Cyber Essentials mark: Cloud Security Companion Guide

Date of Publication: 17-10-2023 (First edition)

A publication by

CSA SINGAPORE

SG CYBER SAFE | CYBER ESSENTIALS

CSA cloud security alliance®

About the Cyber Security Agency of Singapore (CSA)

Established in 2015, CSA seeks to keep Singapore's cyberspace safe and secure to underpin our National Security, power a Digital Economy and protect our Digital Way of Life. It maintains an oversight of national cybersecurity functions and works with sector leads to protect Singapore's Critical Information Infrastructure. CSA also engages with various stakeholders to heighten cybersecurity awareness, build a vibrant cybersecurity ecosystem supported by a robust workforce, pursue international partnerships and drive regional cybersecurity capacity building programmes.

For more news and information, please visit www.csa.gov.sg

© Cyber Security Agency of Singapore 2023

Contents

Page

1 Introduction 3
2 Intended audience 3
3 Scope of this document 3
4 Acknowledgements 3
5 Shared Responsibility Model (SRM) in the Cloud for Cyber Essentials 4
6 References 6

Tables

1 Shared Responsibility Model (SRM) in the Cloud for Cyber Essentials 5

Annexes

I Cloud-specific implementation guidance for Cyber Essentials 7

COPYRIGHT

1 Introduction

CSA Cyber Essentials mark and Cyber Trust mark are tiered cybersecurity standards that are designed to support the cybersecurity needs of a range of organisations.

The Cyber Essentials mark takes on a baseline control approach and is intended to protect organisations against common cyberattacks. The Cyber Trust mark takes on a risk-based approach and is intended to enable organisations to put in place the relevant cybersecurity preparedness measures that commensurate with their cybersecurity risk profile.

Together, the Cyber Essentials mark and Cyber Trust mark provide a cybersecurity risk management framework for organisations.

Globally, the industry has seen a rise in cloud adoption[1]. As organisations embrace cloud, adversaries are also evolving their Tactics, Techniques and Procedures (TTPs) to target organisations in the cloud. Cloud exploitation cases have grown, and the industry has seen an increase in cases involving adversaries targeting cloud environments.[2]

The “Cyber Essentials mark: Cloud Security Companion Guide” helps organisations in their defence against cloud-specific risks as cloud deployments rise and adversaries become more targeted.

2 Intended audience

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

3 Scope of this document

There are three (3) main types of cloud computing service models: (i) Software-as-a-Service (SaaS), (ii) Infrastructure-as-a-Service (IaaS) and (iii) Platform-as-a-Service (PaaS).

Cyber Essentials mark is targeted at smaller or less digitalised organisations that are starting out in their cybersecurity journey, such as Small and Medium Enterprises (SMEs). Correspondingly**,** this document is **scoped to target organisations that subscribe to the SaaS cloud computing model** as this model tends to be more suited for small organisations.

Organisations that subscribe to the IaaS or PaaS cloud computing model may refer to a similar companion guide for the Cyber Trust mark, “Cross-mapping between CSA Cyber Trust and Cloud Security Alliance Cloud Controls Matrix v4” instead.

4 Acknowledgements

This companion guide is jointly developed between CSA and Cloud Security Alliance.

[1] Cloud Security Alliance, 2022, *“Measuring Risk and Risk Governance”*
[2] CrowdStrike, 2023, *“2023 Cloud Risk Report”*

CSA has partnered with the following cloud services providers to further outline their respective cloud security best practices in alignment to the cloud security companion guides for Cyber Essentials and Cyber Trust:

- Amazon Web Services
- Microsoft Singapore
- Google Cloud

CSA has also sought inputs from the following cloud services providers:

- Huawei International Pte Ltd

CSA would like to acknowledge all industry partners for their support and contributions.

5 Shared Responsibility Model (SRM) in the Cloud for Cyber Essentials

The cloud SRM 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.

As the “Cyber Essentials mark: Cloud Security Companion Guide” is scoped to target organisations that subscribe to the SaaS cloud computing model, this Guide will address the following roles in the cloud value chain:

- Cloud customer subscribing to SaaS, or the end user organisation;
- SaaS provider; and
- Cloud infrastructure provider that the SaaS provider, in turn, subscribes to.

Collectively, the SaaS provider and cloud infrastructure provider are referred to as “cloud providers”.

The SRM is organised according to the security measures in the Cyber Essentials mark and the scope focuses on the **responsibilities of the end user organisation**, i.e. the SaaS customer, in the context of its SaaS subscription (see Table 1). Depending on the local setup and environment of the end user organisation, beyond what is outlined for its SaaS subscription in Table 1, the organisation is also responsible for the security its local environment, e.g. end point devices connecting to the SaaS subscription.

Whilst the SRM has not outlined the respective responsibilities of the cloud providers, they are expected to implement their respective cybersecurity measures to provide assurance of their own cybersecurity posture to their cloud customers. Major cloud providers also typically publish the cybersecurity best practices put in place for their respective offerings.

Table 1 – SRM in the Cloud for Cyber Essentials

(Scope focuses on responsibilities of SaaS users in the context of their SaaS subscriptions, i.e. these organisations continue to be responsible for the cybersecurity of their respective local environment)

● SaaS user responsibility
○ Cloud provider responsibility

		End user organisation (SaaS customer) responsibility	**Cloud provider responsibility**	
			SaaS provider	**Cloud infrastructure provider**
Category: Assets				
People	●			
Hardware and software	●	*SaaS as part of software inventory management*		
Data	◕	*Responsible for their own data within SaaS*	*Responsible for ensuring data in the cloud is online*	
Category: Secure/Protect				
Virus and malware protection	◔		*Protection of SaaS application(s)*	*Protection of host infrastructure*
Access control	●			
Secure configuration	◔	*User settings in SaaS and management of logging*	*Application-level configurations and ability to enable logging*	*Host infrastructure configuration*
Category: Update				
Software updates	○		*Update of SaaS application(s)*	*Update of host infrastructure*
Category: Backup				
Back up essential data	●	*Backup of data within SaaS*	*Backup of SaaS application(s)*	*Backup of host infrastructure*
Category: Respond				
Incident response	●			

The pie chart in Table 1 summarises the key areas that the end user organisation (or SaaS customer) and the cloud provider are responsible for respectively.

Annex 1 contains the cloud-specific implementation guidance that is relevant to the respective requirements and recommendations in Cyber Essentials mark.

6 References

In preparing this document, reference was made to the following publications:

1. CIS Controls Cloud Companion Guide v8 by Center for Internet Security (CIS)
2. ISO/IEC 27017- Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services by ITU-T
3. Top Threats to Cloud Computing by Cloud Security Alliance
4. SaaS Governance Best Practices for Cloud Customers by Cloud Security Alliance
5. Cloud Incident Response Framework – A Quick Guide by Cloud Security Alliance
6. 2022 SaaS Security Survey Report by Cloud Security Alliance and Adaptive Shield
7. Cloud Security Foundations, Frameworks and Beyond by SANS Institute
8. The State of SaaS Sprawl by Productiv Inc
9. 2023 State of SaaSOps by BetterCloud, Inc
10. Cloud and Threat Report: Global Cloud and Web Malware Trends by Netskope

Acknowledgement is made for the use of information from the above publications.

Annex I

Cloud-specific implementation guidance for Cyber Essentials

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
A.1	**Assets: People – Equip employees with know-how to be the first line of defence**			
A.1.4 (a)	Requirement	• The end user organisation (SaaS customer) is solely responsible[3] **Why is this important** • Increasingly, business users (as opposed to the IT division) are accessing and managing SaaS applications, and they may not be adequately equipped to manage the security of the SaaS[4] • Human error is commonly acknowledged as one of the leading drivers of cloud risk **What the organisation should do** • Beyond the inclusion of general cyber awareness training for employees, the organisation should also include topics for business users managing SaaS to understand why they play important roles in cloud security, and how they can operate securely in the cloud	• Major cloud providers may also publish best practices to provide better support to their cloud customers	
A.1.4 (b)	Requirement			
A.1.4 (c)	Recommendation	• This should include cloud-specific topics covering the key cloud risks and mitigation measures, such as: – Human error as one of the key drivers of cloud risk – Shared responsibility in the cloud – Risks arising from compromise of identity or user		

[3] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 14, Security Awareness and Skills Training
[4] Cloud Security Alliance and Adaptive Shield, 2022, *"2022 SaaS Security Survey Report"*

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		access accounts, and best practices to mitigate – Risks arising from misuse of accounts with elevated privileges, and best practices to mitigate – Risks arising from selection of weak configuration settings, and best practices to mitigate – Secure management of data in the cloud		
A.1.4 (d)	Recommendation			
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	• For hardware assets (in the cloud), this is not applicable to the end user organisation (SaaS customer) as SaaS is considered as software asset[5],[6] • For software assets, the end user organisation (SaaS customer) is responsible[7] **Why is this important** • The SaaS model has been growing in popularity – increasingly, organisations are managing a large number of SaaS subscriptions **What the organisation should do** • Implement a mechanism to track and monitor the inventory of its		For hardware assets, the cloud infrastructure provider is responsible

[5] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 1, Inventory and Control of Enterprise Assets

[6] The organisation is responsible for the hardware in its local environment.

[7] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 2, Inventory and Control of Software Assets

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		SaaS subscriptions across different business functions • This can be achieved through process or technology solutions, for example[8]: – Through procedural methods, in which all potential purchase and acquisition of SaaS is brought to IT and security prior to use – Through the analysis and evaluation of logs from firewalls, web gateways, and Cloud Access Service Brokers (CASBs) – Through the usage of a SaaS Security Posture Management (SSPM) solutions – Through the analysis of expense reports and financial records for line items relating to SaaS		
A.2.4 (b)	Recommendation			
A.2.4 (c)	Recommendation			
A.2.4 (d)	Requirement			
A.2.4 (e)	Recommendation			
A.2.4 (f)	Recommendation			
A.2.4 (g)	Requirement	• Verify the SaaS providers' obligations with respect to End of Support (EOS) assets as outlined in its service description and/or		

[8] Cloud Security Alliance, 2022, *“SaaS Governance Best Practices for Cloud Customers”*, 5.1: Responsibility for assets

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		terms of service, e.g. lead time to customers for migration or transition		
A.2.4 (h)	Requirement			
A.2.4 (i)	Requirement	**Why is this important** - Business users are increasingly accessing and managing SaaS applications, which may potentially be "unknown" to the IT division[9,10], i.e. shadow IT **What the organisation should do** - Implement a mechanism to track and monitor the inventory of its SaaS subscriptions across different business functions		
A.2.4 (j)	Requirement			
A.2.4 (k)	Requirement			
A.2.4 (l)	Requirement			- Major cloud infrastructure providers typically publish their practices in managing hardware disposal securely
A.2.4 (m)	Recommendation			
A.3	**Assets: Data – Know what data the organisation has, where they are and secure the data**			
A.3.4 (a)	Requirement	- The end user organisation (SaaS customer) is responsible for the inventory management of its data in the SaaS subscription[11]		

[9] Productiv, 2021, *"The State of SaaS Sprawl"*
[10] BetterCloud, 2023, *"2023 State of SaaSOps"*
[11] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 7.1: Security of data in SaaS environments

COPYRIGHT

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
A.3.4 (b)	Recommendation			
A.3.4 (c)	Requirement	• The end user organisation (SaaS customer) is responsible for the protection of its data in the SaaS subscription[12] **Why is this important** • Accidental cloud data disclosure and cloud storage data exfiltration are some of the top cloud security concerns[13] **What the organisation should do** • In transferring its data to the cloud, the organisation should consider[14]: – What data is transferred to the SaaS environment? – How will the data be transferred? – The data that the SaaS provider will have access to? – The company's reliance on the SaaS subscription for its data – Geolocation requirements for the data, such as to meet client service requirements – Any associated supervisory authorities and jurisdiction, where relevant, in relation to the geographical location	• The cloud provider is only responsible for making sure the data is online and that access is not granted outside of the application controlled by the cloud customer[17] • Major cloud providers typically publish their best practices in how they protect their customers' data	

[12] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 7.1: Security of data in SaaS environments
[13] Cloud Security Alliance, 2022, *"Top Threats to Cloud Computing"*
[14] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 5.1: Responsibility for assets
[17] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 3, Data Protection

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		where data is stored, processed or transmitted[15] • Verify the SaaS providers' approach[16] for the following: – Does the SaaS provider offer granular controls for sharing data (e.g. share only internally, share with select partners, share with everyone, etc) – Does the SaaS provider offer encryption of data in-transit and at rest? – Does the SaaS provider support end-to-end encryption? – What encryption algorithms and transport protocols does the SaaS provider support? – Does the SaaS provider have a capability to identify and/or mask sensitive data? – Does the SaaS provider provide a mechanism for users to tag sensitive data or fields?		
A.3.4 (d)	Requirement			
A.3.4 (e)	Requirement			
A.4 Secure/Protect: Virus and malware protection – Protect from malicious software like viruses and malware				

[15] ITU-T, 2015, *"ISO/IEC 27017- Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services",* 6 Organisation of information security

[16] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 7.1: Security of data in SaaS environments

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
A.4.4 (a)	Requirement	• The majority of the responsibility for malware protection (of the cloud) lies in the cloud provider[18] • However, some vectors for malware distribution still exist under the control of the SaaS user[19], e.g. customizable static-file hosting and attachments, which may be uploaded by other employees in the organisation, or by the general public if the SaaS application is providing a public-facing portal **Why is this important** • Cloud applications, particularly those that are popular with enterprises, are becoming an increasingly popular channel for malware delivery[20] **What should the organisation do** • Be familiar with any standardised malware and virus scanning capabilities built-in to the SaaS platform, and also verify their SaaS providers obligations on virus and malware protection as outlined in its service description and/or terms of service	• The majority of the responsibility for malware protection (of the cloud) lies in the cloud provider	
A.4.4 (b)	Requirement			
A.4.4 (c)	Requirement			

[18] The organisation is responsible for malware protection in its local environment
[19] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 8.2: Protection from malware
[20] Netskope, 2023, *"Cloud and Threat Report: Global Cloud and Web Malware Trends"*

COPYRIGHT

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
A.4.4 (d)	Requirement	- Accessing the cloud environment typically requires Internet web access, and many web-based applications are now operating in the cloud - The end user organisation (SaaS customer) is responsible for email and web browser security[21], where browsers are typically used to interact with the application - Web browsers should be up-to-date - Any third-party extensions should be updated and the highest possible security policies should be applied according to the organisation's requirements		
A.4.4 (e)	Recommendation			
A.4.4 (f)	Requirement	- The end user organisation (SaaS customer) is not responsible for physical and virtual network device configuration[22] - The organisation should verify their SaaS providers' obligations with respect to network security as outlined in its service description and/or terms of service		- The cloud infrastructure provider is responsible for physical and virtual network device configuration
A.4.4 (g)	Recommendation	- In the scenario where the organisation uses virtual firewalls, the configuration should deny by default[23]		

[21] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 9, Email and Web Browser Protection
[22] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 12, Network Infrastructure Management
[23] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 12, Network Infrastructure Management

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
A.4.4 (h)	Recommendation			
A.4.4 (i)	Recommendation			
A.4.4 (j)	Requirement			
A.4.4 (k)	Requirement	• In a SaaS deployment, the connection to the SaaS may traverse the public Internet • The organisation should protect sensitive data in transit, e.g. via encryption using Transport Layer Security (TLS) or Open Secure Shell (SSH)[24,25]		
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	• The end user organisation (SaaS customer) is responsible **Why is this important** • Insufficient identity, credentials, access management and privileged accounts are some of the top cloud security concerns[26] • Increasingly, organisations may see a growth in the number of SaaS subscriptions they manage • Business users from different business units may also be accessing and managing their respective SaaS applications • Each SaaS subscription may have its respective separate/distinctive identity		

[24] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 9.2: SaaS consumer network controls
[25] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 3, Data Protection
[26] Cloud Security Alliance, 2022, *"Top Threats to Cloud Computing"*

COPYRIGHT

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		• As a result, the organisation may have a large number of identities to manage • Each SaaS subscription may potentially have different ways to define, view and secure identities **What should the organisation do** • Implement a mechanism to track and monitor the inventory of its accounts to its SaaS subscriptions • For organisations with a large number of SaaS subscriptions and identities to manage, the organisation may scale identity management by leveraging identity providers to authenticate users through Single Sign On (SSO) solutions[27,28] as opposed to maintaining and managing separate passwords to individual SaaS subscriptions • Consider limiting user access to the SaaS subscription, e.g. allow user access only from approved devices that adhere to business security policies • If the organisation has a Bring Your Own Device (BYOD) practice, consider a risk-based approach, e.g. limit access to SaaS subscriptions from uncontrolled BYOD devices[29]		
A.5.4 (b)	Requirement			

[27] Cloud Security Alliance, 2022, *“SaaS Governance Best Practices for Cloud Customers”*, 6.3.2: Secure log-on procedures
[28] Cloud Security Alliance, 2022, *“SaaS Governance Best Practices for Cloud Customers”*, 6.3.3: Password management system
[29] SANS Institute, 2023, *“Cloud Security Foundations, Frameworks and Beyond”*, Foundation #2:Unified Endpoint Management (UEM)

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
A.5.4 (c)	Requirement			
A.5.4 (d)	Requirement	• Identify and set resource limits to the account(s) or service(s) If the features are supported by the SaaS provider [30]		
A.5.4 (e)	Requirement	• Halt the billing of the cloud resource(s) related to any removed account(s), where relevant		
A.5.4 (f)	Requirement	• For access control of accounts with administrative functions, use just-in-time access, elevating privileges only when required, and reverting back to non-privileged access, if the features are supported by the SaaS provider[31]		
A.5.4 (g)	Requirement	• The organisation's SaaS provider (and other 3rd party providers engaged by the organisation to manage its SaaS subscription) form part of the 3rd parties or contractors in its value chain • The organisation should consider and evaluate the cybersecurity posture of its 3rd party providers, e.g. – Providers, including those appointed to manage its SaaS subscription: Consider if the providers are cybersecurity		
A.5.4 (h)	Requirement			

[30] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 6.2.1 User registration and deregistration, 6.2.5 Removal or adjustment of access rights

[31] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 6.2.2: Management of privileged access rights

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		certified, e.g. have attained CSA Cyber Essentials or Cyber Trust mark – Cloud providers: Consider if these providers adhere to the Multi-Tier Cloud Security Standard (MTCS) • The organisation is responsible for verifying if its SaaS providers align to these best practices: – Articulate roles and responsibilities between the end user organisation (i.e. SaaS customer) and SaaS provider[32] – Support Service level agreements (SLA) for not only the SaaS product's availability but also the confidentiality and integrity of the underlying data[33] – Undergo external verification processes of the SaaS provider or product[34], e.g. cybersecurity certification, audits, penetration tests		
A.5.4 (i)	Requirement	• The end user organisation (SaaS customer) is not responsible for physical access control		• The cloud infrastructure provider is responsible for the physical security of the underlying cloud infrastructure • Major cloud infrastructure providers typically publish their

[32] ITU-T, 2015, *"ISO/IEC 27017- Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services"*, 6 Organisation of information security

[33] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 10.1.2 Addressing security within suppler agreements

[34] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 10.1.2 Addressing security within suppler agreements

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
				best practices on their physical security measures
A.5.4 (j)	Recommendation			
A.5.4 (k)	Recommendation			
A.5.4 (l)	Requirement	• See guidance in A.5.4(a) on the use of identity providers and SSO, as opposed to maintaining and managing separate passwords for each SaaS subscription • If separate passwords need to be maintained and managed: – Implement the use of secure passphrases – Ensure passphrases are not re-used across multiple SaaS subscriptions – Ensure passphrases are not shared across accounts		
A.5.4 (m)	Requirement			
A.5.4 (n)	Requirement			
A.5.4 (o)	Recommendation	• As the SaaS subscription may be accessed over the public internet, deploy two-factor authentication (2FA) to ensure the users accessing the SaaS subscription are who they claim to be[35]		
A.5.4 (p)	Recommendation	• See guidance in A.5.4(a) on the use of identity providers and SSO, as opposed to maintaining and		

[35] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 6.3.2 Secure log-on procedures

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		managing separate passwords for each SaaS subscription • If separate passphrases need to be maintained and managed, store passphrases in a key vault or similar security device to protect confidentiality, integrity and availability[36]		
A.6	**Secure/Protect: Secure configuration – Use secure settings for the organisation's hardware and software**			
A.6.4 (a)	Requirement	• The end user organisation (SaaS customer) is responsible for user-level configuration settings in the SaaS subscription **Why is this important** • With the rise in popularity of the SaaS model, and the trend towards business-led SaaS where business users are increasingly accessing and managing SaaS applications, organisations may have a large number of SaaS subscriptions potentially managed by different business functions • Such organisations run the risk[37] of: – Too many departments having access to SaaS security settings – Lack of visibility into changes in SaaS security settings **What the organisation should do**	• The SaaS provider is responsible for application-level settings	• The cloud infrastructure provider is responsible for the configuration of the underlying cloud infrastructure

[36] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 6.3.3 Password management system
[37] Cloud Security Alliance & Adaptive Shield, 2022, *"2022 SaaS Security Survey Report"*

COPYRIGHT

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		• If the organisation has a large number of SaaS subscriptions, scale the SaaS management efforts through automation of its monitoring with SSPM tools[38] • Also consider the use of CASBs that can provide granular controls for monitoring user's application sessions and blocking actions[39]		
A.6.4 (b)	Requirement	• Review and update, where relevant, the default configuration in the SaaS subscriptions as these settings may be configured for usability or convenience rather than for security • Where available, also implement the secure configuration best practices published by its SaaS provider(s)		
A.6.4 (c)	Requirement			
A.6.4 (d)	Requirement			
A.6.4 (e)	Requirement			
A.6.4 (f)	Recommendation	• The end user organisation (SaaS customer) is responsible for the setup, maintenance, monitoring, and process analysis of the audit logs once they are made available by the SaaS provider[40]	• The SaaS provider is responsible for providing the features for their customers to enable logging and the time sources of the logs[42]	

[38] Cloud Security Alliance & Adaptive Shield, 2022, *"2022 SaaS Security Survey Report"*
[39] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 4, Secure Configuration of Enterprise Assets and Software
[40] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 8, Audit Log Management
[42] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 8, Audit Log Management

COPYRIGHT

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		• There is no industry standard accepted format for SaaS application log output • The timeliness of log delivery from the SaaS provider may also vary • If the organisation has a large number of SaaS subscriptions to manage, consider the folllowing[41]: – Automate the retrieval of logs from the SaaS provider – Normalise the SaaS logs to a common format across SaaS applications before being delivered to log analysis and/or storage solution for effective monitoring across SaaS applications – Normalise event, audit, activity, and other log entries that include user information such as usernames to a corporate identity such that events that refer to the same person in different usernames/user accounts in different SaaS applications can be correlated – Document and understand the expected, average, and maximum delay between action and log entry availability for each SaaS subscription		
A.6.4 (g)	Recommendation			

[41] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 8.4 Logging and monitoring

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
A.6.4 (h)	Recommendation			
A.7 Update: Software updates – Update software on devices and systems				
A.7.4 (a)	Requirement	• The end user organisation (SaaS customer) typically relies on its cloud providers to update their respective software. **Why is this important** • Software updates provide new features and address newly discovered security vulnerabilities **What the organisation should do** • The end user organisation (SaaS customer) is responsible for verifying their SaaS providers' obligations with respect to software updates and vulnerability management as outlined in its service description and/or terms of service, including[43]: – Notification to the organisation within a specific time period if the provider identifies a vulnerability for which the organization can apply compensating controls to reduce its severity or likelihood of exploitation – Support from the provider for resolving or mitigating vulnerabilities in the provider's products, based on the organisation's requirements	• The SaaS provider is responsible for the updates to the software used for its SaaS	• The cloud infrastructure provider is responsible for the updates to the underlying cloud infrastructure

[43] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 10.1.2 Addressing security within supplier agreements

COPYRIGHT

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
A.7.4 (b)	Recommendation			
A.7.4 (c)	Recommendation			
A.7.4 (d)	Recommendation			
A.8	**Backup: Back up essential data – Back up the organisation's essential data and store them offline**			
A.8.4 (a)	Requirement	• The end user organisation (SaaS customer) is responsible for the backup and recovery of its data in the SaaS subscription **Why is this important** • Having offline data backups are critical in enabling quick recovery from cybersecurity incidents **What should the organisation do** • Verify the SaaS providers' obligations with respect to high availability and redundancy as outlined in its service description and/or terms of service[44]		
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			
A.8.4 (h)	Requirement	• Establish and maintain an isolated instance of recovery data, e.g. version controlling backup destinations through offline, cloud		

[44] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 8.3 Backup and high availability

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		(including alternative cloud providers), or off-site systems or services[45]		
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	• The end user organisation (SaaS customer) is responsible for its incident response **Why is this important** • Cloud incident response typically differs from "traditional" incident response from these perspectives[46]: – Governance – Shared responsibility – Visibility **What the organisation should do** • Maintain a register of critical cloud services providers' contact points • Service Level Agreements (SLAs) for security and non-security incidents should be agreed with via contractual agreements[47] • Verify the SaaS providers' obligations on cooperating with the organisation in investigating and remediating incidents that have impacted or might impact the		

[45] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 11.4 Data recovery
[46] Cloud Security Alliance, 2021, *"Cloud Incident Response Framework – A Quick Guide"*
[47] Cloud Security Alliance, 2022, *"SaaS Governance Best Practices for Cloud Customers"*, 11 Incident management

Clause	Provisions in Cyber Essentials	End user organisation (SaaS customer) responsibility	Cloud provider responsibility	
			SaaS provider	Cloud infrastructure provider
		confidentiality, integrity, or availability of the organisation's data[48] • Include scenarios related to cybersecurity incidents in the cloud environment in the incident response plan • Examples of the key cloud risk or security scenarios[49] include: – Accidental cloud disclosure – Cloud storage data exfiltration – Breach arising from insufficient identity, credential, access, or privilege account management – Breach arising from use of weak configuration settings and inadequate change control – Breach arising from insecure 3rd party supply chain partners, including suppliers and vendors		
A.9.4 (b)	Requirement			
A.9.4 (c)	Recommendation			
A.9.4 (d)	Recommendation			

[48] Center for Internet Security (CIS), 2022, *"CIS Controls Cloud Companion Guide v8"*, CIS Control 17, Incident Response Management

[49] Scenarios suggested take reference from Cloud Security Alliance, 2022, *"Top Threats to Cloud Computing"* publication and industry inputs

COPYRIGHT