# ARINCO

# Azure Security Assessment

## REVIEW YOUR AZURE SECURITY POSTURE AND IDENTIFY ACTIONABLE RECOMMENDATIONS

Arinco's Azure Security Assessment is structured around the Microsoft Security Adoption Framework and CIS Critical controls.

The objective is to identify security configuration weaknesses and poor practices which exposure your organisation to cloud security threats.

Our report provides you with a structed, actionable set of recommendations organised into a roadmap of initiatives which priorise risk reduction.

We assess the use and configuration of the following Azure security controls:

- Entra ID PIM
- Entra ID Governance
- Log Analytics Workspace
- Azure Firewall
- Azure Key Vault
- Azure Policy
- Azure Secure Score

- Azure Backup
- Azure RBAC
- Azure DevOps
- Azure Private Link
- Network Security Groups
- Web App Firewall
- Defender for Cloud

## WHY CUSTOMERS USE THE AZURE SECURITY ASSESSMENT

**Concern** about misconfigurations and poor security practices

**Start the journey** to align with a control framework

**Validate** infrastructure and applications are secure

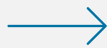**Quickly action** findings using prioritised, tangible recommendations

**Improve** Azure secure score

---

### DISCOVER

Environment discovery conducted via workshops and automated assessment tools
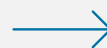
**Workshops**

### ASSESS

Analysis of your data and recommendations in order of priority

**Report**

### REPORT

Detailed findings and recommendations walk-through, including alignment on next steps

**Presentation**

---