CYBERSECURITY

365 ARCHITECHS

Information Sheet

Cybersecurity Frameworks and Standards

Tags: Cybersecurity, Governance

Frameworks, standards, methodologies and other guidance is available for organisations seeking to align their cybersecurity activities to best practice. A variety of solutions are available, each with its own advantages and disadvantages. It is common for organisation to utilise the clauses in multiple documents, and also to choose individual clauses to adopt without complying with documents in their entirety.

This information sheet seeks to provide examples of some of the more common cybersecurity frameworks, standards and methodologies used by Australian organisations. Other guidance is available, and some choose to develop their own frameworks.

Compliance with all documents is generally voluntary, unless an obligation is imposed on an organisation such as through a contract.

Microsoft Secure Score

Microsoft provide a tool for assessing the maturity of an organisation's cyber defences, which is particularly useful for businesses that predominately use Microsoft Cloud technologies including Office 365, Dynamics 365 and Azure.

It provides a score which can be used to benchmark organisations against similar businesses, identify a target score and indicate progress in a simple numerical value.

NIST Cybersecurity Framework

The US National Institute of Standards and Technology (NIST) identify cybersecurity as an important component of any organisation's overall risk management activities.

The Framework identifies five core functions that should be considered:

Identity	Protect	Detect	Respond	Recover

ACSC Essential Eight

The Australian Cybersecurity Centre (ACSC) has developed a series of eight simple strategies to mitigate cybersecurity incidents, as follows:

<u>Mitigation strategies to prevent malware delivery and execution</u>

- Application whitelisting
- Configure Microsoft Office macro settings
- Patch applications
- User application hardening

<u>Mitigation strategies to limit the extent of cybersecurity incidents</u>

- Restrict administrative privileges
- Multi-factor authentication
- Patch operating systems

<u>Mitigation strategies to recover data and system availability</u>

- Daily backups

ISO27001

The international standard for information security management provides granular and detailed guidance on 114 controls in 14 clauses and 35 categories available for managing cyber risks.

About us

365 Architechs is a technology company based in Brisbane, Australia. We deliver solutions to support organisations on their digital transformation including cloud, modern applications, cybersecurity and artificial intelligence to drive profitability, growth and achievement of strategic objectives.

(07) 3393 1186 | www.365a.com.au | sales@365a.com.au

Disclaimer

These Information Sheets are designed to provide general information only. They should not be relied upon without consulting professional advice on your specific circumstances. 365 Architechs will not be held liable for any acts or reliance upon the information provided contained within.