Cyber Essentials mark: Cloud Security Companion Guide

Provider-specific implementation examples from Microsoft Singapore

Jointly developed with the
Cyber Security Agency of Singapore (CSA)

17 Oct 2023

Cyber Essentials mark: Cloud Security Companion Guide
Implementation examples from Microsoft Singapore

1 Background

The “Cyber Essentials mark: Cloud Security Companion Guide” is intended to serve as an implementation guide to accompany the Cyber Essentials mark certification document. The guide is targeted at end user organisations that are Software-as-a-Service (SaaS) users (see “3 Scope of this document” in “Cyber Essentials mark: Cloud Security Companion Guide” for further elaboration) and implementing or preparing to implement the security measures in the Cyber Essentials mark.

This document, outlining provider-specific implementation, is intended to be read alongside the “Cyber Essentials mark: Cloud Security Companion Guide”.

2 Provider-Specific Implementation

The cloud shared responsibility model is commonly used to describe the responsibilities of the cloud user or customer and the cloud provider in securing the cloud environment. This is a joint responsibility that is shared, and the amount of responsibility that each party bears depends on the cloud computing service model and how the cloud provider has implemented its offering.

Correspondingly, CSA has partnered with major cloud providers such as **Microsoft Singapore** to outline their respective provider-specific implementation based on the cloud-specific guidance in “Cyber Essentials mark: Cloud Security Companion Guide”.

Table 1 outlines the following provider-specific implementation examples:

- SaaS – Microsoft 365
- Cloud infrastructure – Microsoft Azure

3 Acknowledgements

CSA would like to acknowledge and thank **Microsoft Singapore** for its participation and contribution.

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) **E.g. Microsoft 365 customer**	**SaaS provider** **E,g. Microsoft 365**	**Cloud Infrastructure Provider** **E.g. Microsoft Azure**
A.1 Assets: People – Equip employees with know-how to be the first line of defence				
A.1.4 (a)	Requirement	Refer to CSA Cyber Essentials mark: Cloud Security Companion Guide	Cyber security awareness contents are publicly shared by Microsoft. Customers may leverage such contents within their organization freely, to raise cyber security awareness (link). For General Cyber Security Awareness: Learning pathway for beginners, business decision makers, students and administrators (link) Cyber Security 101 (link) For small businesses – 5 steps to protect against cybercrime (link)	Cyber security awareness contents are publicly shared by Microsoft. Customers may leverage such contents within their organization freely, to raise cyber security awareness (link). For General Cyber Security Awareness: Learning pathway for beginners, business decision makers, students and administrators (link) Cyber Security 101 (link) For small businesses - 5 steps to protect against cybercrime (link) Customers managing an Azure cloud infrastructure will benefit from having deeper technical knowledge in order to manage and secure systems hosted on Azure. Customers are strongly recommended to train technical staff on Security Engineer learning pathway (link)
A.1.4 (b)	Requirement		(link)	(link)
A.1.4 (c)	Recommendation			
A.1.4 (d)	Recommendation		Resources for various enterprise roles: For everyone (link) For small businesses (link)	Resources for various enterprise roles: For everyone (link) For small businesses (link)

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) **E.g. Microsoft 365 customer**	**SaaS provider** **E,g. Microsoft 365**	**Cloud Infrastructure Provider** **E.g. Microsoft Azure**
			For security professionals (link)	For security professionals (link)
A.1.4 (e)	Recommendation			
A.2 Assets: Hardware and software – Know what hardware and software the organisation has and protect them				
A.2.4 (a)	Requirement	Refer to CSA Cyber Essentials mark: Cloud Security Companion Guide	**SaaS Inventory Management** *M365 SaaS licenses & subscriptions* Customers can manage their M365 subscriptions via Admin Center: Admin Center → Billing → Your Products page, or via this link. *Software inventory* (link) *3rd-Party app subscriptions* Customers subscribing to 3rd-party SaaS applications or services may also be able to manage their subscription through M365 (link) **Hardware Inventory Management** Microsoft is responsible for the servers providing M365 services. Customers do not have administrative access to M365 servers. (link) *Client Compute devices - Hardware Inventory (Outside the SaaS environment)* Customers with access to endpoint manager service, can use M365 to manage their corporate hardware devices. This will allow them to manage and update devices plus deployed software. An	**Cloud Service Inventory Management** Azure customers can leverage Azure portal to list and review all services deployed on Azure. To view the inventory list of services owned by customer, login to Azure Portal: Home → All Resources. Results can also be exported into a CSV format for further processing if needed. Customers may refer to Cloud Adoption Framework - Azure Management Guide for Inventory and visibility as well (link). **Hardware Inventory Management** Customers using Azure services do not manage server hardware. Server hardware are managed by Microsoft. Customers focus on their hosted infrastructure instead. (link) More information on joint responsible model for cloud: (link)

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) **E.g. Microsoft 365 customer**	**SaaS provider** **E,g. Microsoft 365**	**Cloud Infrastructure Provider** **E.g. Microsoft Azure**
			inventory list of managed devices can be generated. Hardware inventory (link)	
A.2.4 (b)	Recommendation		M365 can be used to manage corporate and mobile devices (link) Customers can use M365 to manage compute devices within their organization. Devices that are managed can be reflected via the Device Inventory (link) Inventory can also be exported out in CSV format for further processing as required (link)	
A.2.4 (c)	Recommendation			
A.2.4 (d)	Requirement		See A.2.4(a)	See A.2.4(a)
A.2.4 (e)	Recommendation			
A.2.4 (f)	Recommendation			
A.2.4 (g)	Requirement		*M365 server-side service* M365 is provided as a SaaS. it consists of services such as SharePoint Online, OneDrive for Business, Exchange Online, Teams..etc. These SaaS services will be updated, upgraded and	Azure allows customers to deploy and host two types of cloud service models (PaaS & IaaS). More details on Shared Responsibility with regards to the service models: (link)

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) **E.g. Microsoft 365 customer**	**SaaS provider** **E,g. Microsoft 365**	**Cloud Infrastructure Provider** **E.g. Microsoft Azure**
			maintained by Microsoft. EOS will not apply as it is a service. *M365 applications* M365 subscriptions inclusive of M365 Apps, provides Office applications (installed on devices) via a subscription model. Customers on this will receive regular updates/upgrades to the applications. Customers on M365 may also choose to use Intune / Microsoft Endpoint Management to help them manage updates to their devices. More information on the inventory for M365 Apps Admin Center for managing the endpoints/devices: (link)	For PaaS services, Microsoft will manage underlying platforms and keep them updated, relevant and supported. Customers will be responsible for keeping their codes and data relevant and updated. For IaaS services, customers will manage and update their software, and as necessary and timely, update/replace/upgrade when EOS is reached. More information about updates for IaaS services on Azure: (link)
A.2.4 (h)	Requirement			
A.2.4 (i)	Requirement			
A.2.4 (j)	Requirement			
A.2.4 (k)	Requirement			
A.2.4 (l)	Requirement		*Data destruction* When customers delete data or leaves service, Microsoft follows strict standards for deleting data, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.	*Data destruction* When customers delete data or leaves service, Microsoft follows strict standards for deleting data, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination.

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) E.g. Microsoft 365 customer	**SaaS provider E,g. Microsoft 365**	**Cloud Infrastructure Provider E.g. Microsoft Azure**
			More information on data management at Microsoft: (link)	More information on data management at Microsoft (link)
A.2.4 (m)	Recommendation		Any data bearing devices, when decommissioned, are destroyed in compliance to NIST SP-800-88 purge guidelines (link)	Any data bearing devices, when decommissioned, are destroyed in compliance to NIST SP-800-88 purge guidelines (link)
A.3 Assets: Data – Know what data the organisation has, where they are and secure the data				
A.3.4 (a)	Requirement	Refer to CSA Cyber Essentials mark: Cloud Security Companion Guide		
A.3.4 (b)	Recommendation			
A.3.4 (c)	Requirement		Customers leveraging M365, Azure and D365, are invited to familiarize themselves with how Microsoft protects their data when using Microsoft's cloud services at Microsoft Trust Center: (link)	Customers leveraging M365, Azure and D365, are invited to familiarize themselves with how Microsoft protects their data when using Microsoft's cloud services at Microsoft Trust Center: (link)
A.3.4 (d)	Requirement		Customers may leverage the Intune service in M365 to restricted USB ports as necessary: (link) Customers may also explore the use of Information Protection as necessary: (link)	

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) **E.g. Microsoft 365 customer**	**SaaS provider** **E,g. Microsoft 365**	**Cloud Infrastructure Provider** **E.g. Microsoft Azure**
A.3.4 (e)	Requirement			
A.4 Secure/Protect: Virus and malware protection – Protect from malicious software like viruses and malware				
A.4.4 (a)	Requirement	Refer to CSA Cyber Essentials mark: Cloud Security Companion Guide	Microsoft is responsible for protecting the services hosted as part of the M365 services. This is documented and audited in SOC2: (link) Customers can use Defender for Endpoints as anti-malware solution on their endpoints. More information on deployment overview: (link)	Customers deployed IaaS assets on Azure can use Defender services. More information on various defender services and using them to protect your Azure resources at Defender for Cloud: (link) Customers may also be interested on the security recommendations for virtual machines in Azure: (link)
A.4.4 (b)	Requirement			
A.4.4 (c)	Requirement			
A.4.4 (d)	Requirement			
A.4.4 (e)	Recommendation			
A.4.4 (f)	Requirement		For M365, Microsoft is both the SaaS provider and the cloud infrastructure provider, and is responsible for securing the infrastructure that is providing the M365 services to customers. The SOC2 Type 2 report documents the use of firewall to protect M365's infrastructure: (link) Referencing shared responsibility model, customers are responsible for environments within their administrative control. For endpoints managed by M365, customers can consider to	Customers hosting server services on Azure, can leverage Azure Firewall to protect their hosted resources: (link) It is also important for customers to be aware, and regularly check on Azure Advisor's recommendation to secure services and infrastructure on Azure. More information at: (link)

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) E.g. Microsoft 365 customer	**SaaS provider E,g. Microsoft 365**	**Cloud Infrastructure Provider E.g. Microsoft Azure**
			enforce use of firewall on endpoints via a policy: (link)	
A.4.4 (g)	Recommendation			
A.4.4 (h)	Recommendation			
A.4.4 (i)	Recommendation			
A.4.4 (j)	Requirement			
A.4.4 (k)	Requirement			
A.4.4 (l)	Requirement			
A.5 Secure/Protect: Access control – Control access to the organisation's data and services				
A.5.4 (a)	Requirement	Refer to CSA Cyber Essentials mark: Cloud Security Companion Guide	M365 uses Azure Active Directory to manage user accounts. M365 customers can use M365 Admin Center, or Azure Active Directory to manage user accounts: (link) Customers may also leverage PowerShell script to list user accounts and export them into Excel: (link)	Azure customers uses Azure Active Directory as the identity management platform. To access a list of users in Azure portal: (link) Customers may also leverage PowerShell script to list user accounts and export them into Excel: (link)
A.5.4 (b)	Requirement			
A.5.4 (c)	Requirement			
A.5.4 (d)	Requirement			
A.5.4 (e)	Requirement			
A.5.4 (f)	Requirement			

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) E.g. Microsoft 365 customer	**SaaS provider E,g. Microsoft 365**	**Cloud Infrastructure Provider E.g. Microsoft Azure**
A.5.4 (g)	Requirement			
A.5.4 (h)	Requirement			
A.5.4 (i)	Requirement		See inputs on Microsoft Azure	Customers may learn about how Microsoft physically secure the data centers: (link)
A.5.4 (j)	Recommendation			
A.5.4 (k)	Recommendation		Customers are recommended to regularly check for and review inactive user accounts. More information on how to manage inactive user accounts: (link)	Customers are recommended to regularly check for and review inactive user accounts. More information on how to manage inactive user accounts: (link)
A.5.4 (l)	Requirement		Customers may refer to this article on the password policy recommendations for M365 passwords: (link) Microsoft recommends the use of Multi-Factor Authentication (MFA) for all users, and not rely on passwords for authentication purposes. More information on implementing multi-factor authentication for M365: (link) Customers may also want to consider passwordless MFA: (link)	Customers are recommended to review and practise Azure identity management best practises and access control: (link) Microsoft recommends the enforcement of MFA for Azure user accounts: (link).
A.5.4 (m)	Requirement		In place of disabling/locking accounts due to multiple password attempts (which can be inconvenient to users), Microsoft supports and recommends use of passwordless MFA, which	In place of disabling/locking accounts due to multiple password attempts (which can be inconvenient to users), Microsoft supports and recommends use of passwordless MFA, which

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) **E.g. Microsoft 365 customer**	**SaaS provider** **E,g. Microsoft 365**	**Cloud Infrastructure Provider** **E.g. Microsoft Azure**
			can also prove ownership of accounts, beyond that of passwords: (link).	can also prove ownership of accounts, beyond that of passwords: (link).
A.5.4 (n)	Requirement			
A.5.4 (o)	Recommendation		See A.5.4 (l)	See A.5.4 (l)
A.5.4 (p)	Recommendation			
A.6 Secure/Protect: Secure configuration – Use secure settings for the organisation's hardware and software				
A.6.4 (a)	Requirement	Refer to CSA Cyber Essentials mark: Cloud Security Companion Guide	The SaaS provider is responsible for the application-level configuration settings: (link)	The cloud infra provider is responsible for the configuration of the underlying cloud infrastructure: (link)
A.6.4 (b)	Requirement			
A.6.4 (c)	Requirement			
A.6.4 (d)	Requirement			
A.6.4 (e)	Requirement			
A.6.4 (f)	Recommendation		M365 customers may refer to this document for an overview: (link) More information • M365 Audit Log collection (link) • M365 Auditing and Reporting (link) • M365 Reporting features (link)	Azure Customers may refer to this document for an overview: (link) More information about Azure's managing and logging operations and reporting: (link)

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) **E.g. Microsoft 365 customer**	**SaaS provider** **E,g. Microsoft 365**	**Cloud Infrastructure Provider** **E.g. Microsoft Azure**
				In addition, Azure customers may deploy IaaS and PaaS assets differently, depending on the applications hosted. Under shared responsibility model, customers would also need to ensure security logging and monitoring is planned, logged and monitored. To help Azure customers with this planning, please refer to Azure's Cloud Adoption Framework on defining a security strategy: (link)
A.6.4 (g)	Recommendation			
A.6.4 (h)	Recommendation			
A.7 Update: Software updates – Update software on devices and systems				
A.7.4 (a)	Requirement	Refer to CSA Cyber Essentials mark: Cloud Security Companion Guide	As part of the shared responsibility model, Microsoft is responsible for ensuring that the infrastructure and systems are updated and secured. SOC2 certification of MS Cloud services indicates compliance with the requirements of the program, indicative of controls present to keep systems secured, and updated. The SOC2 report for Office 365 may be downloaded from: (link)	As part of the shared responsibility, Microsoft is responsible for the underlying infrastructure and services where customers do not have administrative access. Customers will continue to be responsible for IaaS services they deploy and ensuring software within IaaS are updated. SOC2 certification of Azure indicates compliance with the requirements of the program, indicative of controls present to keep systems secured, and updated. The SOC2 report for Azure may be downloaded from: (link)
A.7.4 (b)	Recommendation			
A.7.4 (c)	Recommendation			
A.7.4 (d)	Recommendation			

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) **E.g. Microsoft 365 customer**	**SaaS provider** **E,g. Microsoft 365**	**Cloud Infrastructure Provider** **E.g. Microsoft Azure**
A.8	**Backup: Back up essential data – Back up the organisation's essential data and store them offline**			
A.8.4 (a)	Requirement	Refer to CSA Cyber Essentials mark: Cloud Security Companion Guide	As part of shared responsibility model, Microsoft as the provider for M365 as a SaaS, is responsible for maintaining backups and perform recovery of SaaS infrastructure. SOC2 validates that M365 services complies and performs this responsibility. The SOC2 report for Office 365 may be downloaded from: (link) It is recommended that customers also be familiar with the resiliency and continuity overview for M365, and the various data resiliency approach for various M365 services available on the same site: (link) Customers may also consider backing their data beyond what is provided.	As part of shared responsibility model, Microsoft is responsible for backup and recovery of the Azure platform services. SOC2 validates that Azure services complies and performs this this responsibility. The SOC2 report for Azure may be downloaded from: (link) To learn about resiliency and continuity on Azure infrastructure, please refer to: (link) Also be familiarized with Azure infrastructure availability, Azure resiliency and data center network resiliency. As part of shared responsibility, customers deploying PaaS and IaaS services are responsible for ensuring that their data and applications are backed up.
A.8.4 (b)	Requirement			
A.8.4 (c)	Recommendation			
A.8.4 (d)	Recommendation			
A.8.4 (e)	Requirement			
A.8.4 (f)	Recommendation			
A.8.4 (g)	Requirement			

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) E.g. Microsoft 365 customer	**SaaS provider E,g. Microsoft 365**	**Cloud Infrastructure Provider E.g. Microsoft Azure**
A.8.4 (h)	Requirement			
A.8.4 (i)	Recommendation			
A.8.4 (j)	Requirement			
A.8.4 (k)	Recommendation			
A.9	**Respond: Incident response – Be ready to detect, respond to, and recover from cybersecurity incidents**			
A.9.4 (a)	Requirement	Refer to CSA Cyber Essentials mark: Cloud Security Companion Guide	Microsoft provides an overview of a security incident management: (link) When Microsoft becomes aware of a security incident, Microsoft will notify affected customers within 72 hours as outlined in the Data Protection Addendum (DPA): (link) Notifications include a description of the nature of the breach, approximate user impact, and mitigation steps (if applicable). If Microsoft's investigation isn't complete at the time of initial notification, the notification will also indicate next steps and timelines for subsequent communication. If a customer becomes aware of an incident that could have an impact on Microsoft, including but not limited to a data breach, the customer is responsible for promptly notifying Microsoft of the incident as defined in the DPA.	Microsoft provides an overview of a security incident management: (link) When Microsoft becomes aware of a security incident, Microsoft will notify affected customers within 72 hours as outlined in the Data Protection Addendum (DPA): (link) Notifications include a description of the nature of the breach, approximate user impact, and mitigation steps (if applicable). If Microsoft's investigation isn't complete at the time of initial notification, the notification will also indicate next steps and timelines for subsequent communication. If a customer becomes aware of an incident that could have an impact on Microsoft, including but not limited to a data breach, the customer is responsible for promptly notifying Microsoft of the incident as defined in the DPA.

Clause	Provisions in Cyber Essentials	Cloud responsibility		
		SaaS customer (End user) E.g. Microsoft 365 customer	SaaS provider E,g. Microsoft 365	Cloud Infrastructure Provider E.g. Microsoft Azure
			Affected customers may raise a support request to assist in investigations/retrieval of forensic information as permissible.	Affected customers may raise a support request to assist in investigations/retrieval of forensic information as permissible.
A.9.4 (b)	Requirement			
A.9.4 (c)	Recommendation			
A.9.4 (d)	Recommendation			