SIMPLE STEPS TO PROTECT YOUR WORKLOAD IN CLOUD

Harry Pun

Deputy Chairman (Hong Kong)
Cloud Security Alliance
Hong Kong & Macau Chapter

cloud security alliance®

ABOUT THE CLOUD SECURITY ALLIANCE

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

BUILDING SECURITY BEST PRACTICES FOR NEXT GENERATION IT

GLOBAL, NOT-FOR-PROFIT ORGANIZATION

RESEARCH AND EDUCATIONAL PROGRAMS

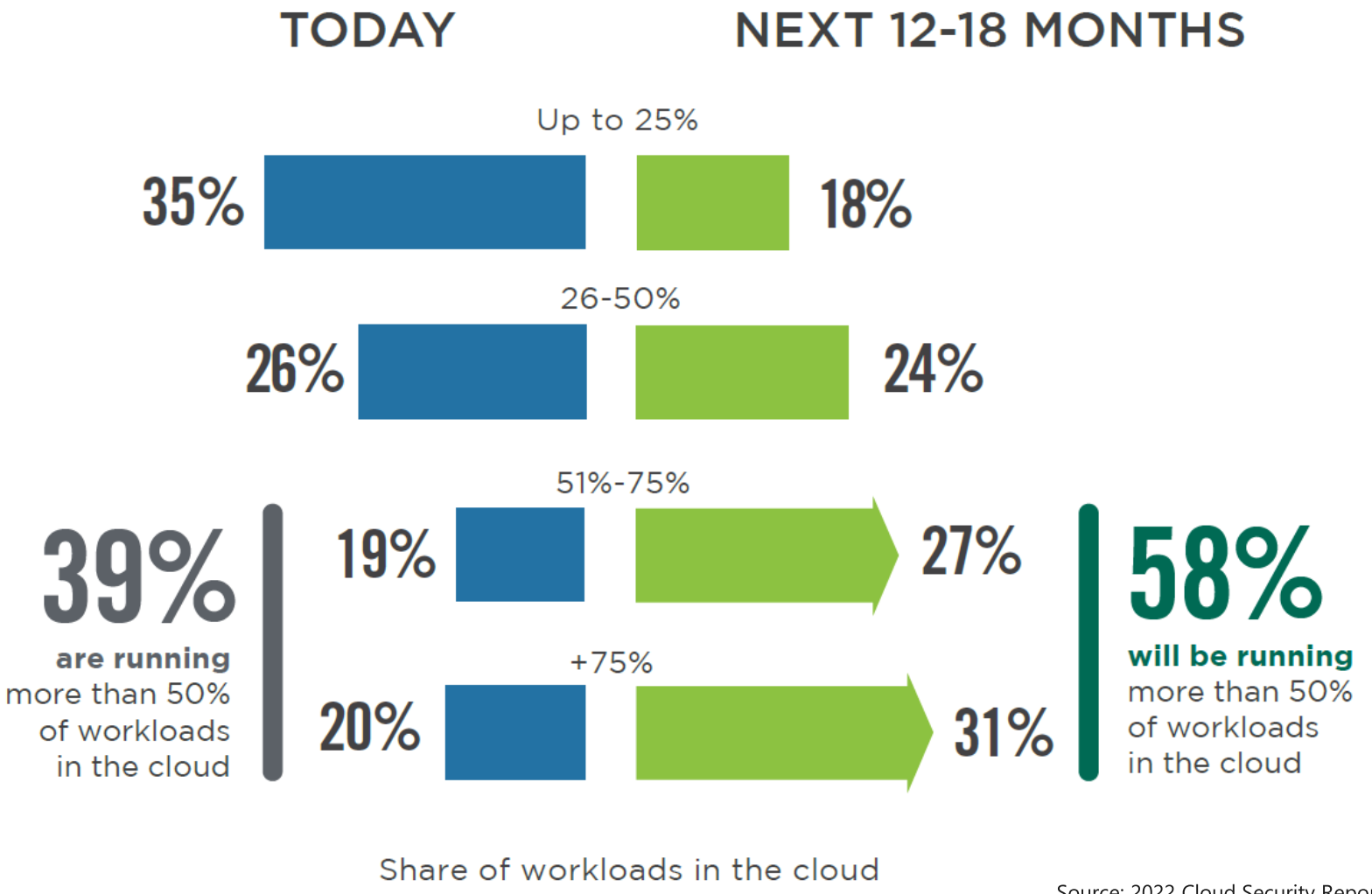
CLOUD PROVIDER CERTIFICATION – CSA STAR

USER CERTIFICATION – CCSK

THE GLOBALLY AUTHORITATIVE SOURCE FOR TRUST IN THE CLOUD

What percentage of your workloads are in the cloud today?

What percentage of your workloads will be in the cloud in the next 12-18 months?



Source: 2022 Cloud Security Report – (ISC)[2] and Cybersecurity Insiders

CSA APAC cloud security ASIA PACIFIC REGION alliance

What do you see as the biggest security threats in public clouds?

62%

Misconfiguration of the cloud platform/wrong setup

54%

Insecure interfaces/APIs

51%

Exfiltration of sensitive data

Source: 2022 Cloud Security Report – (ISC)[2] and Cybersecurity Insiders

Which part of the cloud compliance process is the most challenging?

57%

Lack of staff expertise/ knowledge

44%

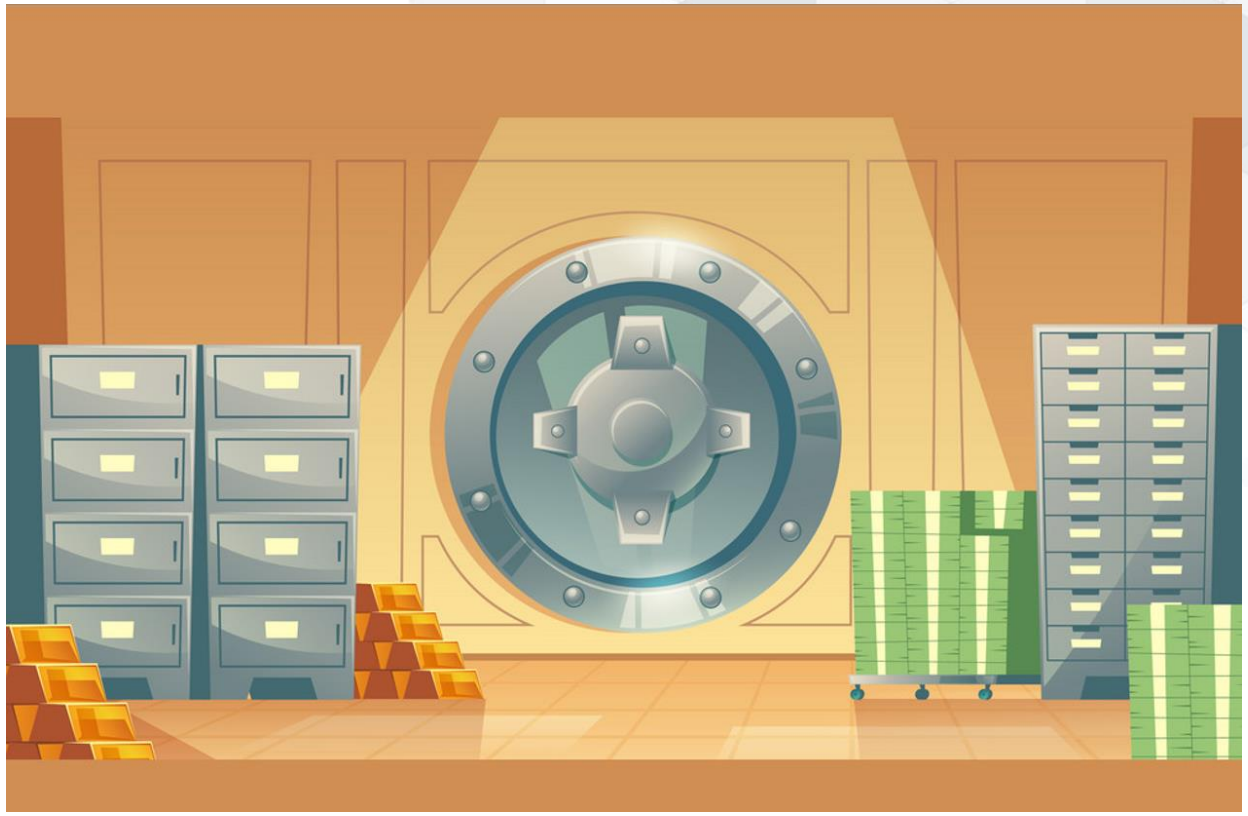
Continuously staying in compliance as cloud environment changes

39%

Going through audit/ risk assessment within the cloud environment

Source: 2022 Cloud Security Report – (ISC)[2] and Cybersecurity Insiders

VS



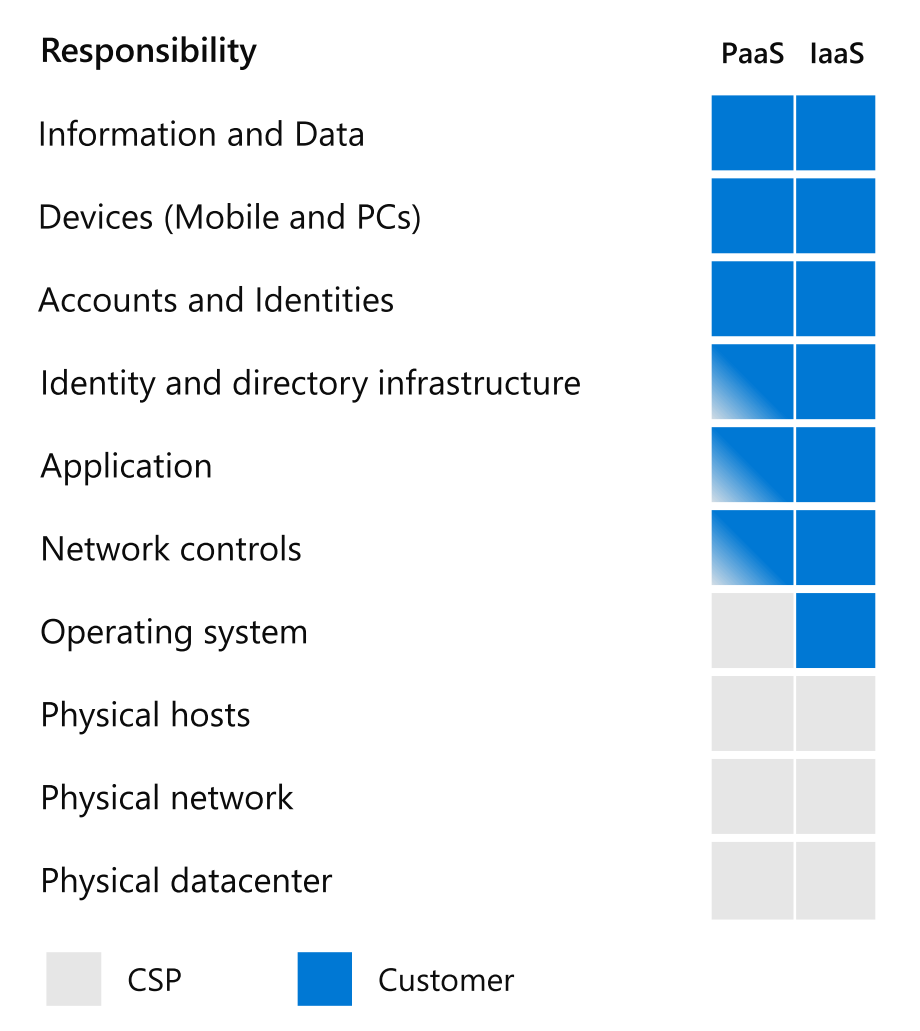
CSA APAC cloud security ASIA PACIFIC REGION alliance

Shared Responsibility Model and Key Strategies

Responsibility	SaaS	PaaS	IaaS	On-prem	
Information and Data	Customer	Customer	Customer	Customer	ESTABLISH A MODERN PERIMETER
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer	
Accounts and Identities	Customer	Customer	Customer	Customer	
Identity and directory infrastructure	Customer	Customer	Customer	Customer	MODERNIZE INFRASTRUCTURE SECURITY
Applications	CSP	Customer	Customer	Customer	
Network Controls	CSP	Customer	Customer	Customer	
Operating system	CSP	CSP	Customer	Customer	
Physical hosts	CSP	CSP	CSP	Customer	"TRUST BUT VERIFY" EACH CLOUD PROVIDER
Physical network	CSP	CSP	CSP	Customer	
Physical datacenter	CSP	CSP	CSP	Customer	

CSP Customer

Security Responsibilities Transfer to Cloud



Transferred for PaaS

Security Patches

Feature Upgrades

VMs/Containers security –
OS and Middleware Installation, Maintenance, troubleshooting, etc.

Marketplace
fits PaaS or IaaS model

Transferred for IaaS and PaaS

Denial of Service*

Racking/Stacking Servers, Delays in Adding Capacity

Fabric/Virtualization Patching, Maintenance & Troubleshooting

Fabric Availability / Uptime
→ SLA from CSP

Attacks on

- Physical Attacks
- Virtualization Fabric
- Hardware/Firmware
- Network Infrastructure

What Is CCM?

- Industry leading cloud security control framework since 2010
- Research driven by cloud customers, providers & assurance professionals
- Simplified approach to implementation, validation & compliance across all clouds
- Delineates control owners aligned to a shared responsibilities model for providers & consumers
- Provider per control service delivery model applicability for SaaS, PaaS & IaaS
- Aligned & Mapped to global regulations and the most relevant security frameworks
- Backbone of CSA STAR to assess & compare Cloud Service Providers (CSPs)

CCM™
Cloud Controls Matrix

cloud security alliance℠

Cloud Controls Matrix v4

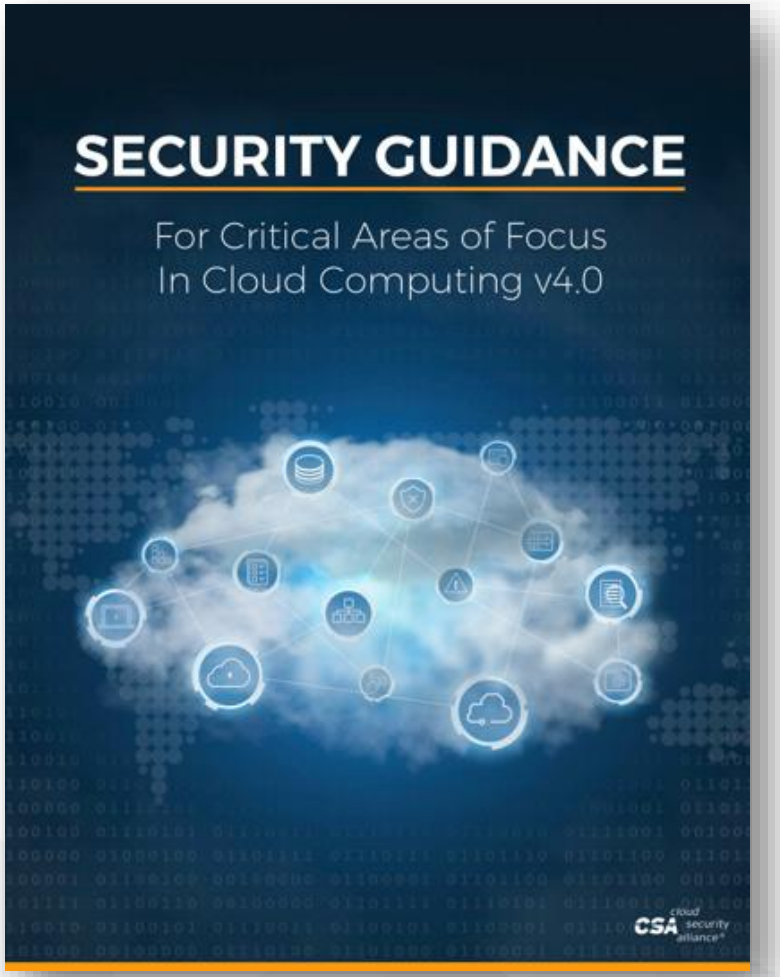
Release Date: 01/20/2021

A&A	Audit and Assurance
AIS	Application & Interface Security
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control and Configuration Management
CEK	Cryptography, Encryption and Key Management
DCS	Datacenter Security
DSP	Data Security and Privacy
GRC	Governance, Risk Management and Compliance
HRS	Human Resources Security
IAM	Identity & Access Management
IPY	Interoperability & Portability
IVS	Infrastructure & Virtualization Security
LOG	Logging and Monitoring
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management
UEM	Universal EndPoint Management

17 Control Domains
Over 190+ Controls

CSA APAC cloud security ASIA PACIFIC REGION alliance

CSA Security Guidance v4.0



- Fundamental cloud security research that started CSA
- Foundation for certificate of cloud security knowledge (CCSK)
- 4th version, released July 2017
- Architecture
- Governing in the cloud
  - Governance and enterprise risk management
  - Legal
  - Compliance & audit management
  - Information governance
- Operating in the cloud
  - Management plane & business continuity
  - Infrastructure security
  - Virtualization & containers
  - Incident response
  - Application security
  - Data security & encryption
  - Identity management
  - Security as a service
  - Related technologies

CSA STAR: Security, Trust & Assurance Registry

Launched in 2011, the CSA STAR is the first step improving transparency and assurance in the cloud.

- Searchable registry to allow cloud customers to review the security practices of providers, accelerating their due diligence and leading **to higher quality procurement experiences**
- STAR is a **publicly accessible** registry that documents the security controls provided by cloud computing offerings
- Helps users to assess the security of cloud providers
- It is based on a multi-layered structure defined by **Open Certification Framework working group**

11 Security Recommendations for Production Instances on Alibaba Cloud

1. Identity Access Management
2. Enable ActionTrail
3. KMS and Encryption Setup
4. Protect Data Stored in OSS Buckets
5. TLSv1.2 on Server Load Balancer
6. Reduce External Exposure of Alibaba Cloud Resources
7. Secure Bastion Hosts
8. Hardening ECS OS Images
9. Vulnerability and Penetration Testing of ECS Instance
10. Monitoring
11. Incident Management and Response

Source: https://www.alibabacloud.com/blog/11-security-recommendations-for-production-instances-on-alibaba-cloud_594743

Ten places security teams should spend time

1. Accurate account info
2. Use MFA
3. No hard-coding secrets
4. Limit security groups
5. Intentional data policies
6. Centralize AWS logs
7. Validate IAM roles
8. Take action on security findings
9. Rotate your secrets
10. Involve security in the development lifecycle

Source: Amazon Web Services

Top 10 (+1) Best Practices

Microsoft Azure

People

Cloud security journey https://aka.ms/AzSec1	1
Cloud technical training https://aka.ms/AzSec2	2

Process

Assign Accountability https://aka.ms/AzSec3	3
Rapid incident response https://aka.ms/AzSec4	4
Posture Management https://aka.ms/AzSec5	5

Technology

Passwordless / MFA https://aka.ms/AzSec6	6
Native Network Security & Firewall https://aka.ms/AzSec7	7
Native Threat Detection https://aka.ms/AzSec8	8

Foundational Architecture Decisions

Single directory / identity https://aka.ms/AzSec9	9
Identity access controls https://aka.ms/AzSec10	10
Single strategy https://aka.ms/AzSec11	11

Source: https://aka.ms/AzureSecurityTop10

CSA APAC cloud security ASIA PACIFIC REGION alliance

Google Cloud Whitepaper
December 2021

Google Cloud security foundations guide

Security Foundations Blueprint

1. Google Cloud foundation security model
2. Google Cloud foundation Design
3. Google Cloud Organization Structure
4. Resource Deployment
5. Authentication and authorization
6. Networking
7. Key and secret management
8. Logging
9. Detective controls
10. Billing
11. Creating and deploying secured applications
12. General Security guidance

Source: Google Cloud Security Foundations Guide

CIS AWS Foundations controls

Security Hub con

Filter contro

2.3 Ensure the CloudTrail logs accessible

Compliant

1 account passe

2.6 Ensure S3 I enabled on the

Non-complia

1 account failed

Findings

Findings document a security or compliance issue.

Record st

Severit

LOW

LOW

LOW

LOW

LOW

Insights (33)

An insight is a c

Filter insig

1. AWS resour findings

4. EC2 instanc Tactics, Techn (TTPs)

7. AWS resour potential data

Integrations

By enabling an integration, you put in place the permissions to receive findings from that integration.

Filter integrations

Amazon GuardDuty

A threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.

Disable | Configure

Amazon Inspector

An automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

Disable | Configure

Amazon Macie

A security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

Disable | Configure

ARMOR Armor Anywhere

Armor Anywhere delivers managed security and compliance for AWS.

Disable | Configure

Alert Logic SIEMless ThreatManagement

Get the right level of coverage: Vulnerability and asset visibility, threat detection and incident management, WAF, and assigned SOC analyst options.

Enable | Purchase

Barracuda Networks Cloud Security Guardian

Barracuda Cloud Security Guardian is a SaaS service that makes it simple and easy to stay secure while building applications in, and moving workloads to, public-cloud infrastructures.

Disable | Configure

Source: https://aws.amazon.com/blogs/aws/aws-security-hub-now-generally-available/

Microsoft Azure

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Regulatory compliance

Showing 33 subscriptions

Microsoft Defender for Cloud | Recommendations

Showing 33 subscriptions

Download CSV report | Guides & Feedback

Secure score 67%

Microsoft Defender for Cloud | Workload protections

Showing 54 subscriptions

Subscriptions | What's new

Defender for Cloud coverage

665 TOTAL

- Fully covered (89.5%)
- Agent not installed (3.8%) Install
- Not covered (6.8%) Upgrade all

216/225 Servers	51/51 App service	21/30 Containers	40/40 Key vaults	
Upgrade	Upgrade	Upgrade	Upgrade	
27/27 Azure SQL database servers	195/209 Storage	12/12 Resource manager subscriptions	12/12 DNS subscriptions	
Upgrade	Upgrade	Upgrade	Upgrade	

Security alerts

High severity 4.8K
Medium severity 1K
Low severity 1.9K

Advance protection

VM vulnerability assessment 127 Unprotected	Just-in-time VM Access 70 Unprotected	Adaptive application control 44 Unprotected	Container image scanning 6 Unprotected
SQL vulnerability assessment 9 Unprotected	File integrity monitoring	Network map	IoT security

Insights

Upgrade to New Containers

Click here to upgrade >

Most prevalent recommend

- Audit diagnostic setting
- Storage account public acc
- A vulnerability assessment

Most attacked resources

- contoso5.cloudapp.net
- Virtual machine 2
- CentOS

View full alert list >

Controls with the highest pc

- Remediate vulnerabilities
- Enable encryption at rest
- Remediate security configu

View controls >

Source: Microsoft Defender for Cloud

CSA APAC cloud security ASIA PACIFIC REGION alliance

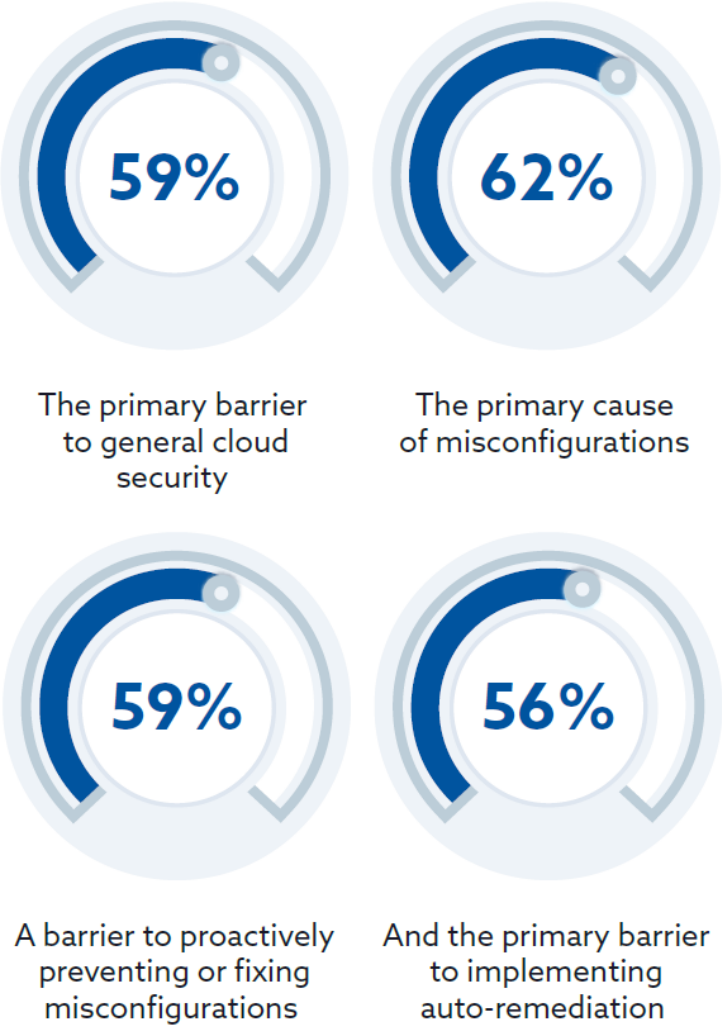
Key Finding 1

Lack of knowledge and expertise continue to plague security teams

Lack of knowledge and expertise are well-known issues within the information security industry. It is no surprise then, that lack of knowledge and expertise was consistently identified as:

- The primary barrier to general cloud security (59%)
- The primary cause of misconfigurations (62%)
- A barrier to proactively preventing or fixing misconfigurations (59%)
- The primary barrier to implementing auto-remediation (56%)

These findings highlight the trickle-down effect that lack of knowledge can have on security teams. It starts as a general barrier to implementing effective cloud security measures. This leads to misconfigurations, the primary cause of data breaches. But it's also preventing security teams from implementing a solution, such as auto-remediation, which could supplement this knowledge and skills deficit.



Source: The State of Cloud Security Risk, Compliance, and Misconfigurations (2021) – Cloud Security Alliance

STAR Resources, CCAK, CCSK

CCM™
Cloud Controls Matrix

https://cloudsecurityalliance.org/research/cloud-controls-matrix

STAR™
Security, Trust, Assurance & Risk Registry

https://cloudsecurityalliance.org/star/
https://cloudsecurityalliance.org/star/registry/

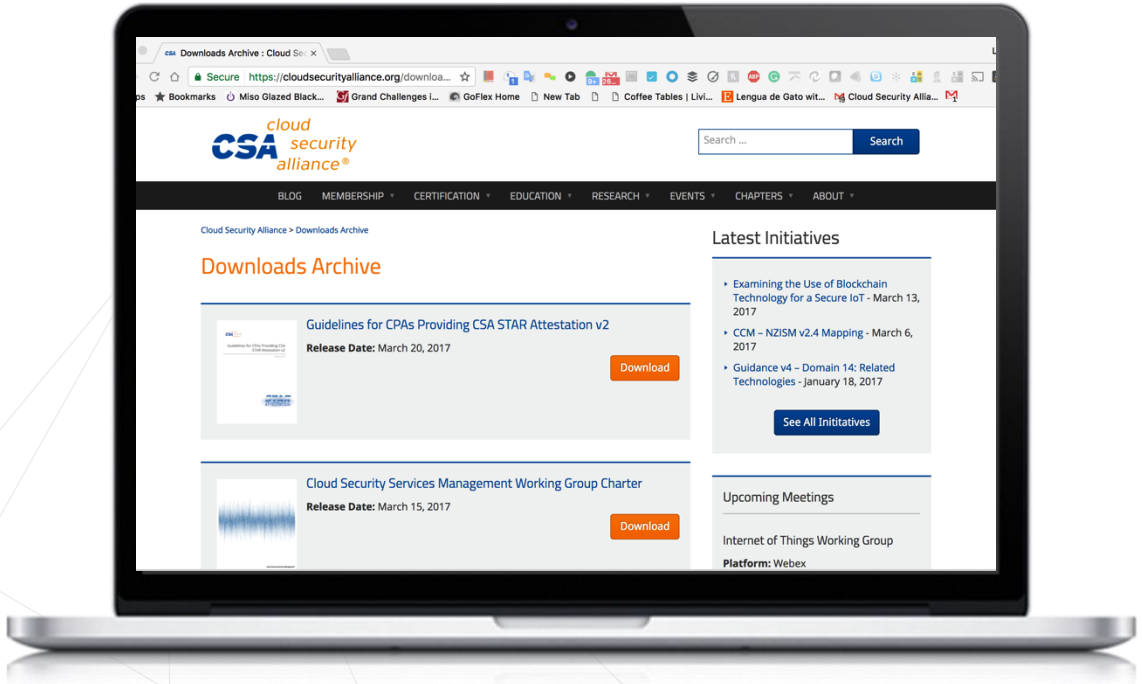
CCAK™
Certificate of Cloud Auditing Knowledge
A Cloud Security Alliance® and ISACA® Credential

https://cloudsecurityalliance.org/education/ccak

CCSK™
Certificate of
Cloud Security Knowledge

https://cloudsecurityalliance.org/education/ccsk

THANK YOU



Contact CSA

Email: chairman@csahkm.org

Twitter: @Cloudsa

Site: www.cloudsecurityalliance.org

Hong Kong & Macau Chapter: www.csahkm.org

Learn: www.cloudsecurityalliance.org/research/cloudbytes

Download: www.cloudsecurityalliance.org/download

GDPR Resource center: https://gdpr.cloudsecurityalliance.org