Prepared by Aurian Security
on behalf of CloudMonitor

Aurian
Security. Simplified.

Web Application Penetration Test

Technical Report

Version: 0.1
Report ID: CM-WAPT-2022-05-TR
Project ID: CM-WAPT-2022-05

15 July 2022

ACN: 639 930 528

903/50 Clarence St,
Sydney NSW 2000

1300 748 788
sales@aurian.com.au
www.aurian.com.au

Document Properties

Aurian Security Pty Ltd	
Client	CloudMonitor
Title	Web Application Penetration Test Technical Report
Prepared by:	Cameron Smith
Reviewed by:	James Coyne

Document Control

Version	Author	Purpose / Change	Date
0.1	Cameron Smith	Initial Draft	15 July 2022

Distribution List

Name	Title	Organisation
Rodney Joyce	Managing Director	CloudMonitor

Table of Contents

1. Introduction

Aurian Security is proud to present the results of the Web Application Penetration Test conducted on behalf of CloudMonitor.

This document details all vulnerabilities identified during the Web Application Penetration of CloudMonitor's in-scope portal application. The Technical Report is targeted at personnel that are responsible for remediating security issues in CloudMonitor's application infrastructure, as well as CloudMonitor stakeholders with a technical interest in the security of the portal application.

For each finding, Aurian has outlined a detailed description of the underlying issue, potential risk and impact to the organisation, as well as recommended remedial measures to minimise the risk of exploitation or eliminate the issue entirely.

A separate report CM-WAPT-2022-05-ER, containing a high-level overview of the engagement, the overall security posture, and related core remedial actions has been issued to CloudMonitor for review by management and executive-level staff.

2. Background

CloudMonitor is web-based solution that monitors Azure cloud consumption costs and looks for cost-saving opportunities by finding oversized resources and services that are no longer in use, as well as suggesting best-practices based on real-time utilisation patterns

CloudMonitor requested a security assessment of its portal application to gain an independent perspective on the risk to the application infrastructure and environment, as well as to assess the implementation of current security controls.

Any exposure of sensitive data contained within CloudMonitor's portal application may have extensive negative consequences for the organisation, including significant financial losses, notable reputational damage as well as the potential violation of various compliance standards. Furthermore, security flaws discovered and exploited within the portal application may have significant implications for other organisations in connection with CloudMonitor.

2.1. Security Review Scope

The security assessment was performed commensurate with the Aurian Security proposal (CM-WAPT-2022-05), dated 30 May 2022. The scope, security review performed, and testing methodologies are limited to those outlined at the time the proposal was agreed to by CloudMonitor.

Authenticated Web Application Penetration Testing was conducted against the public facing application front-end:

- https://aasj6cmdkqkljjoq.z8.web.core.windows.net/

The following accounts were used for testing the application: (role)

- cameron@aurian.com.au (Administrator)
- sales@aurian.com.au (AppCostGroupAdmin/AppCostGroupEditor)
- sales+1@aurian.com.au (ReportCostGroupViewer/AppCostGroupViewer)

2.2. Security Review Approach

Aurian held an initial discussion meeting on 15 June 2022 at 2:30 PM AEST to discuss the proposed security testing of the portal application and gain a deeper understanding of how the application functions and the technologies that are in use.

Additionally, Aurian reviewed the following documentation when performing the security architecture review: (author)

- AdminApp Roles and Permissions.pdf (CloudMonitor)

2.3. Security Review Exclusions and Restrictions

As agreed with CloudMonitor prior to the commencement of testing, the following exclusions and restrictions apply to the engagement:

- While Aurian may have identified vulnerabilities that have the potential to impact the availability of systems, at no point did Aurian conduct any means of Denial of Service (DoS) stress testing. If the application is required to have exceptional uptime service level agreements, the application should be stress tested at a later date.
- A Source Code Review was not performed on the application. As a result, there may be vulnerabilities present within the application that could be exploitable in exceptional circumstances or with a good working knowledge of the underlying codebase.

3. Findings Summary

During the engagement, Aurian discovered 5 security weaknesses that have implications for the overall confidentiality, integrity, and availability of the in-scope application services. The distribution of assessment findings, ranked by their overall risk according to Aurian's risk framework, is as follows:

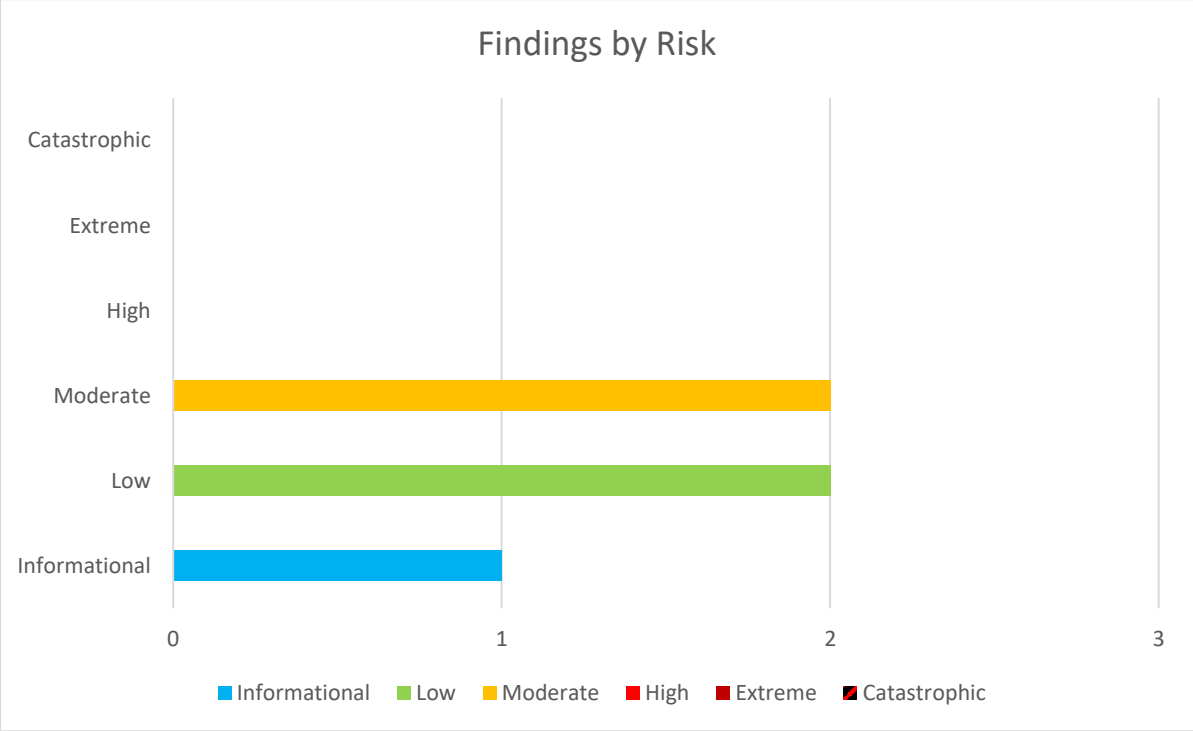

Figure 1: Risk Summary of Findings

All issues identified by Aurian have been manually verified and exploited (where applicable) to analyse and demonstrate the underlying risk to CloudMonitor and public users.

4. Core Strategic Recommendations

To assist CloudMonitor in addressing the risk and implication of security weaknesses identified during the assessment and preventing them and other similar issues arising in the future, Aurian recommends the following high-level actions be performed in conjunction with the specific remedial steps contained within each finding:

Session Management

In the current implementation, Aurian noticed that sessions appeared to still be active after an observed 2-hour idle window. Allowing long session lifetimes increases the window of opportunity an attacker has to brute force or hijack valid session tokens. Aurian recommends restricting session validity to one hour or less.

Transport Layer Security

Aurian identified that the application supports legacy TLS protocols, namely TLS 1.0 and TLS 1.1. These protocols contain a variety of cryptographic flaws and weaknesses and are no longer considered safe to use. The application must be configured to accept connections only over TLS 1.2 and the newer TLS 1.3.

Web Application Firewall

The current UAT environment is exposed to the public Internet and is not protected by a Web Application Firewall (WAF). A WAF helps protect web applications from common web exploits that could affect the availability, integrity and confidentiality of web resources. Aurian recommends that a WAF is placed in front of the application and configured such that all traffic is inspected for malicious activity.

Security Best Practices

Additional enhancements could be made to further tighten the security of the application, such as the addition of HTTP security headers. Additionally, all server banners should be configured such that they do not unintentionally reveal information that could be useful to an attacker.

5. Penetration Test Findings

5.1. Web Application Penetration Test

Finding ID	Risk	Description	Recommendation
WAPT-1	M (9)	**Sessions do not expire in a reasonable timeframe.** Impact: Medium (3) Likelihood: Possible (3) A web session is a user identifier resulting from a sequence of HTTP request and response transactions. Sessions are used to track user actions and establish an application context (access rights, display settings, dynamic data retrieval etc). Once a valid session has been assigned to an authenticated user, the session token is temporarily equivalent to the strongest authentication method used by the application, such as username and password, one-time passwords (OTP) and client-based digital certificates. During the engagement, Aurian consultants observed that the primary session token did not expire within an observed 2-hour period. Allowing long session lifetimes increases the window of opportunity an attacker has to brute force or hijack valid session tokens.	Aurian recommends revoking all sessions associated with a user after a pre-determined period has elapsed. More specifically, if a user is noted to be inactive for a period of 60 minutes, their associated session token should be invalidated.
WAPT-2	M (8)	**Missing HTTP security headers.** Impact: High (4) Likelihood: Improbable (2) HTTP security headers are a fundamental part of web application security. When implemented correctly, they protect the application against common vulnerabilities and attacks. The following headers were not supplied by the application: 1. Content Security Policy (CSP)	Aurian recommends serving all HTTP security headers to ensure the application has the best protection against current common and emerging threats, and as a defence in depth measure toward application security. Instructions for adding security headers to an Azure CDN endpoint can be found at the following URL: https://medium.com/datadigest/using-azure-cdn-to-specify-custom-http-headers-for-an-azure-static-website-hosted-spa-41a9b9ec1674 Aurian recommends the following values for each security header listed: 1. Content Security Policy

Finding ID	Risk	Description	Recommendation
		CSP defines approved sources of content that the browser may load, thereby allowing the developers the ability to whitelist the application's content sources. It can be an effective countermeasure to Cross Site Scripting (XSS) attacks and is widely supported, and usually easily deployed. 2. X-Frame-Options (XFO) The XFO header protects end users against clickjacking attacks. The header is used to indicate whether or not a browser should be allowed to render a page in a <frame>, <iframe>, <embed> or <object>, preventing the application content from being embedded into other sites. 3. X-Content-Type-Options (XCTO) The XCTO header specifically prevents Google Chrome and Internet Explorer from trying to mime-sniff the content-type of a response away from the one being declared by the server. It reduces client exposure to 'drive-by downloads' and the risks of user-uploaded content that, with crafted file naming, could be treated as a different content-type, such as an executable. 4. Referrer-Policy When a browser requests a resource, it typically adds a 'Referrer' header which indicates the URL of the resource from which the request originated. If the resource being requested resides on a different domain, then the Referrer header is still included in the cross-domain request. If the originating URL contains any sensitive information in any query strings such as a session token, then this information will be transmitted to the other domain which could lead to a security breach. 5. Permissions-Policy Earlier known as the Feature-Policy, the Permissions-Policy header provides a mechanism to allow and deny the use of browser features (access to geolocation, camera, full screen mode, auto play et.al), along with content within any <iframe> elements in the page. Being able to restrict features that sites you embed can use affords end users even greater protection.	Content-Security-Policy default-src 'none'; child-src 'self'; connect-src 'self'; font-src 'self'; img-src 'self'; media-src 'self'; object-src 'self'; script-src 'self'; style-src 'self'; 2. X-Frame-Options (XFO) X-Frame-Options SAMEORIGIN; 3. X-Content-Type-Options (XCTO) X-Content-Type-Options nosniff; 4. Referer Referrer-Policy "no-referrer"; 5. Permissions-Policy Permissions-Policy "accelerometer 'none'; ambient-light-sensor 'none'; autoplay 'none'; battery 'none'; camera 'none'; display-capture 'none'; document-domain 'none'; encrypted-media 'none'; fullscreen 'none'; geolocation 'none'; gyroscope 'none'; legacy-image-formats 'none'; magnetometer 'none'; microphone 'none'; midi 'none'; oversized-images 'none'; payment 'none'; picture-in-picture 'none'; publickey-credentials 'none'; sync-xhr 'none'; unoptimized-images 'none'; unsized-media 'none'; usb 'none'; vibrate 'none'; vr 'none'; wake-lock 'none'; xr-spatial-tracking 'none';" 6. HTTP Strict Transport Security (HSTS) Strict-Transport-Security "max-age=31536000; includeSubDomains" always; Note: Some security headers may not be support by all browsers. Note: CloudMonitor should audit the above default recommended security header values as some security restrictions may impact application functionality.

Finding ID	Risk	Description	Recommendation
		6. HTTP Strict Transport Security (HSTS) HSTS ensures that all communication takes place over a secure transport layer on the client side. Importantly, HSTS mitigates variants of man-in-the-middle (MiTM) attacks where communications can be intercepted, leaving the user vulnerable to further risk.	
WAPT-3	L (6)	**Insecure TLS protocols supported.** Impact: Medium (3) Likelihood: Improbable (2) Transport Layer Security (TLS) is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. TLS encryption can help protect web applications from malicious activities such as man-in-the-middle attacks. Additionally, TLS-protected HTTPS is quickly becoming a standard practice for websites. Vulnerabilities in older TLS protocols can allow attackers to intercept and tamper with data between applications and clients. This could include credit card data, intellectual property, credentials – all of which are an attacker's prime targets. The following insecure TLS protocols are supported by the application: 1. TLS 1.0 Among other weaknesses, TLS 1.0 is vulnerable to man-in-the-middle attacks, risking the integrity and authenticity of data sent between a website and a browser. Additionally, TLS 1.0 is no longer permissible for hosts that form part of an organisation's PCI DSS scope. 2. TLS 1.1 TLS 1.1 is based on a combination of MD5 and SHA-1, both of which are affected by a number of cryptographic weaknesses. It's successor, TLS 1.2, enables use of authenticated encryption	Aurian recommends disabling legacy TLS protocols (TLS 1.0 and TLS 1.1) and ensure that support for TLS 1.3 is added where possible. To configure a minimum acceptable TLS version for Azure Storage Accounts, please see Microsoft's instructions at the following URL: https://docs.microsoft.com/en-us/azure/storage/common/transport-layer-security-configure-minimum-version?tabs=portal

Finding ID	Risk	Description	Recommendation
		modes like Galois Counter Mode (GCM). This can replace the more traditional Cipher Block Chain (CBC) encryption mode, which has historically been a source of many flaws.	
WAPT-4	L (6)	**TLS cipher weaknesses and vulnerabilities.** Impact: Medium (3) Likelihood: Improbable (2) Transport Layer Security (TLS) is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A cipher suite is a set of algorithms that help secure a network connection that uses TLS. A number of issues arise from the use of weak cipher suites, including the following: 1. Sweet32 The Sweet32 attack allows an attacker to recover small portions of plaintext when encrypted with 64-bit block ciphers (such as Triple-DES and Blowfish), under certain (limited) circumstances. 2. BEAST The Browser Exploit Against SSL/TLS (BEAST) is an attack that leverages weaknesses in cipher block chaining (CBC) to exploit the Secure Sockets Layer (SSL) / Transport Layer Security (TLS) protocol. The CBC vulnerability can enable man-in-the-middle (MITM) attacks against SSL in order to silently decrypt and obtain authentication tokens, thereby providing hackers access to data passed between a Web server and the Web browser accessing the server.	Aurian recommends the following changes are made to mitigate the risks associated with the use of weak cipher suites: 1. Sweet32 a. Prefer minimum 256-bit cipher suites b. Limit the length of TLS sessions with a 64-bit cipher, which could be done with TLS renegotiation or closing and starting a new connection c. Disable cipher suites using 3DES 2. BEAST Disallow support for legacy versions of SSL and TLS, allowing only connections over TLS 1.2 and TLS 1.3.

Finding ID	Risk	Description	Recommendation
WAPT-5	I (2) 	**Services return installed product and version information.** Impact: Low (2) Likelihood: Remote (1) Information about software and technologies in use is vital to attackers looking to target vulnerable applications and services. This information can include the name of the technology or software in use, along with the specific version number that is running in the environment. An attacker can use this information to research known vulnerabilities and exploits that affect the version of software in use, or obtain a copy of the source code for the specific version in order to identify new, undiscovered and unpatched (zero-day) vulnerabilities. The following product information was obtained from server responses: • `Server: Windows-Azure-Web/1.0 Microsoft-HTTPAPI/2.0` Modifying application banners affords the application some extra protection from automated scanners and unskilled attackers but is less likely to prevent a motivated attacker from attempting to compromise the application.	Where possible, remove all banners that identify technologies and version numbers of software used in the application environment. It is recommended to remove the applications build version from any front-end component of the application.

Table 1: Web Application Penetration Test-Findings and Recommendations

6. Target Application Analysis

During our comprehensive analysis of the target application, Aurian identified and tested the following URLs and parameters in the frontend application:

Dynamic URLs: 33

Static URLs: 9

Total Number of Parameters: 33

Total Number of Unique GET Parameter Names: 1

A complete list of the parameters, dynamic and statics URLs that were tested during the engagement can be found in the associated '`Portal-Tested-URLs-and-Parameters.html`' file distributed with this report.

7. Aurian Testing Methodology

Aurian's testing methodologies are formulated from industry leading standardised methodologies including the Penetration Testing Execution Standard, Open Web Application Security Project Testing Guide, Information Systems Security Assessment Framework and Open Source Security Testing Methodology Manual.

Our security testing is heavily focused on the three major information security objectives:

1. **Confidentiality** – protecting information from being accessed by unauthorised parties;
2. **Integrity** – ensuring that information is not altered and that the source of the information is genuine; and
3. **Availability** – ensuring that information and services can be accessed by authorised, legitimate parties.

Penetration testing, by definition, is an authorised cyberattack on computer systems, and uses tools and techniques used by real attackers to compromise systems and gain unauthorised access to corporate networks. Therefore, any vulnerabilities and misconfigurations identified during penetration testing should be thought of as those that an unauthorised intruder could find while probing the network and connected systems.

Once testing has completed, any changes to systems or applications will be restored to the state as they existed prior to the commencement of the test.

7.1. Web Application Penetration Test

Aurian focuses on identifying vulnerabilities as defined in the Open Web Application Project (OWASP) Top 10 Most Critical Application Vulnerabilities.

The goal of this testing is to assess the resilience of the CloudMonitor in-scope application(s) to well-known vulnerabilities and sophisticated manual testing techniques and determine if the current defences are sufficient. Recommended mitigation strategies will be provided to assist CloudMonitor in improving where security may be lacking. Testing is performed across the Internet from Aurian's dedicated penetration testing network.

The test is comprised of five stages – Reconnaissance, Threat Modelling and Vulnerability Analysis, Exploitation, Post-Exploitation, and Reporting and Documentation.

7.1.1. Reconnaissance

The Reconnaissance phase is one of the most critical steps of a web application penetration test. Information gathering is done through the use of public tools such as search engines, framework discovery tools, and sending simple HTTP requests and specially crafted requests to determine the format of expected output. In many cases, is possible to force the application to leak information by disclosing error messages or revealing the versions and technologies in use.

7.1.2. Threat Modelling and Vulnerability Analysis

During the Threat Modelling and Vulnerability Analysis phase, our consultants will attempt to comprehend the deployed configuration of the infrastructure hosting the web application. Particular platform configuration errors can compromise the application in the same way an unsecured application can compromise the hosting infrastructure.

Additionally, our consultants will assess important security configuration parameters such as supported Transport Layer Security (TLS) protocols and ciphers, exposed database listeners and file extension handling and support.

7.1.3. Exploitation

The Exploitation phase will test a variety of common web application security flaws, and also determine where business logic issues may exist that don't directly affect the security of application, rather they affect the way that CloudMonitor operates.

A non-exhaustive list of tests that will be conducted includes the following:

- Authentication Testing
  - Brute-force testing
  - User enumeration
  - Authentication bypass
  - Password policy
  - Authentication scheme (Form based, Basic, Digest and Single Sign-On)
- Session Management
  - Cross-Site Request Forgery (CSRF)
  - Cookie management
  - Session timeout
  - Session fixation
- Information Disclosure
- Platform misconfigurations
- Authorisation Testing
  - Directory traversal
  - Privilege escalation
    - Horizontal – can a user access data of another user or assume their identity without authorisation?
    - Vertical – can a low-privileged user access functions limited to users with higher privileges?
    - Principle of least privilege – are users assigned the least amount of privileges possible such that they can still function as required?
- Input Validation
  - Cross-Site Scripting (XSS)
  - SQL Injection (SQLi)
  - Operating system command injection
  - Server-side injection
  - Deserialisation flaws
  - Template injection
  - File upload flaws
  - XPath injection

  - Server-Side Request Forgery
  - Cross-Site Request Forgery
  - CSV Injection
- Business Logic
  - Integrity checks
  - Workflow circumvention
  - Execution limits

7.1.4. Post-Exploitation

Post-Exploitation is where Aurian consultants will determine the value of the compromised asset(s), including any sensitive data stored within and the asset's usefulness in further compromising the network. The implication of the compromise will be demonstrated by identifying sensitive information such as credit card details, health data, personally identifiable information, confidential internal communications, and any other high-priority data as defined by CloudMonitor.

Where authorised and time permitting, Aurian will assess the possibility for an intruder to further penetrate the external or internal networks in which the application server resides.

7.1.5. Reporting and Documentation

Reporting is the final stage of the penetration test and is a culmination of all technical observations identified during the assessment. Aurian will create and deliver two formal test reports at the completion of testing – an executive report and technical findings report.

All Aurian reports go through a strict and rigorous quality assurance process which may involve follow up with CloudMonitor to confirm details as appropriate. Once this process is complete, Aurian will present CloudMonitor with the draft report materials and perform a walkthrough of the findings, address any questions and make any necessary changes. Following any updates, Aurian will issue the final documentation package and schedule any re-testing as desired.

8. Risk Assessment Framework

8.1. Risk Matrix

For the purpose of this report, Aurian defines each risk level as the following:

		Organisational Impact					
		Trivial (1)	**Low (2)**	**Medium (3)**	**High (4)**	**Severe (5)**	**Critical (6)**
Threat Likelihood	Almost Certain (5)	Low (5)	Moderate (10)	High (15)	Extreme (20)	Catastrophic (25)	Catastrophic (30)
	Likely (4)	Low (4)	Moderate (8)	Moderate (12)	High (16)	Extreme (20)	Extreme (24)
	Possible (3)	Informational (3)	Low (6)	Moderate (9)	Moderate (12)	High (15)	High (18)
	Improbable (2)	Informational (2)	Low (4)	Low (6)	Moderate (8)	Moderate (10)	Moderate (12)
	Remote (1)	Informational (1)	Informational (2)	Informational (3)	Low (4)	Low (5)	Low (6)

8.2. Risk Rating Scale

Designation	Risk Rating	Description
	**Informational** (1 – 3)	This finding has been raised to highlight the discovery to CloudMonitor. No immediate action is necessary; however, the finding should be monitored to ensure that the risk level does not increase.
	**Low** (4 – 7)	Where applicable, CloudMonitor should investigate the identified issue and plan for remediation within a reasonable timeframe.
	**Moderate** (8 – 14)	This finding has the potential to cause a limited adverse impact on business operations. CloudMonitor should investigate the effectiveness of current security controls and formulate a plan for mitigation of the issue.
	**High** (15 – 19)	This finding has the potential to seriously reduce the effectiveness of business operations and may result in damage to organisational assets. CloudMonitor must plan to mitigate the risk as soon as possible given other security priorities.
	**Extreme** (20 – 24)	This finding has the potential to cause significant damage to business information, finances, reputation, employees and customers. CloudMonitor must plan to mitigate the risk immediately.
	**Catastrophic** (25 – 30)	This finding has multiple **exceptional** consequences for CloudMonitor, including significant financial losses, notable reputational damage and considerable loss of data. Furthermore, the issue may have significant ramifications for other organisations in connection with CloudMonitor. Action **must** be taken **immediately** to adequately mitigate or eliminate the risk entirely.

Aurian provides these risk definitions as a guide to CloudMonitor to assist with the classification and prioritisation of identified issues. CloudMonitor should also consider its own internal risk management framework and determine an appropriate final risk score. Aurian recommends that mitigations to all identified issues are implemented in a reasonable timeframe, irrespective of the risk level, as a matter of security best practice.

Aurian

Security. Simplified.

ACN: 639 930 528

903/50 Clarence St,
Sydney NSW 2000

1300 748 788
sales@aurian.com.au
www.aurian.com.au