CYBER ESSENTIALS | CYBER TRUST

CLOUD SECURITY COMPANION GUIDE

About the Cloud Security Companion Guides

- For organisations to implement cloud security as enterprise cloud adoption rises

- Aligned to Cyber Essentials and Cyber Trust – national cybersecurity standards for organisations in Singapore

Acknowledgments

Cloud Security Companion Guides for Cyber Essentials and Cyber Trust are developed in partnership with:

CSA cloud security alliance®

aws

Microsoft

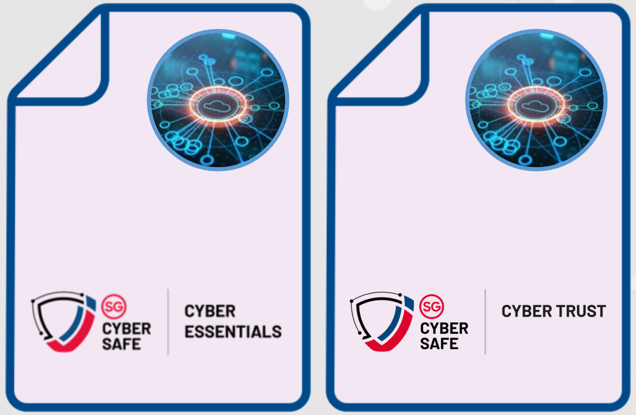
Google Cloud

How to use the Cloud Security Companion Guides

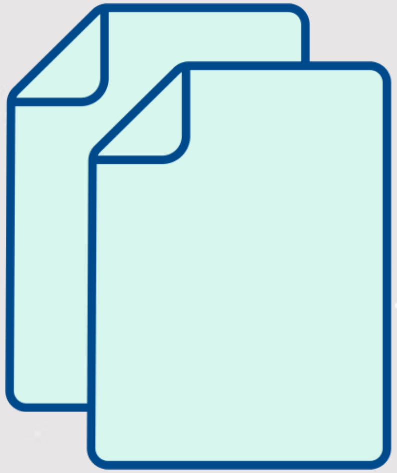
Cyber Essentials | Cyber Trust

National standards for cybersecurity certification of organisations

Cloud Security Companion Guides



Cloud-specific guidance for organisations – Aligned to Cyber Essentials and Cyber Trust



Provider-specific guidance – Outlines provider’s cloud security best practices

Content

01

Key shifts and cybersecurity implications with cloud

02

Cyber Essentials: Cloud Security Companion Guide

03

Cyber Trust: Cloud Security Companion Guide

04

Resources

Key shifts and cybersecurity implications with cloud

- Enterprise cloud adoption has been on the rise
- With cloud adoption, there is a shift in the responsibility of the organisation (cloud user) and its cloud provider(s)
- This has corresponding cybersecurity implications on organisations

	Shared Responsibility Model	**Large no. of SaaS subscriptions** (“SaaS sprawl”)	**Business-led SaaS** (Potential “shadow IT”)
Changes	• Cloud users and providers now take on joint responsibility	• Many standalone, potentially silo-ed subscriptions to manage	• Different business units directly manage their own SaaS
Implications on cybersecurity	• Cloud users misunderstand that cloud provider takes care of everything	• Difficult to scale the management of large number of SaaS subscriptions	• Subscriptions may not comply with organisation’s cybersecurity processes • Business users unaware of cloud security best practices

SaaS - Software-as-a-service

Shift 1

Shared Responsibility Model

> **“ …customers often assume the cloud service provider does more than it really does…**
>
> *SANS, 2023, “Cloud Security Foundations, Frameworks and Beyond”*

Shift 2

Large number of SaaS subscriptions

("SaaS sprawl")

- Organisations are using more SaaS – expansion of attack surface
- In some organisations, business units independently acquire SaaS (outside of their IT teams)
- Whilst this empowers employee productivity, the lack of centralised oversight could also result in blind spots in SaaS portfolio management

364 **Average number of SaaS tools in large enterprises**

242 **Average number of SaaS tools in small enterprises**

Source: Productiv, 2021, *"The State of SaaS Sprawl"*

Shift 3

Business-led SaaS

(Potential “shadow IT”)

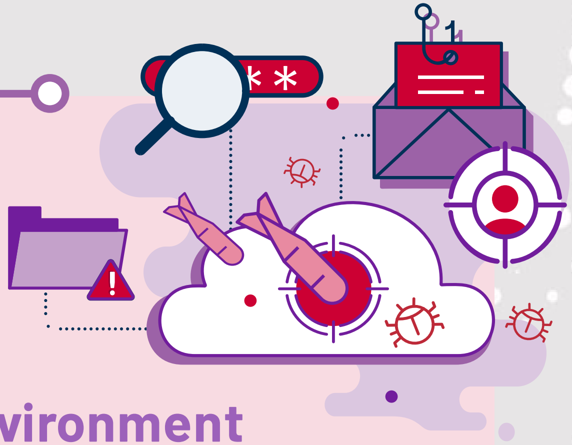
- One of the concerns around SaaS management is the rising trend of shadow IT
- This can lead to lack of visibility over the organisation’s software stack

Source: DarkReading, *“Shadow IT, SaaS pose security liability for enterprises”*, 2023

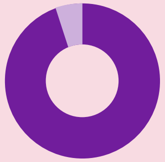
Attackers are evolving their tactics to target cloud environment

- 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

Evolving tactics of attackers



to target cloud environment



95% increase in cloud exploitation

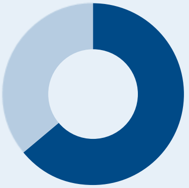
3x increase in attacks targeting cloud environment

Source: CrowdStrike report

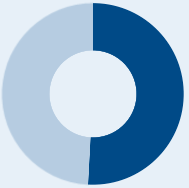
Key attack vectors

- Cloud **credentials** and **identities** targeted
- **Lateral movement** across cloud environment
- Cloud **misconfiguration abuse**

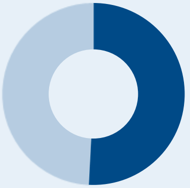
Key security concerns of cloud users



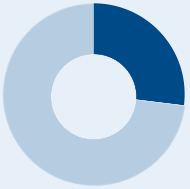
64%
Loss of sensitive data



51%
Unauthorised access



51%
Improper configuration and security settings



26%
Lack of visibility into cloud services

Source: Cloud Security Alliance report

Key security concerns of cloud users

As the cloud threat landscape evolves, organisations need to keep pace with these developments

Content

01

Key shifts and cybersecurity implications with cloud

02

Cyber Essentials: Cloud Security Companion Guide

03

Cyber Trust: Cloud Security Companion Guide

04

Resources

Cyber Essentials:
Cloud Security Companion Guide

For organisations that subscribe to SaaS

WHO is this for?

Shared Responsibility Model – SaaS users' responsibilities and that of their cloud provider(s)

WHAT does it focus on?

Cloud users often confused over shared responsibility model – The model for SaaS is potentially the most confusing[1, 2]

WHY does this matter?

[1] Oracle and KPMG, 2020, *"Demystifying the Cloud Shared Responsibility Security Model"*

[2] ISACA, 2022, *"SaaS Security Risk and Challenges"*

Shared responsibility model in the cloud for Cyber Essentials

- Outlines the areas of responsibilities between SaaS users and their cloud provider(s)
- Aligned to CSA Cyber Essentials mark
- Beyond managing the SaaS, organisations remain responsible for their respective local environment, e.g. end-point devices connected to SaaS

● SaaS user responsibility
○ Cloud provider responsibility

			Responsibility of SaaS user	Responsibility of cloud provider	
				SaaS provider	Cloud infrastructure provider
Assets	People	●			
	Hardware and software	●			
	Data	◕	• Data within SaaS	• Ensure data in the cloud is online	
Secure/Protect	Virus/malware protection	◔		• Protection of SaaS application(s)	• Protection of host infrastructure
	Access control	●			
	Secure configuration	◔	• User settings in SaaS • Management of logging	• Application-level configuration • Ability to enable logging	• Host infrastructure configuration
Update	Software updates	○		• Update of SaaS application(s)	• Update of host infrastructure
Backup	Back up essential data	●	• Backup of organisation's essential data within SaaS	• Backup of SaaS application(s)	• Backup of host infrastructure
Respond	Incident response	●			

SG CYBER SAFE

CYBER ESSENTIALS

Key cloud security concerns for SaaS users

Be aware of the differences in responsibility between you and your cloud provider(s)

Manage cloud credentials and identities securely

Mitigate against cloud misconfiguration

Equip business users with cloud security know-how

Shared responsibility model in the cloud for Cyber Essentials

	ASSET
PEOPLE	Equip business users with cloud security know-how
HARDWARE AND SOFTARE	Include SaaS and other cloud services in the organization's software inventory
DATA	Evaluate the type of data stored in the SaaS and potential external data access

Why is this important?
Human error drives cloud risk[1]

Why is this important?
Accidental cloud data disclosure and cloud storage data exfiltration are some of the top cloud security concerns[2]

1: CrowdStrike, 2023, *"2023 Cloud Risk Report"*
2: Cloud Security Alliance, 2022, *"Top Threats to Cloud Computing"*

Shared responsibility model in the cloud for Cyber Essentials

SG CYBER SAFE

CYBER ESSENTIALS

Why is this important?
Insufficient identity, credentials, access management and privileged accounts are some of the top cloud security concerns[1]

Why is this important?
Cloud misconfigurations become open doors to adversaries[2]

	SECURE/PROTECT
VIRUS/MALWARE PROTECTION	Be familiar with any standard malware and virus scanning capabilities in your SaaS service
ACCESS CONTROL	Manage cloud credentials and identities securely
SECURE CONFIGURATION	Mitigate against cloud misconfiguration

[1] Cloud Security Alliance, 2022, *"Top Threats to Cloud Computing"*

[2] CrowdStrike, 2023, *"2023 Cloud Risk Report"*

Shared responsibility model in the cloud for Cyber Essentials

UPDATE

Verify SaaS providers' obligations with respect to software updates and vulnerability management

BACKUP

Establish and maintain offline data backups

RESPOND

Maintain a register of critical cloud providers' contact points

Include scenarios related to cloud security in your incident response plan

Addressing the key cloud concerns and risks with shared responsibility model for Cyber Essentials

1

Observations on trends towards business-led SaaS
Guidance for business users to understand their role in cloud security and secure cloud practices

2

Concerns on loss of sensitive data
Guidance for cloud users to understand key considerations when transferring data to cloud

3

Findings on weak identity and entitlement practices
Guidance for cloud users on ways to scale the management of cloud subscriptions/identities

● SaaS user responsibility
○ Cloud provider responsibility

			Responsibility of SaaS user	Responsibility of cloud provider	
				SaaS provider	Cloud infrastructure provider
Assets	People 1	●			
	Hardware and software	●			
	Data 2	◕	• Data within SaaS	• Ensure data in the cloud is online	
Secure/Protect	Virus/malware protection	◔		• Protection of SaaS application(s)	• Protection of host infrastructure
	Access control 3	●			
	Secure configuration	◔	• User settings in SaaS • Management of logging	• Application-level configuration • Ability to enable logging	• Host infrastructure configuration
Update	Software updates	○		• Update of SaaS application(s)	• Update of host infrastructure
Backup	Back up essential data	●	• Backup of organisation's essential data within SaaS	• Backup of SaaS application(s)	• Backup of host infrastructure
Respond	Incident response	●			

Content

01

Key shifts and cybersecurity implications with cloud

02

Cyber Essentials: Cloud Security Companion Guide

03

Cyber Trust: Cloud Security Companion Guide

04

Resources

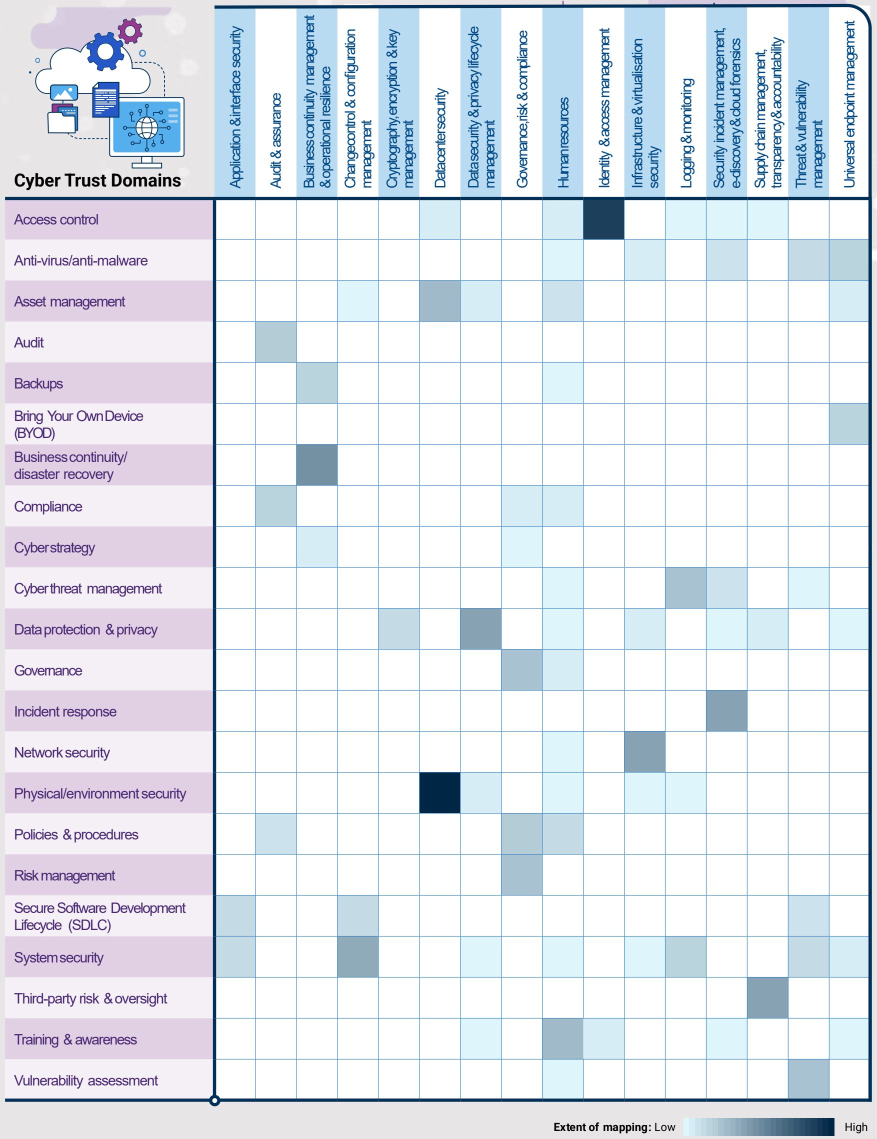
Cyber Trust: Cloud Security Companion Guide

Target audience

- For organisations that subscribe to Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS) cloud computing model

Key areas of focus

- Mapping between CSA Cyber Trust mark and Cloud Security Alliance Cloud Controls Matrix



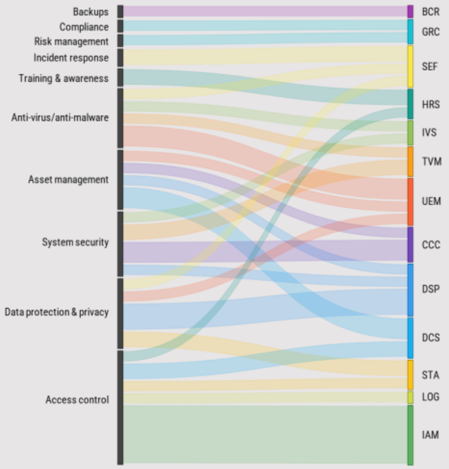
CYBER TRUST

Mapping of Cyber Trust to Cloud Security Alliance Cloud Controls Matrix

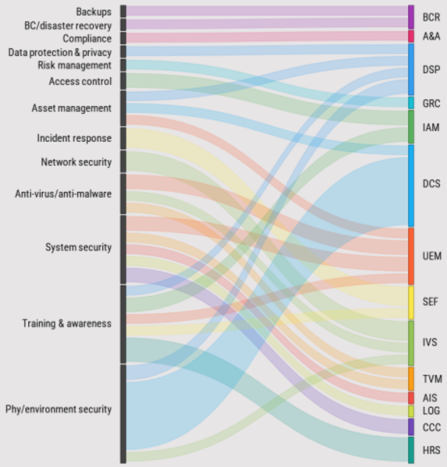
SG CYBER SAFE

CYBER TRUST

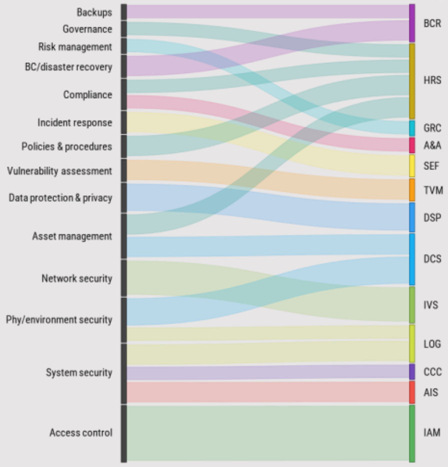
Cyber Trust “**Supporter**” tier mapped to Cloud Controls Matrix



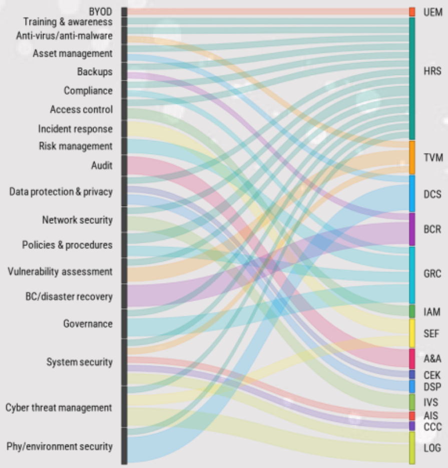
Cyber Trust “**Practitioner**” tier mapped to Cloud Controls Matrix



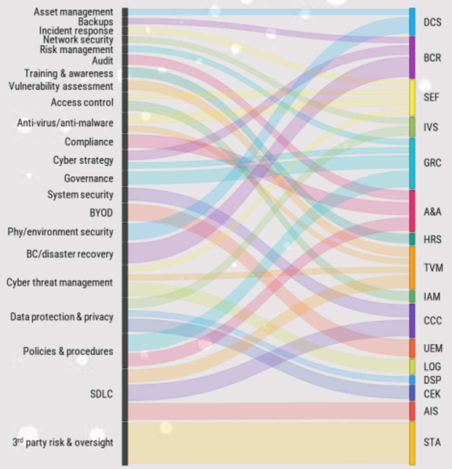
Cyber Trust “**Promoter**” tier mapped to Cloud Controls Matrix

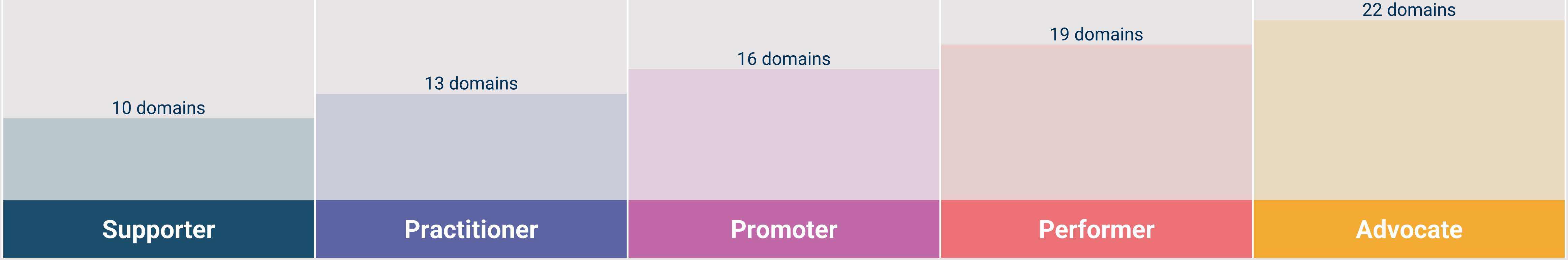


Cyber Trust “**Performer**” tier mapped to Cloud Controls Matrix



Cyber Trust “**Advocate**” tier mapped to Cloud Controls Matrix





Content

01

Key shifts and cybersecurity implications with cloud

02

Cyber Essentials: Cloud Security Companion Guide

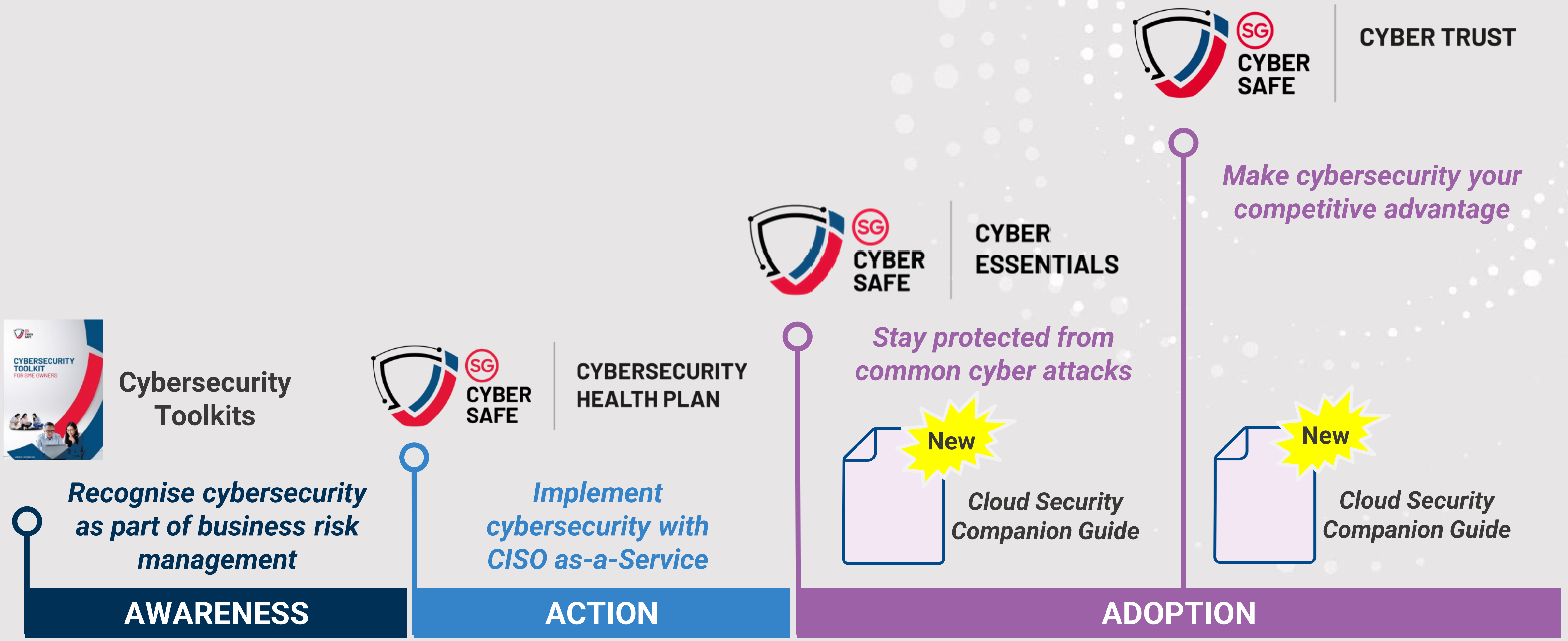
03

Cyber Trust: Cloud Security Companion Guide

04

Resources

Resources for staying SG CYBER SAFE together



AWARENESS

Cybersecurity Toolkits

Recognise cybersecurity as part of business risk management

ACTION

SG CYBER SAFE | CYBERSECURITY HEALTH PLAN

Implement cybersecurity with CISO as-a-Service

ADOPTION

SG CYBER SAFE | CYBER ESSENTIALS

Stay protected from common cyber attacks

New

Cloud Security Companion Guide

SG CYBER SAFE | CYBER TRUST

Make cybersecurity your competitive advantage

New

Cloud Security Companion Guide

Thank You

@csasingapore | www.csa.gov.sg