Appendix D:
VAGO's maturity model for server security

Figure D1: VAGO's maturity model for server security

Maturity level	Operating system version	Industry-standard hardened images	Industry security baseline	Access control and patching	Backup and monitoring	Risk level
Level 1: initial (basic)	Unsupported operating system (e.g. 2008, 2012)	No	None	No patching or role-based access control	No automated backups or monitoring	High
Level 2: managed (basic compliance)	Extended supported operating system (e.g. 2016, 2019)	• Some images hardened • No automated configuration management	Minimal (only using default security policies)	• Manual patching • Minimal access control	Basic backups and logging	Moderate
Level 3: defined (standardised)	Mostly oldest supported operating system (e.g. 2022)	• All critical servers use hardened images • Automated configuration management implemented	Security baseline applied, such as: • Microsoft Security Baseline • Center for Internet Security technical implementation guide	• Regular patching • Role-based access control and least-privilege access	• Automated backups • Logging implemented	Moderate –low
Level 4: proactive (hardened)	Mostly latest supported operating system (e.g. 2025)	Most servers (more than 65%), including all critical servers, use hardened images, with automated configuration management	Customised security baseline based on industry standard	• Automated patching • Privileged access management solution	• Full backup/ restore • SIEM monitoring	Low
Level 5: optimised (highly secure)	Only latest supported operating system (e.g. 2025)	Hardened images across all, with automated configuration management	Continuous monitoring with customised baselines	• Continuous patching • Privileged access management • Privileged access workstations	• Full data protection • 24/7 security operations centre	Very low

Source: VAGO, based on the MCSB.