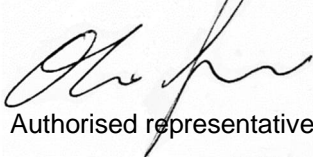
.....  
Title

.....  
Full name

.....  
Date

**Executed** by Deloitte Risk Advisory Pty Ltd (ABN  
76 611 748 184) by its authorised representative:

)  
)  
)  
)

  
Authorised representative

**Partner**

Title

**Oliver Grieter**

Full name

**6<sup>th</sup> of December 2023**

Date