Template Statement Work

Statement of Work – Master Services Agreement

Annexure to Master Services Agreement

Ausgrid Operator Partnership trading as Ausgrid (**Ausgrid**)

Deloitte Touche Tohmatsu (**Supplier**)

Number 1

1. Overview

1.1 Terms which apply to this Statement of Work

The terms of the Master Services Agreement between Ausgrid and Deloitte Touche Tohmatsu (Supplier)) apply to this Statement of Work. Once signed, this Statement of Work will become part of the Agreement and the Supplier must supply to Ausgrid the Contracted Items described in this Statement of Work.

1.2 Overview of Services

This Statement of Work is for the following project/engagement:

(a) Performing web application penetration tests for Ausgrid and PLUSES websites.

The core objectives of the Supplier's Activities are as follows:

(a) To identify and assist customers to understand the key risks and security vulnerabilities associated with their in-scope websites; and

(b) To identify gaps and inherent risks in data protection controls and identify any inconsistencies in security standards.

1.3 Use of Deliverables by Ausgrid Group Members

The supplier’s work is for the exclusive use of Ausgrid and must be used only by Ausgrid and only for the purpose set out in this document. The supplier will accept no responsibility to anyone (apart from Ausgrid) who is provided with or obtains a copy of our deliverable without our written agreement. The supplier reserve the right to include in our deliverable a statement limiting the use to which the report may be put, any limitations on the scope of the Services performed, and setting out the respective responsibilities of Ausgrid and the supplier.

2. Statement of Work Term

This Statement of Work is any other Statement of Work under which Orders are not required.

3. Services

3.1 Services in scope

The Services to be provided are:

(a) *Professional Services* - to deliver penetration testing services to assess and identify potential exposure to cyber threats including:

(i) Web Application Penetration Test

Web Application Penetration Test

The primary purpose of web application penetration testing is to identify and exploit vulnerabilities present in a web application and its components, including the associated infrastructure, and recommend practical solutions to make applications and systems under the scope of engagement more secure.

During testing, the supplier will use a web browser and penetration testing tools that mimic regular client activity as well as generate malicious traffic. The penetration testing assessment methodology incorporates the suggested testing techniques from standard methodologies, such as the Web Application Hackers Handbook (WAHH) and the OWASP Security Testing Guidelines v4.1.

These methodologies will cover many aspects of a web application, and any customisation of further testing will be evaluated during the testing period. These methodologies also cover common vulnerabilities, as highlighted in the OWASP Top 10 2017 and OWASP Top 10 2021.

Furthermore, besides manual testing, the supplier will use several automated tools that are designed to detect vulnerabilities in web applications such as Burp Suite and Nikto.

Application	URL	Comments
Ausgrid Main Website	https://www.ausgrid.com.au	Testing will be conducted in production.
PLUSES websites	https://pluses.com.au	Testing will be conducted in production.

A detailed report highlighting all the issues identified during the engagement including the associated technical risk posed to Ausgrid.

Assumptions

The supplier will provide the Services on the following assumptions:

1. 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, the supplier will inform Ausgrid of any such matters as come to the supplier's attention in the performance of the Services.
    c. Will be subject to the limitations inherent in any test of the vulnerability of networks and web-based applications set out below.
2. Testing is scheduled to be performed in accordance with the agreed timetable. If Ausgrid's systems are unavailable for testing during a scheduled testing period, testing for that period will not be performed. If Ausgrid is aware of system downtime during a scheduled testing period (for example, due to systems maintenance), they should notify the supplier in advance to make alternative arrangements.

Inherent Limitations

Penetration testing has several limitations that must be understood to ensure the correct interpretation of the results:

1. Testing is usually restricted to a number of discrete tests which are performed during a small window of time. Where possible, the supplier will identify additional tests which could be performed, but will not perform these without agreement from Ausgrid.
2. 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 several attempts to obtain information about the systems and any associated vulnerabilities.
3. This type of information is usually cryptic and incomplete, requiring the tester to interpret the data available to state their findings. The results are therefore a skilled interpretation of incomplete information and not a statement of fact. The supplier 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 Ausgrid's overall assessment of their security measures and the application's potential vulnerabilities.
4. Testing in live or production environments will require a modified approach and restriction on the use of tools or techniques that may cause an adverse impact on the environment. More restricted testing may result in gaps or areas of the environment, which cannot be properly evaluated.
5. The tester will be unaware of the composition of Ausgrid's network, and whilst this may increase the risk of damage to Ausgrid's software and data, this is an aspect of the testing.
6. The supplier will not perform destructive tests during a vulnerability test; however, if the supplier identifies potential vulnerabilities that require such an attack, the supplier will inform Ausgrid.

7. 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.
8. The supplier will assume that the information provided by Ausgrid is complete and accurate and will not subject such information to testing except as described in this statement of work.

3.2 Commencement date and expiry date

TBD

3.3 Exclusions

For the avoidance of doubt, the Services:

- Do not include the implementation of any recommendations contained in the deliverable.
- Do not constitute a source code review.

Further, the following areas are specifically excluded from the test:

- Business As Usual ("BAU") processes, such as patch management, change management, and access control.
- Test or review any control, feature, software package, or operating system not defined in the Services.
- Configuration review of any feature, device, software package, or operating system not defined in the Services.
- Re-test of the identified security vulnerabilities.
- Source code or development processes security review.
- Denial of Service ("DoS") exploitation, physical security, and social engineering.
- Authenticated web application penetration testing.
- Personnel security within Ausgrid and/or any third parties.
- Business partner systems or transmission security within any service provider's network.
- Any other test not explicitly defined in the Services.

3.4 Deliverables

The Deliverable to be provided is:

A formal report detailing the testing results. 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. The supplier will explain the implications of the findings within the business context of the customer and provide an overall rating of security within the environment tested.

- **Summary of Findings** (Directed at operational management) – A more detailed breakdown of the vulnerabilities and weaknesses identified for each engagement portion. The supplier will provide an explanation of the finding, as well as the associated risk to the customer's business.

- **Detailed Findings** (Directed at operational management and technical staff) – A detailed description of exposures and their context, together with supporting documentation. The supplier will assess the impact and associated technical 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.

Furthermore, any urgent findings items, such as Critical or High rated findings, will be raised with the management team as they are confirmed to assist with timely remediation.

3.5 Environment

N/A

3.6 Warranty Period

No warranty period

3.7 Specifications

The Supplier will utilise the following penetration testing assessment methodologies:

(a) OWASP (Open Web Application Security Project); and

(b) The OSSTMM (Open-Source Security Testing Methodology Manual).

These methodologies will cover common vulnerabilities, as highlighted in the OSSTMM and OWASP where applicable.

3.8 Step in

N/A

3.9 Disengagement

N/A

3.10 Service Levels

N/A

3.11 Ausgrid Data

N/A

3.12 Client Inputs

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 the supplier will contact your designated contact as soon as possible to facilitate the activities.

- Specify any maintenance windows that might apply to the environment.
- Request authorisation for penetration testing if a third party manages targeted systems.

4. Milestones and stages

The following dates constitute Key Milestones:

Key Milestone ID	Key Milestone	Date
1	Web Application Penetration Test	TBD

5. Acceptance Test Plan

N/A

6. Price

6.1 Price

The Supplier will be entitled to submit a Correctly Rendered Invoice to Ausgrid upon the completion of each of the following milestones:

Milestone Payment Number	Penetration Testing Service	Effort Estimate (Man days)	Total (Ex. GST)
Milestone 1	Web Application Penetration Test including report • https://www.ausgrid.com.au • https://pluses.com.au	11 days	$ 23,500
	Total	**11 days**	**$ 23,500**

6.2 Discounts, credits and rebates

N/A

6.3 Invoicing

The Supplier will be entitled to submit a Correctly Rendered Invoice to Ausgrid upon completion of each milestone.

7. Key Positions

Key Position	Responsibilities
Engagement Partner (Deloitte)	Engagement Partner
Quality Assurance Partner (Deloitte)	Ensure that standards and safety regulations are observed.
Director (Deloitte)	Interface with the Ausgrid and key stakeholders, including coordinating, preparing, and facilitating workshops and scoping.
Executive Project Sponsor (Ausgrid)	• Provide executive leadership • Allocate the required resources • Serve as the key decision-making body • Review issues, provide timely resolution, provide timely approvals • Report progress to stakeholders
Project Manager (Ausgrid)	• Review and revise deliverables • Manage resources and arrange meetings and/ or risks and issues as they arise • Ensure services are delivered within the agreed timeframe and scope as agreed with the project manager

8. Pre-approved Subcontractors

N/A

9. Governance

9.1 Governance procedures

N/A

10. Quality Plans

10.1 Quality standards

N/A

10.2 Certifications

N/A

11. Termination costs

N/A

12. Additional Terms

The provisions of the schedules of the Agreement marked below will apply:

□ Schedule 16 – Penetration or vulnerability testing, ethical hacking, web application security testing, vulnerability scanning, and vulnerability assessments

12.1 Return of Ausgrid Data

N/A

12.2 Business Continuity Plan

N/A

13. Special Conditions

N/A

Signing page – Statement of Work

Signed for **Ausgrid Operator Partnership** (ABN 78 508 211 731) by an authorised officer in the presence of

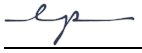
Francis Mason ←
Signature of Officer

Signature of Witness ← Francis Mason
Name of Officer (print)

Name of Witness (print) CISO
Office held

Signed for Deloitte Touche Tohmatsu **(ABN *74 490 121 060)***by an authorised officer in the presence of

 ←
Signature of Officer

 ← Gautam Kapoor
Signature of Witness
Name of Officer (print)

Eloise Powell
Name of Witness (print)

Partner
Office held