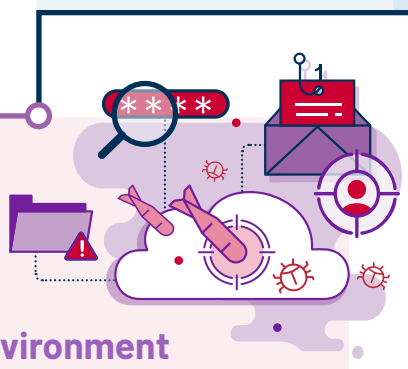
CYBER TRUST

Cloud Security Companion Guide
For Cyber Trust

Key shifts and cybersecurity challenges
when organisations move to the cloud

	Shared Responsibility Model (SRM)	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
Cybersecurity challenges	• Cloud users misunderstand that cloud providers take 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



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

Cyber Trust mapping to Cloud Security Alliance Cloud Controls Matrix

This visualisation depicts the mapping of each of the cybersecurity preparedness domains in the Cyber Trust mark to the control specifications in CCMv4.

Cyber Trust Domains	Application & interface security	Audit & assurance	Business continuity management & operational resilience	Change control & configuration management	Cryptography, encryption & key management	Datacenter security	Data security & privacy lifecycle management	Governance, risk & compliance	Human resources	Identity & access management	Infrastructure & virtualisation security	Logging & monitoring	Security incident management, e-discovery & cloud forensics	Supply chain management, transparency & accountability	Threat & vulnerability management	Universal endpoint management
Access control																
Anti-virus/anti-malware																
Asset management																
Audit																
Backups																
Bring Your Own Device (BYOD)																
Business continuity/ disaster recovery																
Compliance																
Cyber strategy																
Cyber threat management																
Data protection & privacy																
Governance																
Incident response																
Network security																
Physical/environment security																
Policies & procedures																
Risk management																
Secure Software Development Lifecycle (SDLC)																
System security																
Third-party risk & oversight																
Training & awareness																
Vulnerability assessment																

Extent of mapping: Low — High

Get started with implementing cloud security

- **Cyber Trust**
- **Cloud Security Companion Guide for Cyber Trust** — Mapping to Cloud Security Alliance CCM
- **Cloud provider-specific practices**

Find out more
www.csa.gov.sg/cloudsecurity

@csasingapore