

# Microsoft Managed Desktop Readiness 4-Week Assessment

4 week assessment to review the customers environment in line with the MMD Readiness Checker and provide a report outlining changes required to implement successfully



Not all organisations are in an MMD ready state. There are a number of prerequisites that are required before MMD can be successfully deployed. This assessment will give your organisation the confidence that all the required elements of the successful deployment are both understood and associated remediation activities to fill these gaps defined.

Traditional technology infrastructure is often loosely connected, relatively fragmented, and unnecessarily complex making them difficult, labour-intensive, and therefore costly to maintain and update.

These issues can be addressed by taking strategic control of your modernisation journey with end-to-end device management and security monitoring. It allows organisations to focus on digital transformation while keeping everyone productive, secure, and up-to-date.



We will complete a 4 week assessment of the customers environment that involves the execution of the MMD Readiness Checker and additional analysis of:

- Policy Scoping
- Conditional Access
- Store for Business
- Multi Factor Authentication
- Security Baselines
- Windows Hello for Business
- Enterprise State Roaming
- Device Compliance
- Intune Enrolment
- OneDrive for Business Sync Rules
- PowerShell Scripts
- Security Admin Roles
- Self Service Password Reset Scoping
- Windows Update Ring Exclusions for MMD
- Public key infrastructure (PKI)
- An assessment of you're the application portfolio



## Get in Touch

Phone

+61 (0)2 8966 1400

Email

[sales@quorumsystems.com.au](mailto:sales@quorumsystems.com.au)

Address

Level 6, 89 York Street Sydney, NSW, 2000

Member of  
**Microsoft Intelligent  
Security Association**



**SOC 2 – TYPE 1**  
VERIFIED BY ASSURANCELAB