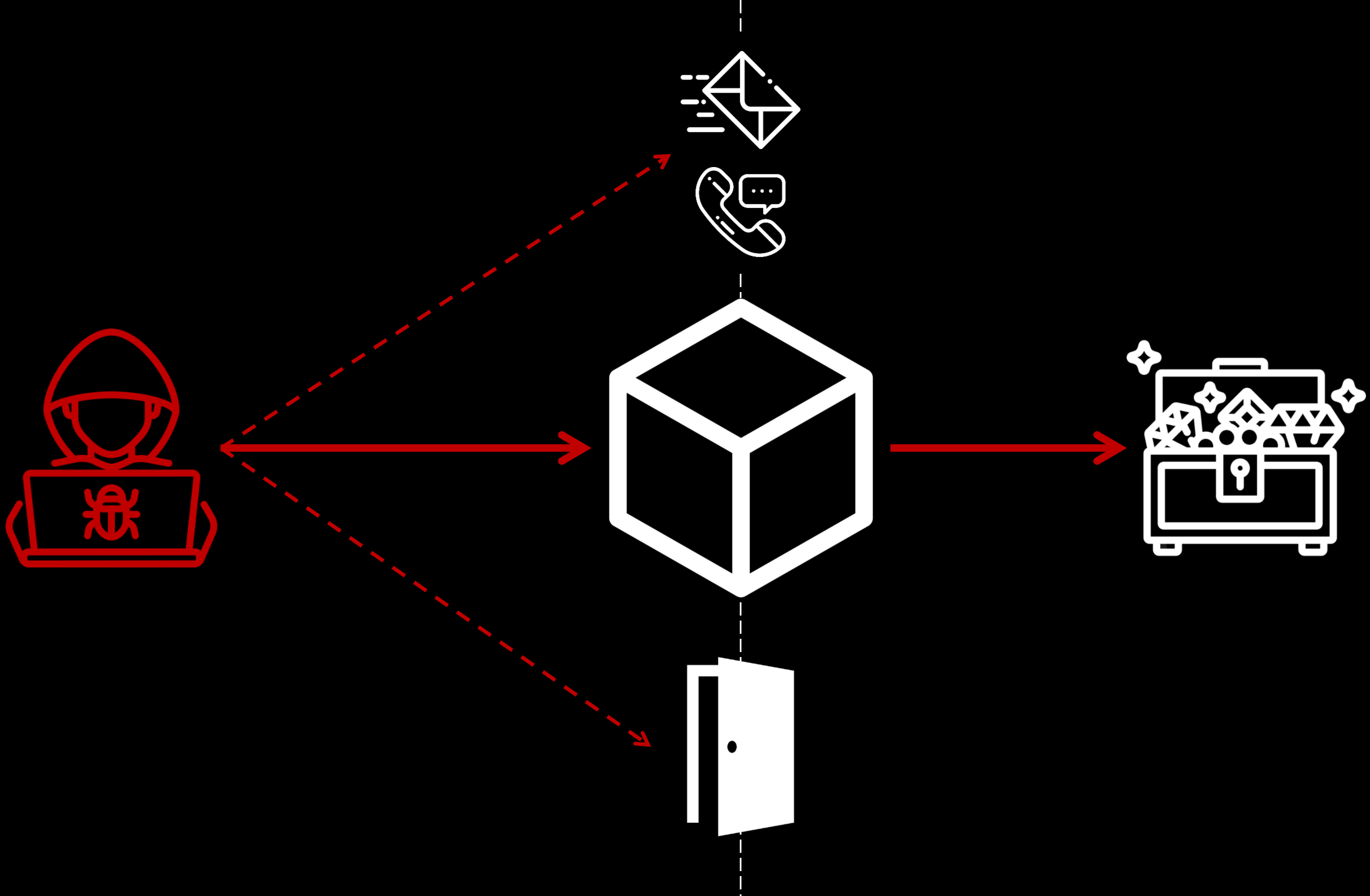
"T.I.S.P. Community Meeting 2021"

Berlin, 03.-04.11.2021

Cloud Security: Konfigurationsprüfung und Audit

Christian Titze, Secorvo Security Consulting GmbH

```
$ whoami
```



pls hack `127.0.0.1, ::1,`
and `169.254.13.37`
kthxbye

Human Operators

⚠ Bad Passwords

Users and Groups

⚠ Exposed Management Interfaces

Applications

Runtimes

Whitelisting

⚠ AV Evasion

Antivirus

Firewall

⚠ Vulnerabilities

Services

Network Segmentation

Network Stack

⚠ Misconfigurations

Cryptography

⚠ RCE & PrivEsc Vulns

Operating System & Virtualization

Hardware & Firmware

Physical Security

Services

Web
Storage
Dev / Management

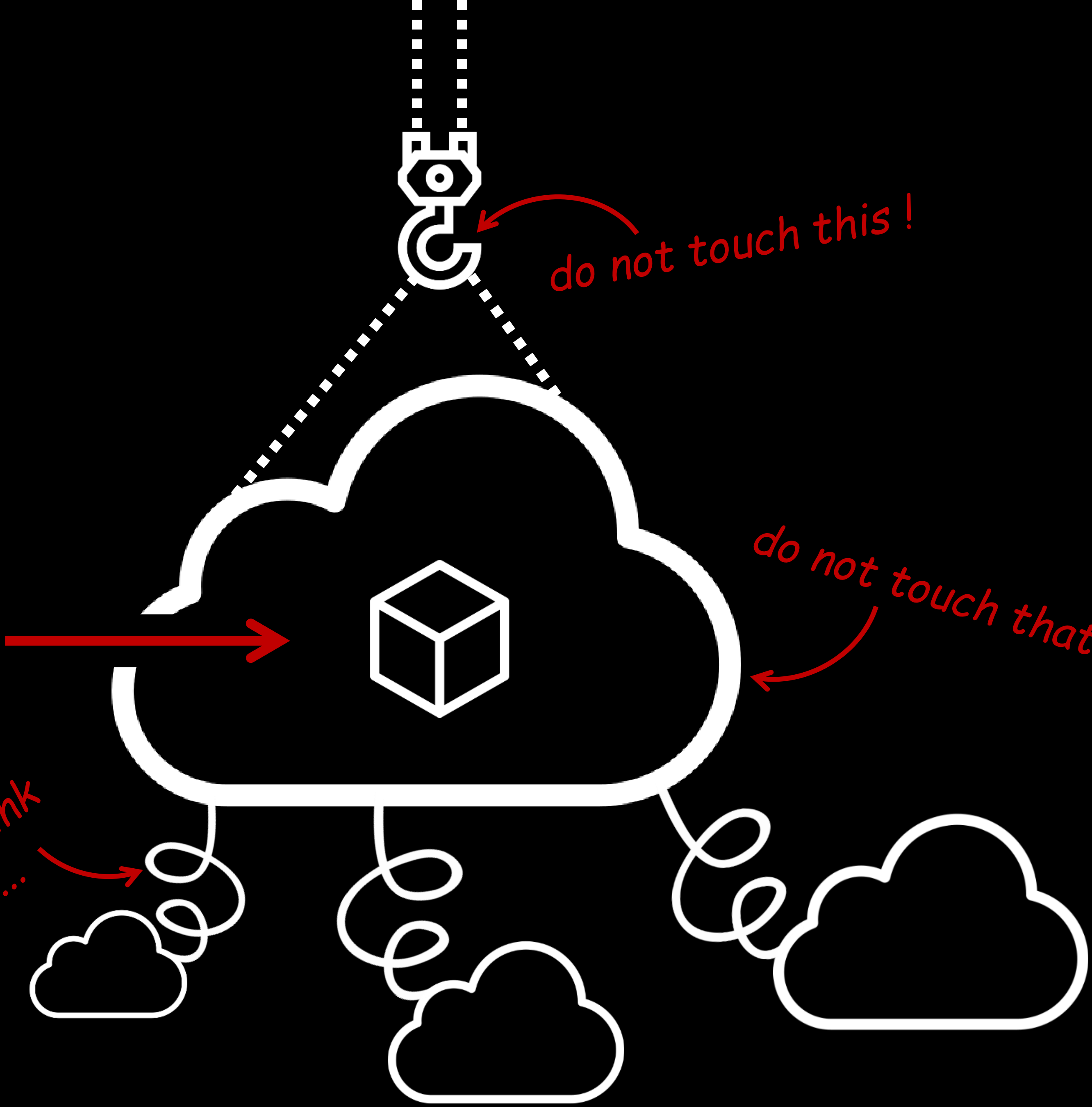
Systems

Virtual Machines
Containers
Serverless Computing

Networks

Segmentation / Filtering
Redundancy
Load Balancing

ENTRANCE THIS WAY



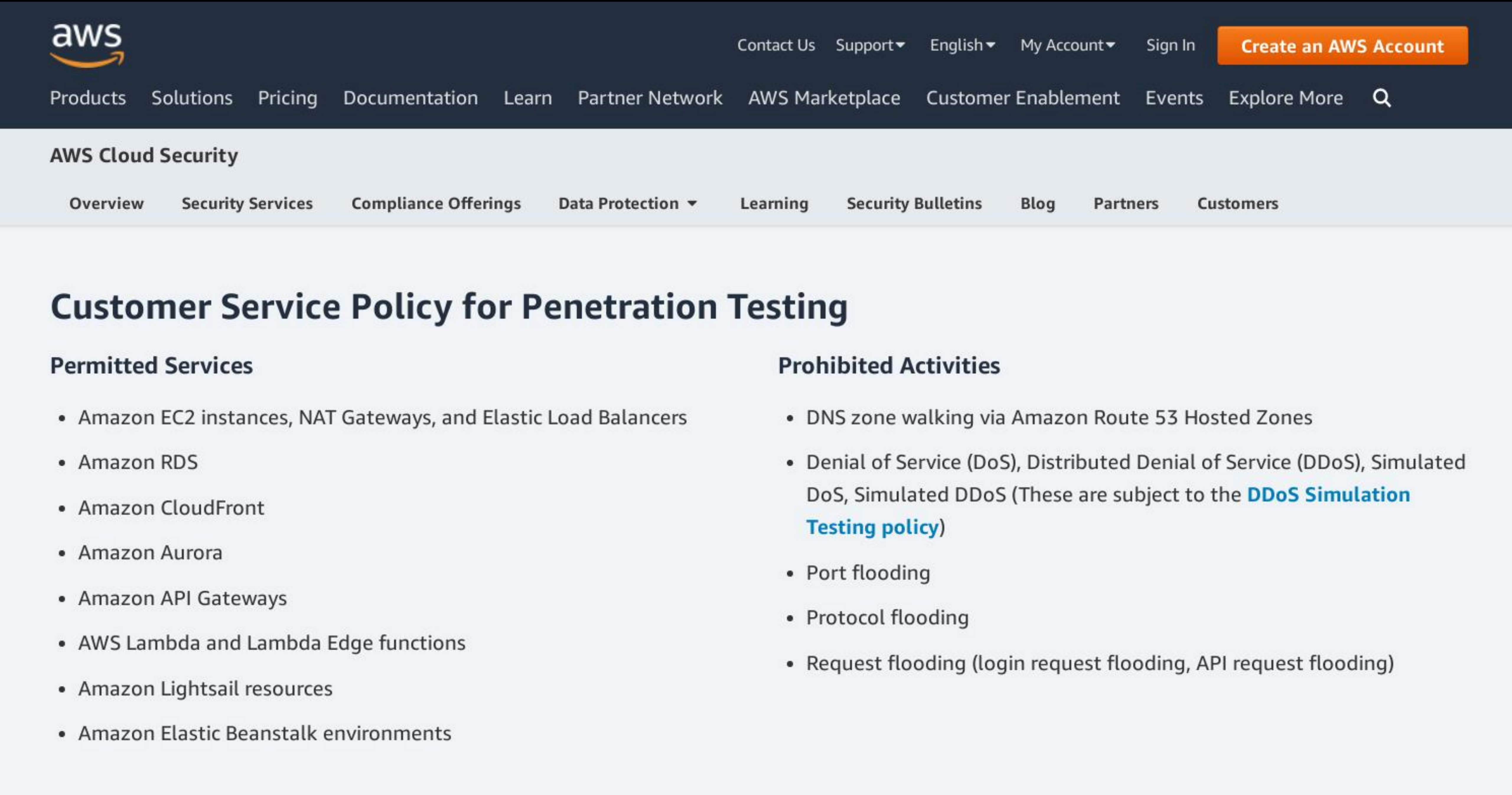
do not touch this !

do not touch that !

don't even think about it ...

step one

Understand CSP‘s Policies for Penetration Testing



Customer Service Policy for Penetration Testing

Permitted Services

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

Prohibited Activities

- DNS zone walking via Amazon Route 53 Hosted Zones
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS (These are subject to the **DDoS Simulation Testing policy**)
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

Penetration Testing Rules of Engagement

Microsoft Cloud

RULES OF ENGAGEMENT TO PERFORM PENETRATION TESTING ON THE MICROSOFT CLOUD

The goal of this program is to enable customers to test their services hosted in Microsoft Cloud services without causing harm to any other Microsoft customers.

The following activities are prohibited:

- Scanning or testing assets belonging to any other Microsoft Cloud customers.
- Gaining access to any data that is not wholly your own.
- Performing any kind of denial of service testing.
- Performing network intensive fuzzing against any asset except your Azure Virtual Machine
- Performing automated testing of services that generates significant amounts of traffic.
- Deliberately accessing any other customer's data.
- Moving beyond "proof of concept" repro steps for infrastructure execution issues (i.e. proving that you have sysadmin access with SQLi is acceptable, running xp_cmdshell is not).
- Using our services in a way that violates the Acceptable Use Policy, as set forth in the **Microsoft Online Service Terms**.
- Attempting phishing or other social engineering attacks against our employees.

Cloud Security FAQ

Here you will find answers to some Frequently Asked Questions related to Security and Compliance on Google Cloud Platform.

For more information about security of the platform and its products, please see Google Cloud Platform Security and Compliance

Penetration testing

Do I need to notify Google that I plan to do a penetration test on my project?

> If you plan to evaluate the security of your Cloud Platform infrastructure with penetration testing, you are not required to contact us. You will have to abide by the Cloud Platform Acceptable Use Policy and Terms of Service, and ensure that your tests only affect your projects (and not other customers' applications). If a vulnerability is found, please report it via the Vulnerability Reward Program.

Help

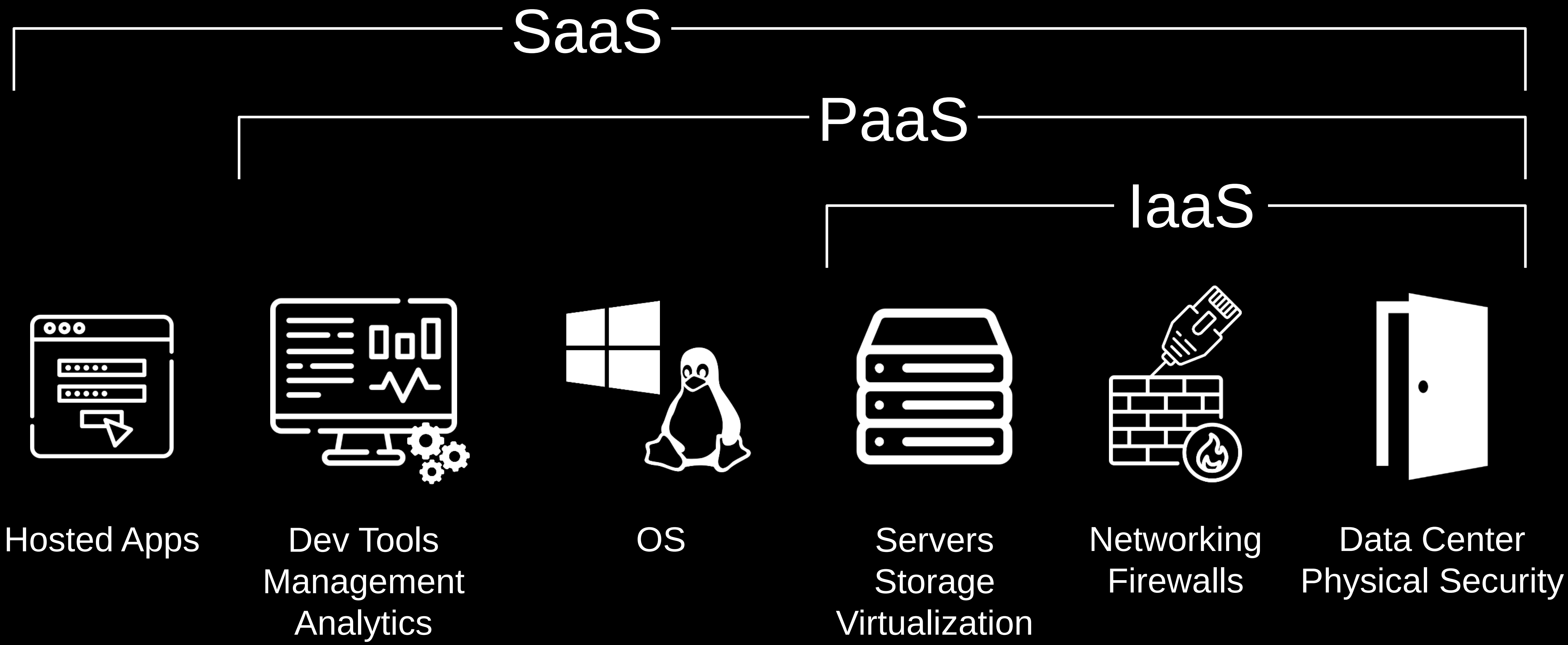
Cloud Security FAQ

Privacy compliance and records for Google Cloud

legal

Shift of Attack Surface

(...and security testing methodology)



SaaS

PaaS

IaaS

Hosted Apps

Dev Tools
Management
Analytics

OS

Servers
Storage
Virtualization

Networking
Firewalls

Data Center
Physical Security

SCHWARZER PETER
Das Original
Das Original nach Entwürfen des Altenburger Skatmalers Otto Pech – genannt Pix
Finde die Paare!
Art.-Nr. 225 72025
4 042677 720252
ASS ALTENBURGER SEIT 1765
ASS Altenburger, Leipziger Str. 7, D-04600 Altenburg
ASS Altenburger
Hahn 5
Maus 14
Hase
2. Wo ist die Häsin?
Igel 3
3. Wo ist die Igelin?
Finkin 10
10. Wo ist der Fink?
7. Wo ist der Enterich?
der Mausbock?

Shared Responsibility

Security *of* the Cloud

Measures that the CSP implements and operates

Security *in* the Cloud

Measures that the customer implements and operates

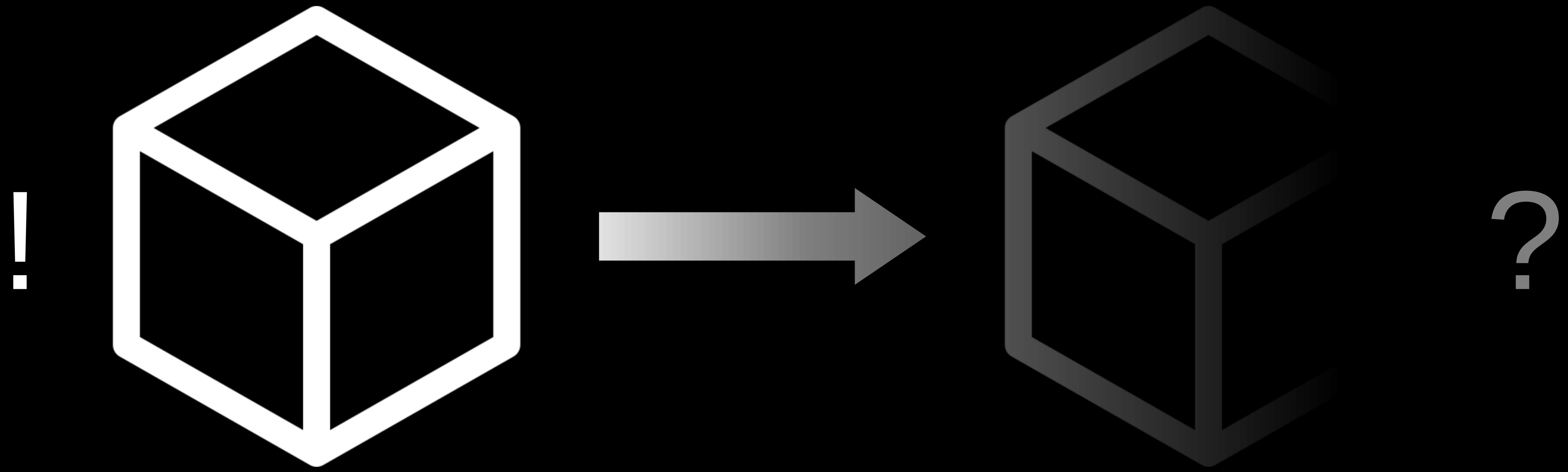
	On-Prem	IaaS	PaaS	SaaS
Information and Data	👥	👥	👥	👥
Clients and Endpoint Protection	👥	👥	👥	👥
Accounts and Identities	👥	👥	👥	👥
Identity and Directory Infrastructure	👥	👥	👥 ☁	👥 ☁
Applications	👥	👥	👥 ☁	☁
Network Controls	👥	👥	👥 ☁	☁
Operating System	👥	👥	☁	☁
Host and Network Infrastructure	👥	☁	☁	☁
Physical Security	👥	☁	☁	☁

	On-Prem	IaaS	PaaS	SaaS
Information and Data	👥	👥	👥	👥
Clients and Endpoint Protection	👥	👥	👥	👥
Accounts and Identities	👥	👥	👥	👥
Identity and Directory Infrastructure	👥	👥	👥 ☁	👥 ☁
Applications	👥	👥	👥 ☁	☁
Network Controls	👥	👥	👥 ☁	☁
Operating System	👥	👥	☁	☁
Host and Network Infrastructure	👥	☁	☁	☁
Physical Security	👥	☁	☁	☁

	On-Prem	IaaS	PaaS	SaaS
Information and Data	👥	👥	👥	👥
Clients and Endpoint Protection	👥	👥	👥	👥
Accounts and Identities	👥	👥	👥	👥
Identity and Directory Infrastructure	👥	👥	👥 ☁	👥 ☁
Applications	👥	👥	👥 ☁	☁
Network Controls	👥	👥	👥 ☁	☁
Operating System	👥	👥	☁	☁
Host and Network Infrastructure	👥	☁	☁	☁
Physical Security	👥	☁	☁	☁

	On-Prem	IaaS	PaaS	SaaS
Information and Data	👥	👥	👥	👥
Clients and Endpoint Protection	👥	👥	👥	👥
Accounts and Identities	👥	👥	👥	👥
Identity and Directory Infrastructure	👥	👥	👥 ☁	👥 ☁
Applications	👥	👥	👥 ☁	☁
Network Controls	👥	👥	👥 ☁	☁
Operating System	👥	👥	☁	☁
Host and Network Infrastructure	👥	☁	☁	☁
Physical Security	👥	☁	☁	☁

	On-Prem	IaaS	PaaS	SaaS
Information and Data	👥	👥	👥	👥
Clients and Endpoint Protection	👥	👥	👥	👥
Accounts and Identities	👥	👥	👥	👥
Identity and Directory Infrastructure	👥	👥	👥 ☁	👥 ☁
Applications	👥	👥	👥 ☁	☁
Network Controls	👥	👥	👥 ☁	☁
Operating System	👥	👥	☁	☁
Host and Network Infrastructure	👥	☁	☁	☁
Physical Security	👥	☁	☁	☁



!

?

Shooting at Clouds

a.k.a. *“Cloud Pentesting”*

External Penetration Test

Pentest with significantly limited scope and a focus on information gathering and / or vulnerability scanning

Cloud-Internal Penetration Test

Simulates an attacker with foothold in virtual cloud infrastructure

Configuration Review

Detection of misconfigurations and disregarded best practices

External Penetration Test

Pentest with significantly limited scope and a focus on information gathering and / or vulnerability scanning

Cloud-Internal Penetration Test

Simulates an attacker with foothold in virtual cloud infrastructure

Configuration Review

Detection of misconfigurations and disregarded best practices

Not to be confused with a custom web application pentest!

Internal pentest and configuration review go hand in hand. Combine them!

step two

Understand the Customer’s Cloud Estate & Create a Cloud Penetration Testing Plan

Map Cloud Estate

Map Cloud Estate

Management Interfaces

Login Interfaces

Directory Services

Web Applications

Databases / Storage

Virtual Machines

Subscriptions

Relationships

Remote Access

APIs / Endpoints

(Sub-) Networks

Development Resources

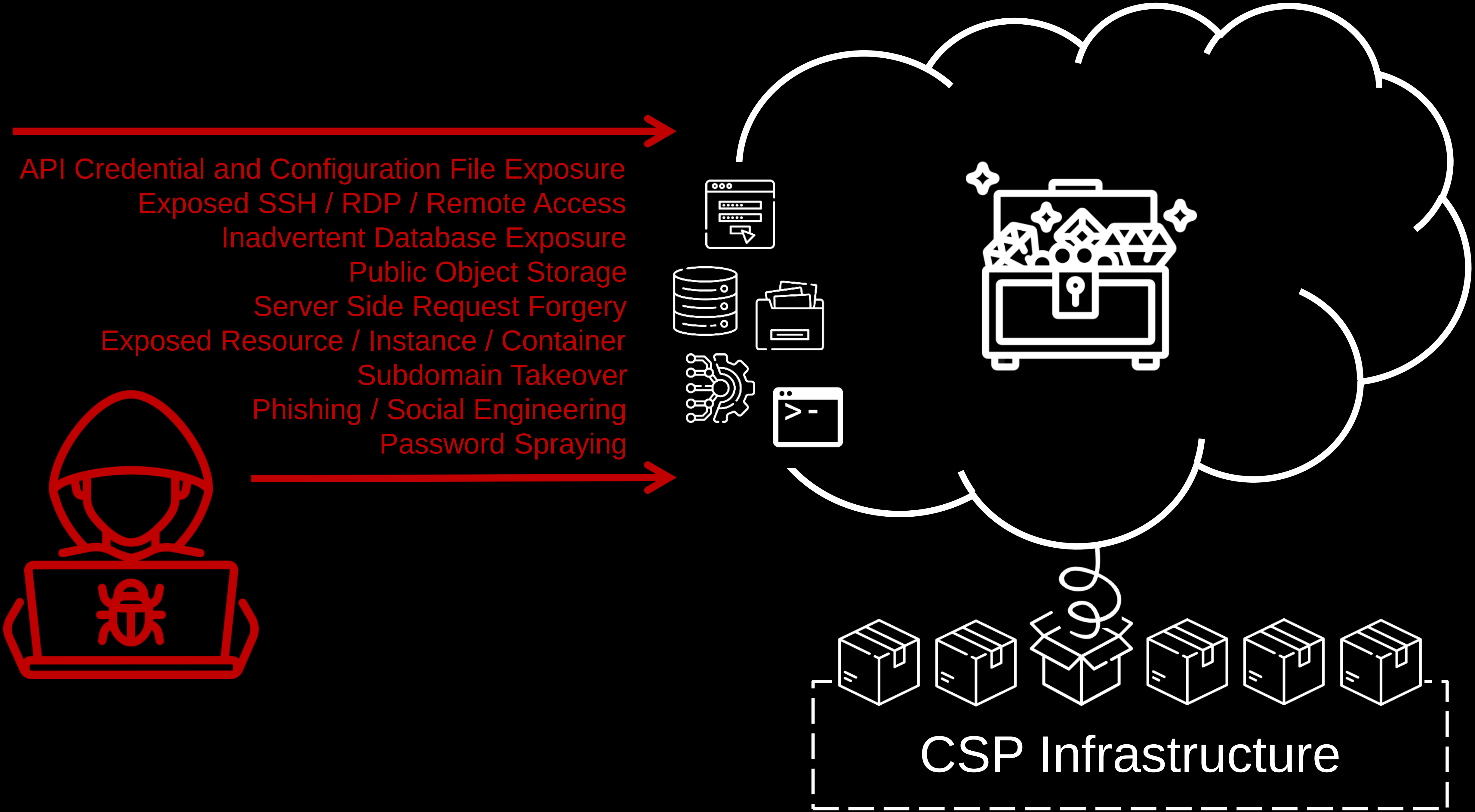
HARD

TIME-CONSUMING

FINANCIALLY UNATTRACTIVE

Alternative:
Reconnaissance?

REALISTIC



API Credential and Configuration File Exposure
Exposed SSH / RDP / Remote Access
Inadvertent Database Exposure
Public Object Storage
Server Side Request Forgery
Exposed Resource / Instance / Container
Subdomain Takeover
Phishing / Social Engineering
Password Spraying

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CSV-T08

Break the Top 10 Cloud Attack Killchains

Rich Mogull
Analyst/Securosis
CISO/DisruptOps
@rmogull

{disrupt:Ops}

Shawn Harris
Managing Principal Security Architect
Starbucks
@infotechwarrior

#RSAC

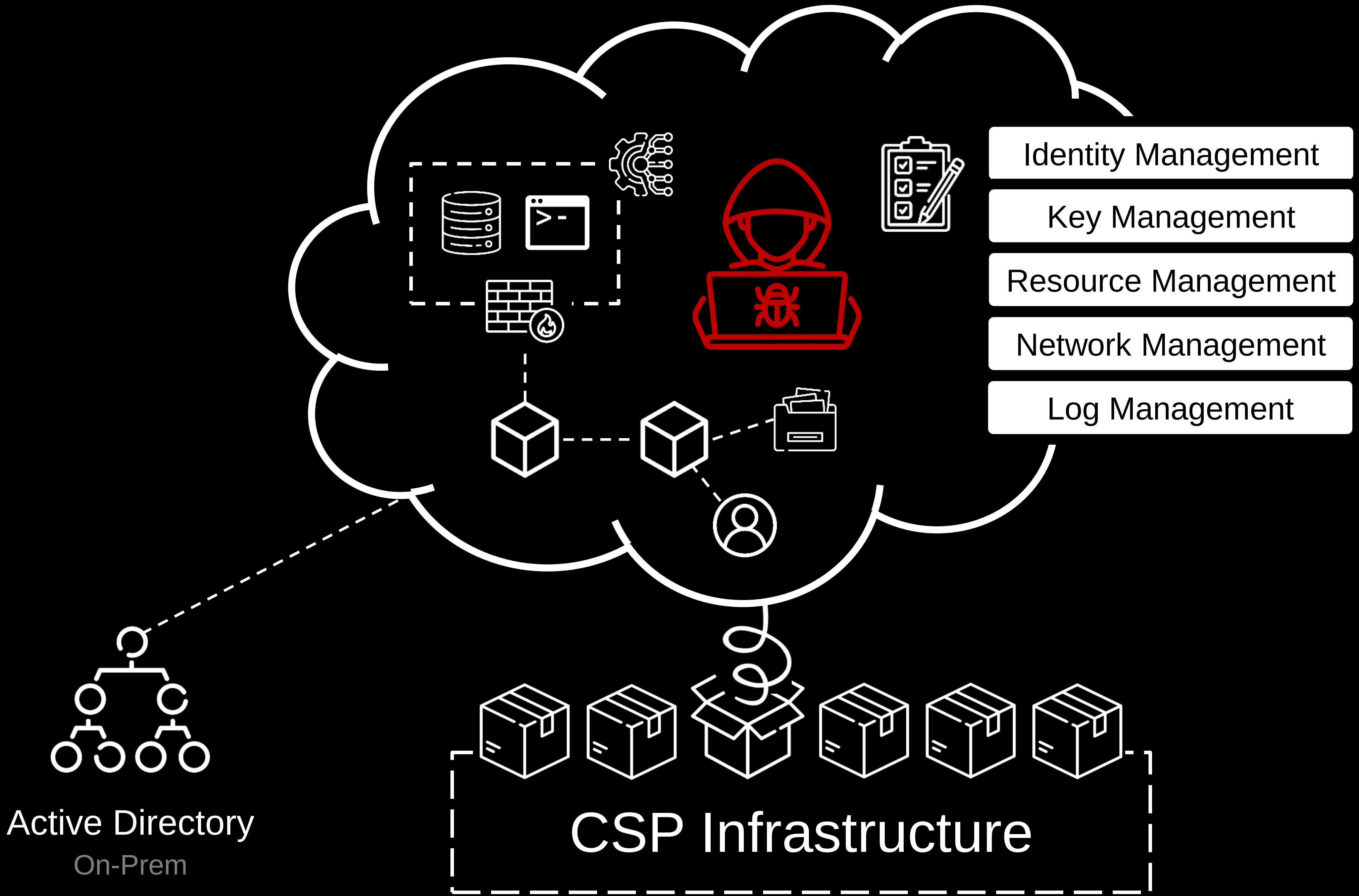
Top Threats to Cloud Computing

The Egregious 11

CSA cloud security alliance®

Top Threats to Cloud Computing: Egregious Eleven Deep Dive

CSA cloud security alliance®

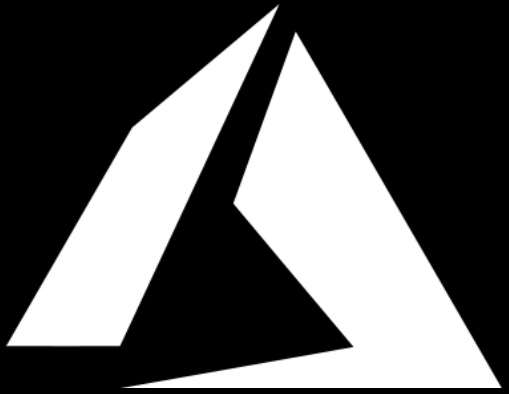

Identity Management
Key Management
Resource Management
Network Management
Log Management
Active Directory
On-Prem
CSP Infrastructure

step three

Execute the Plan & Report the Findings

Cloud Security Scanners

Configuration Review



Azure

Security design principles

11/01/2021 • 5 minutes to read •

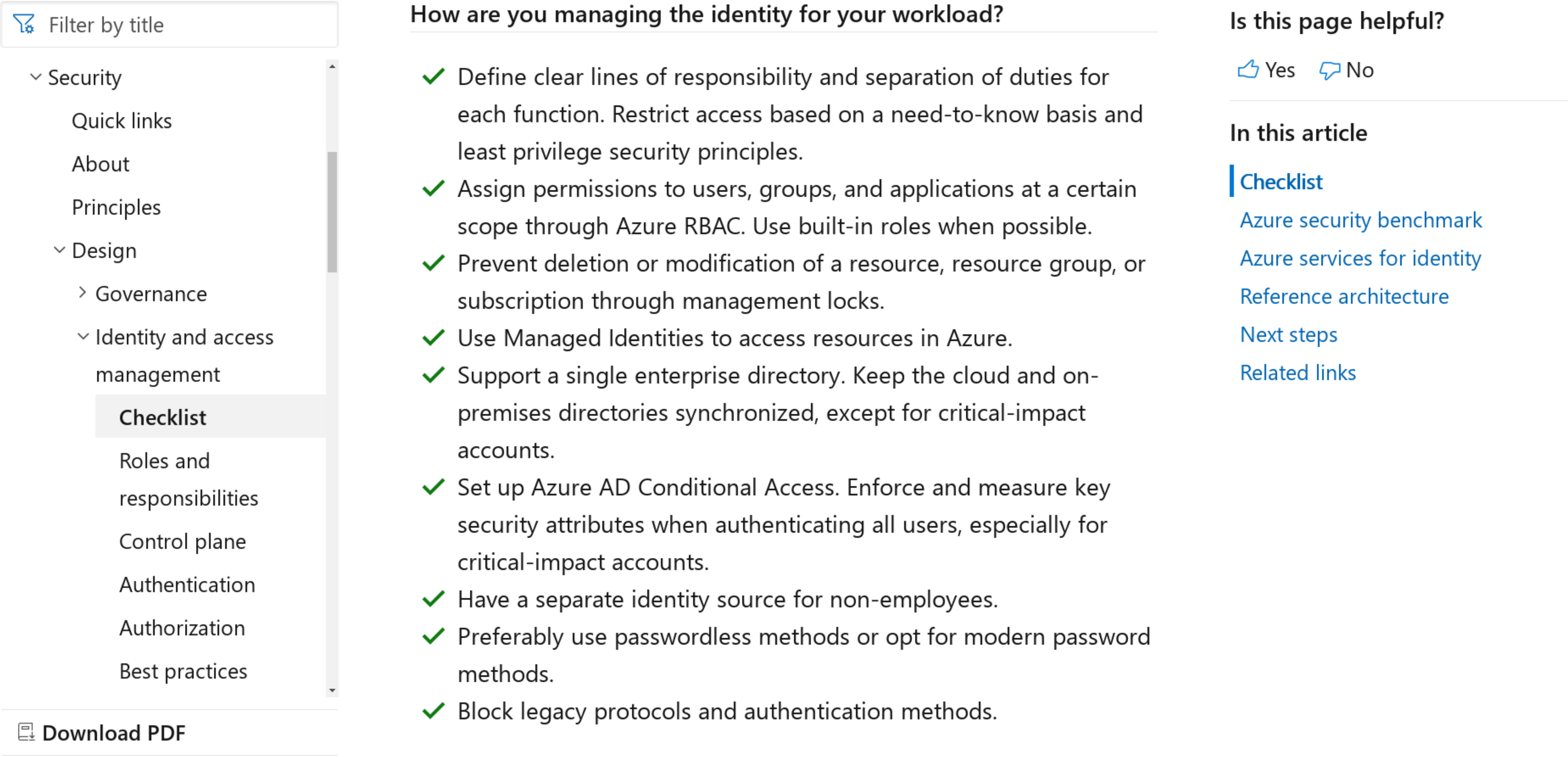
Is this page helpful?

Yes No

These principles support these three key strategies and describe a securely architected system hosted on cloud or on-premises datacenters (or a combination of both). Application of these principles will dramatically increase the likelihood your security architecture will maintain assurances of confidentiality, integrity, and availability.

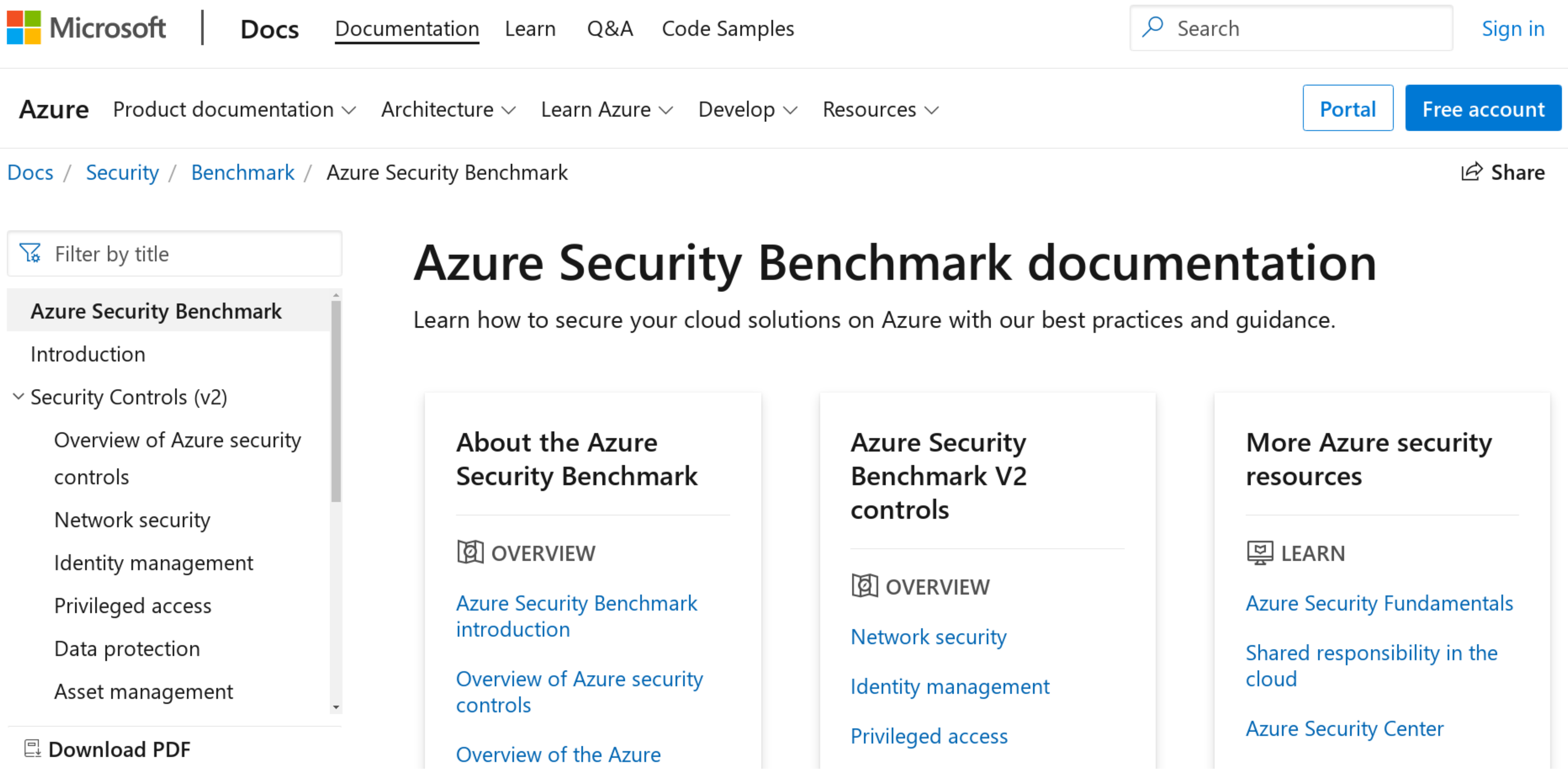
Each recommendation in this document includes a description of why it is recommended, which maps to one of more of these principles:

- **Align Security Priorities to Mission** – Security resources are almost always limited, so prioritize efforts and assurances by aligning security strategy and technical controls to the business using classification of data and systems. Security resources should



How are you managing the identity for your workload?

- ✓ Define clear lines of responsibility and separation of duties for each function. Restrict access based on a need-to-know basis and least privilege security principles.
- ✓ Assign permissions to users, groups, and applications at a certain scope through Azure RBAC. Use built-in roles when possible.
- ✓ Prevent deletion or modification of a resource, resource group, or subscription through management locks.
- ✓ Use Managed Identities to access resources in Azure.
- ✓ Support a single enterprise directory. Keep the cloud and on-premises directories synchronized, except for critical-impact accounts.
- ✓ Set up Azure AD Conditional Access. Enforce and measure key security attributes when authenticating all users, especially for critical-impact accounts.
- ✓ Have a separate identity source for non-employees.
- ✓ Preferably use passwordless methods or opt for modern password methods.
- ✓ Block legacy protocols and authentication methods.



Azure Security Benchmark documentation

Learn how to secure your cloud solutions on Azure with our best practices and guidance.

About the Azure Security Benchmark

OVERVIEW

Azure Security Benchmark introduction

Overview of Azure security controls

Overview of the Azure

Azure Security Benchmark V2 controls

OVERVIEW

Network security

Identity management

Privileged access

More Azure security resources

LEARN

Azure Security Fundamentals

Shared responsibility in the cloud

Azure Security Center

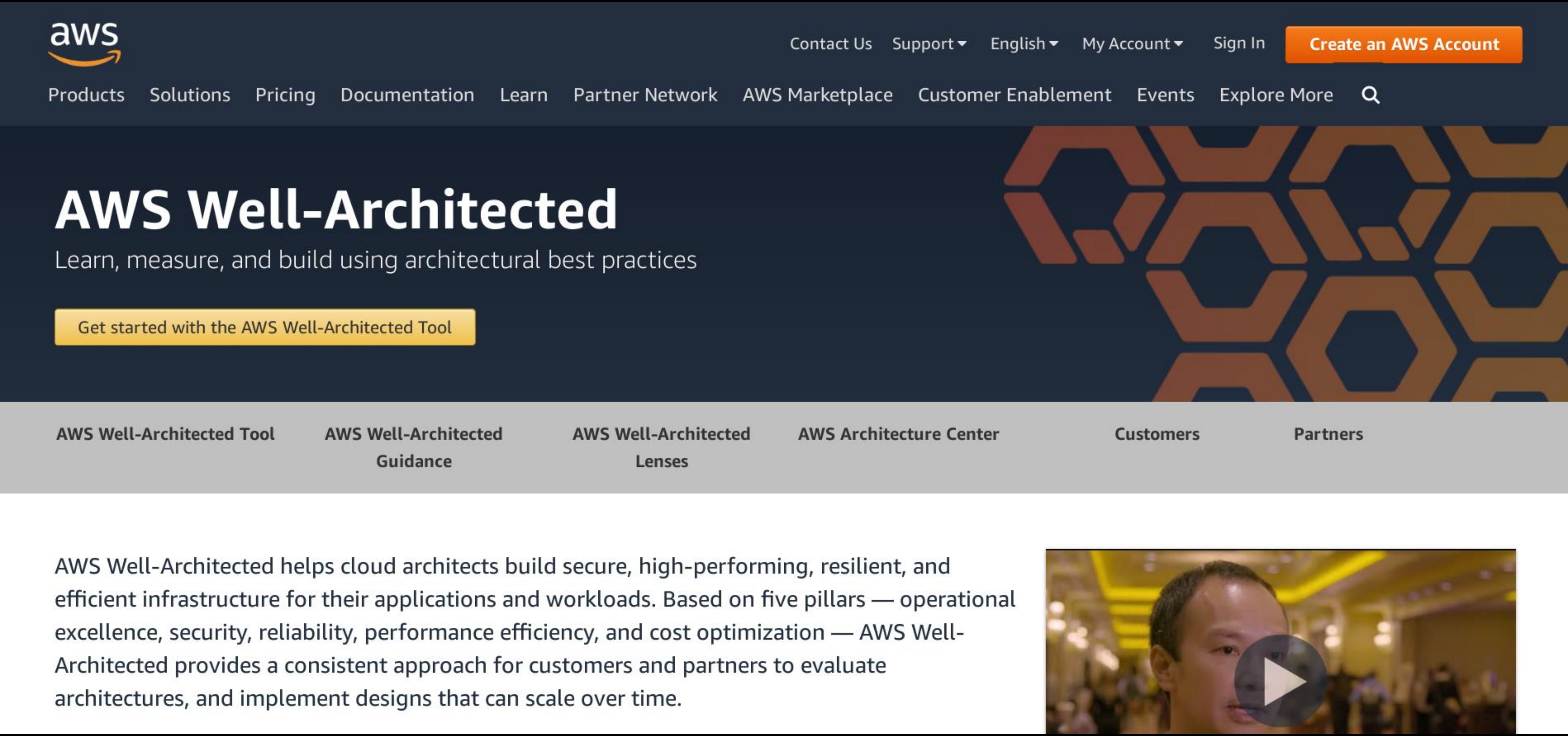
NS-1: Implement security for internal traffic

Azure ID	CIS Controls v7.1 ID(s)	NIST SP 800-53 r4 ID(s)
NS-1	9.2, 9.4, 14.1, 14.2, 14.3	AC-4, CA-3, SC-7

Ensure that all Azure virtual networks follow an enterprise segmentation principle that aligns to the business risks. Any system that could incur higher risk for the organization should be isolated within its own virtual network and sufficiently secured with either a network security group (NSG) and/or Azure Firewall.

Based on your applications and enterprise segmentation strategy, restrict or allow traffic between internal resources based on network security group rules. For specific well-defined applications (such as a 3-tier app), this can be a highly secure "deny by default, permit by exception" approach. This might not scale well if you have many applications and endpoints interacting with each other. You can also use Azure Firewall in circumstances where central management is required over a large number of enterprise segments or spokes (in a

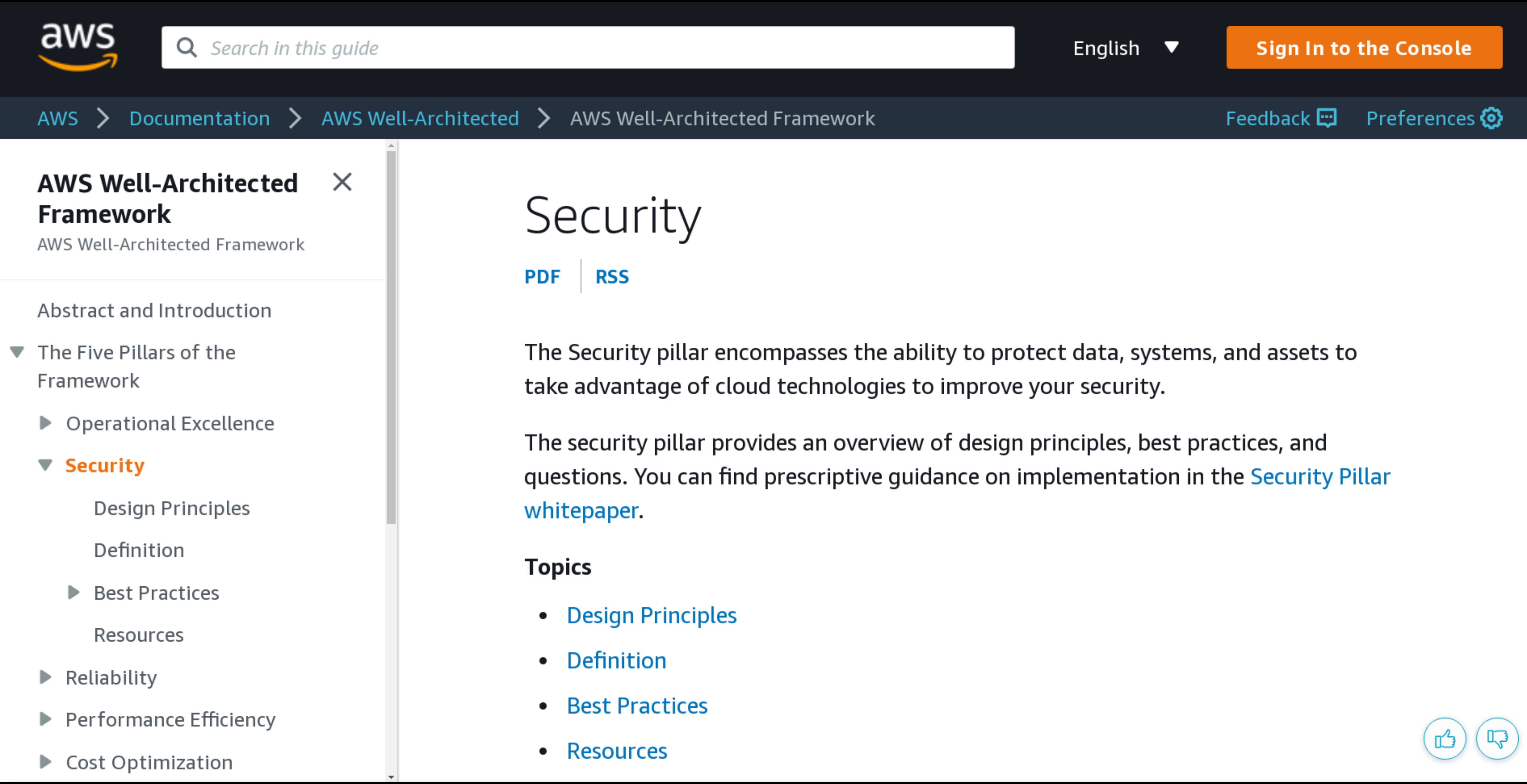
In this article



AWS Well-Architected

Learn, measure, and build using architectural best practices

AWS Well-Architected helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications and workloads. Based on five pillars — operational excellence, security, reliability, performance efficiency, and cost optimization — AWS Well-Architected provides a consistent approach for customers and partners to evaluate architectures, and implement designs that can scale over time.


aws
Search in this guide
English
Sign In to the Console
AWS > Documentation > AWS Well-Architected > AWS Well-Architected Framework
Feedback
Preferences

AWS Well-Architected Framework

AWS Well-Architected Framework

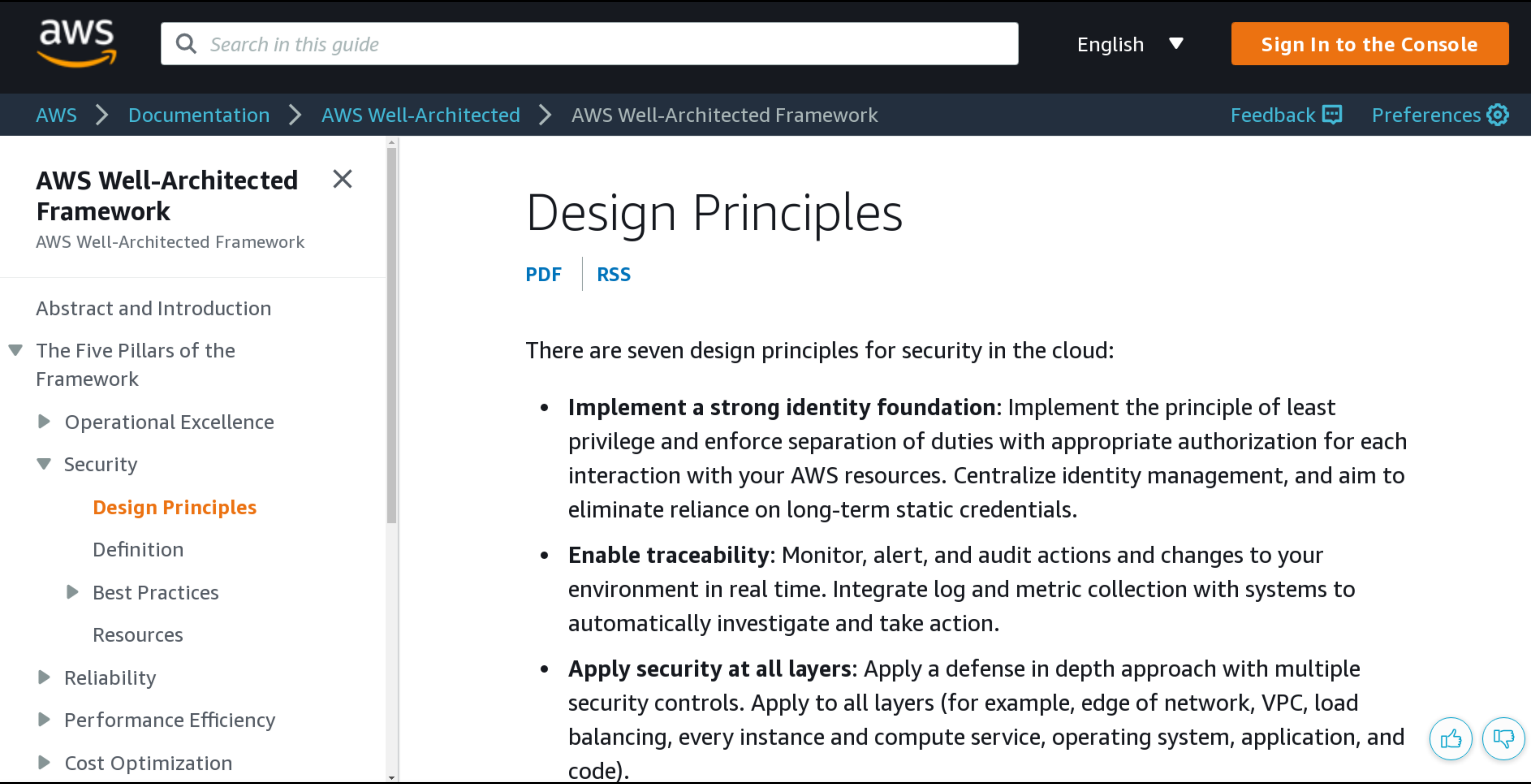
Security

The Security pillar encompasses the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security.

The security pillar provides an overview of design principles, best practices, and questions. You can find prescriptive guidance on implementation in the Security Pillar whitepaper.

Topics

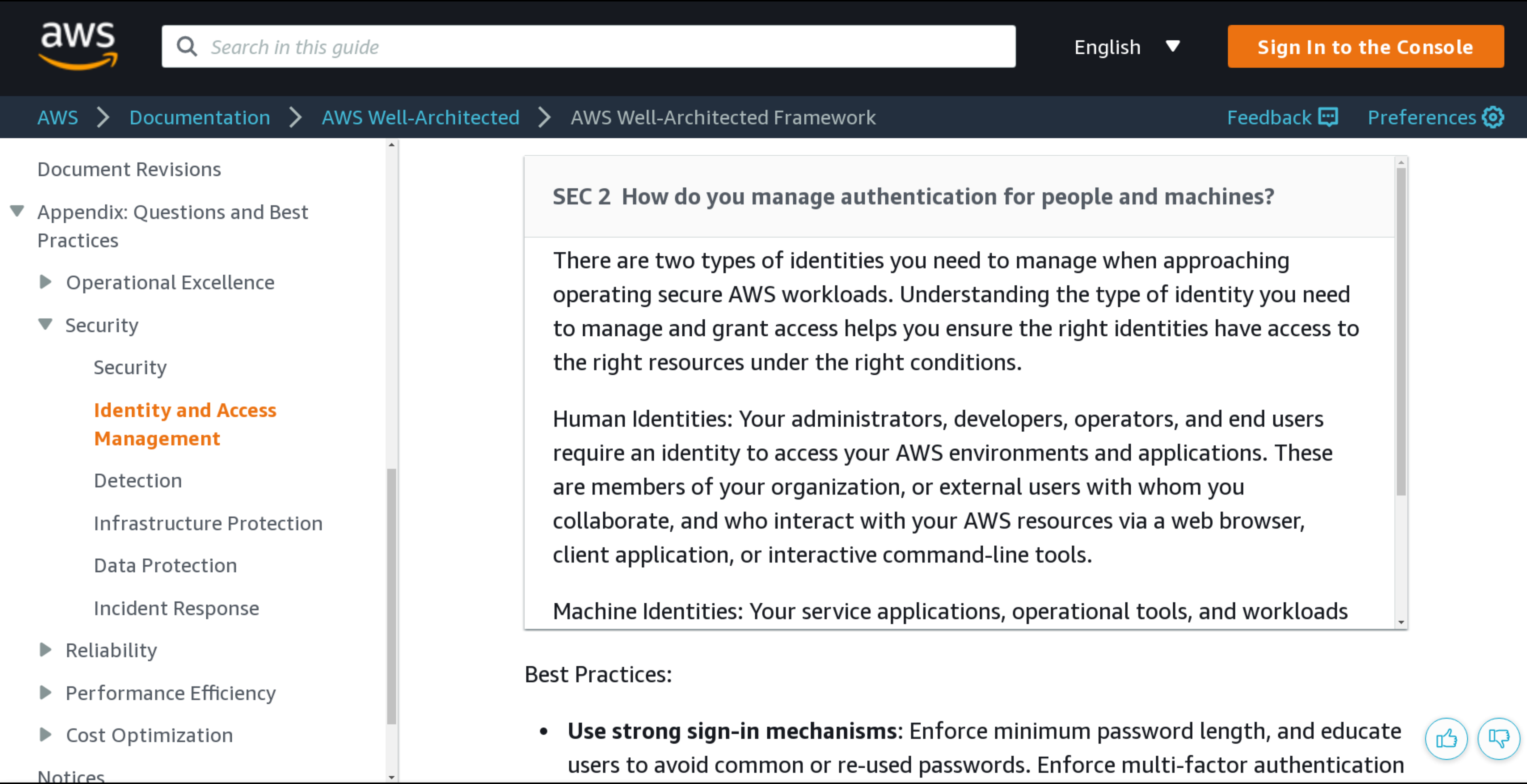
- Design Principles
- Definition
- Best Practices
- Resources



Design Principles

There are seven design principles for security in the cloud:

- **Implement a strong identity foundation**: Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources. Centralize identity management, and aim to eliminate reliance on long-term static credentials.
- **Enable traceability**: Monitor, alert, and audit actions and changes to your environment in real time. Integrate log and metric collection with systems to automatically investigate and take action.
- **Apply security at all layers**: Apply a defense in depth approach with multiple security controls. Apply to all layers (for example, edge of network, VPC, load balancing, every instance and compute service, operating system, application, and code).



SEC 2 How do you manage authentication for people and machines?

There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right conditions.

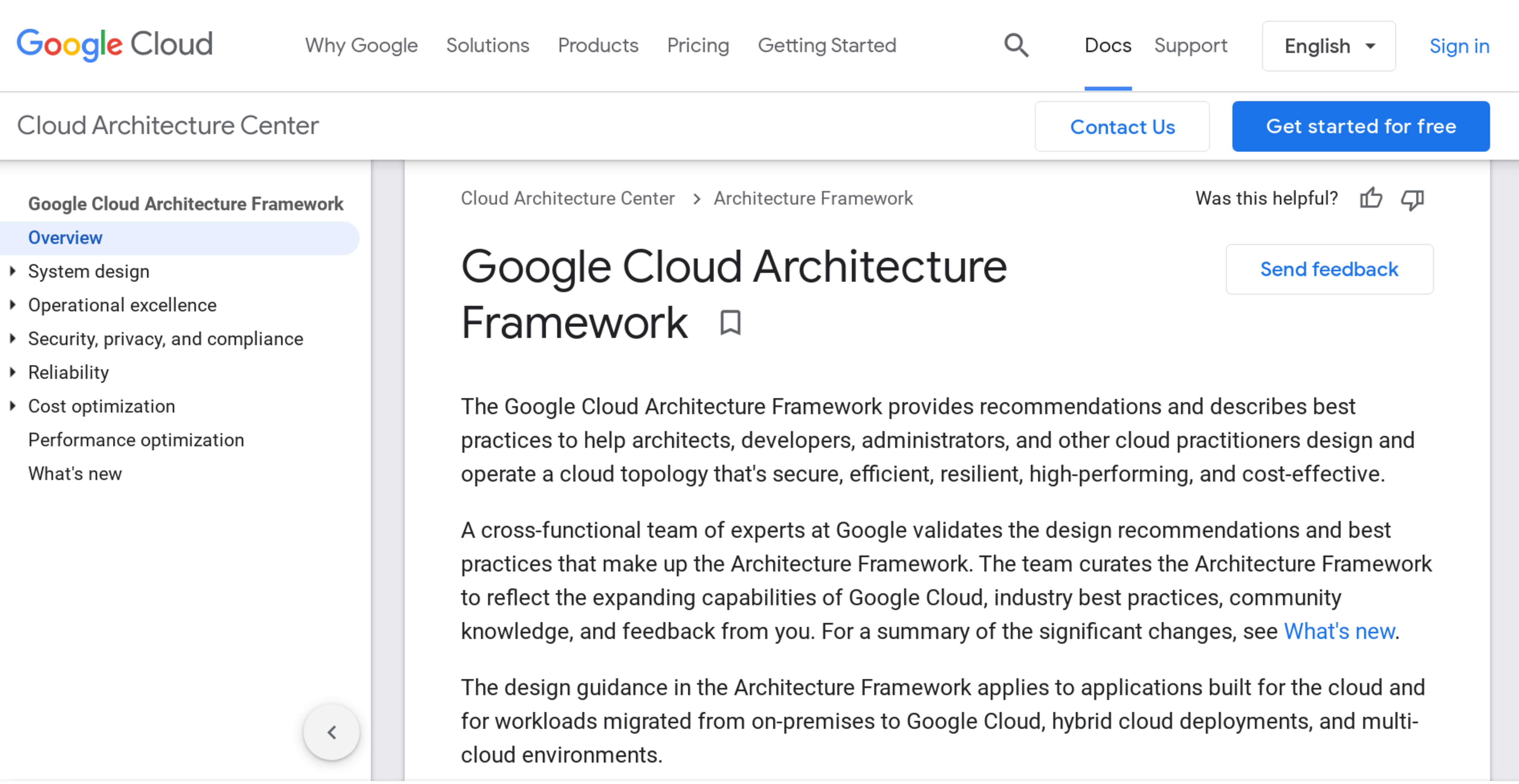
Human Identities: Your administrators, developers, operators, and end users require an identity to access your AWS environments and applications. These are members of your organization, or external users with whom you collaborate, and who interact with your AWS resources via a web browser, client application, or interactive command-line tools.

Machine Identities: Your service applications, operational tools, and workloads

Best Practices:

- **Use strong sign-in mechanisms**: Enforce minimum password length, and educate users to avoid common or re-used passwords. Enforce multi-factor authentication

Google Cloud

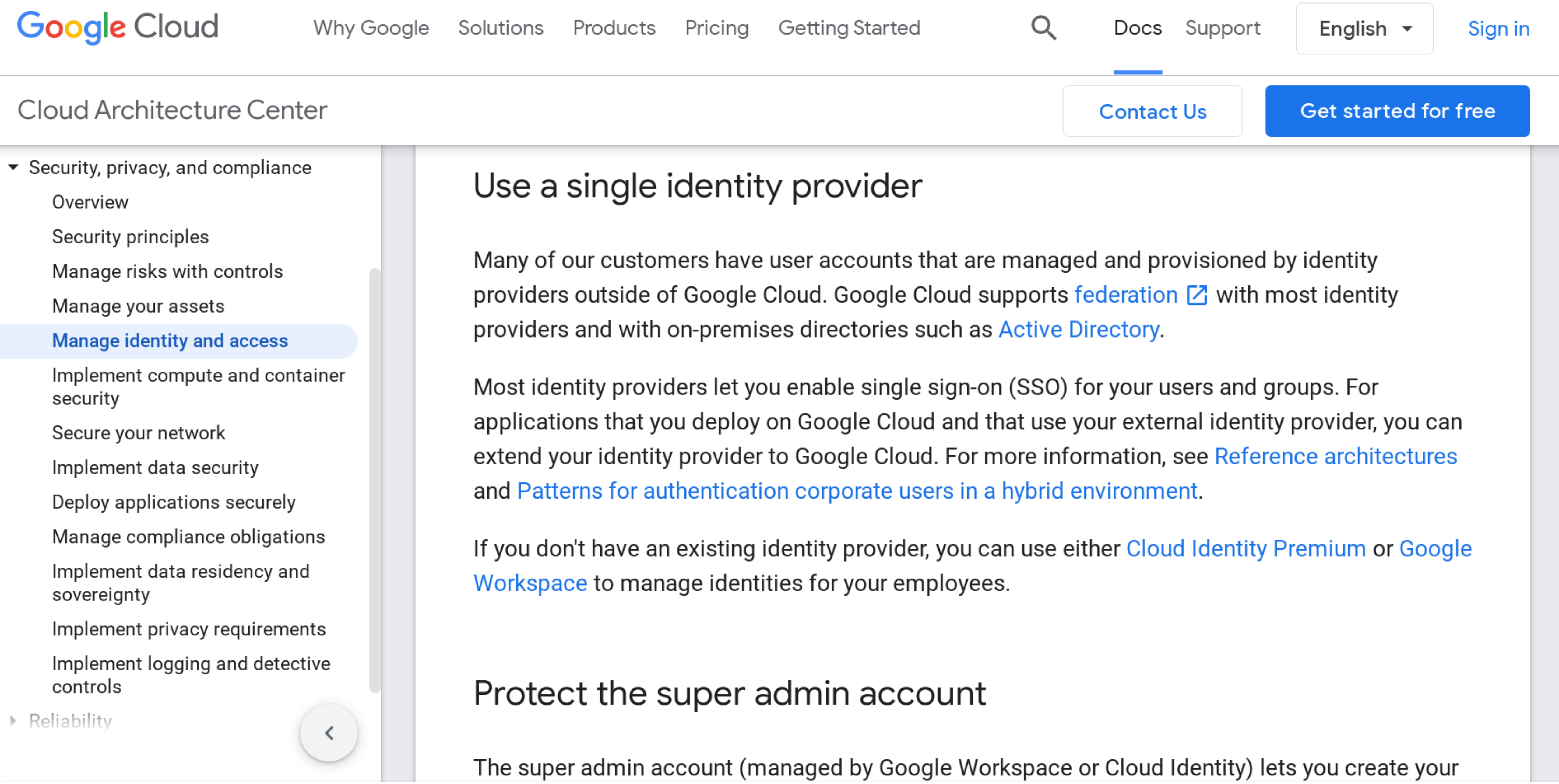


Google Cloud Architecture Framework

The Google Cloud Architecture Framework provides recommendations and describes best practices to help architects, developers, administrators, and other cloud practitioners design and operate a cloud topology that's secure, efficient, resilient, high-performing, and cost-effective.

A cross-functional team of experts at Google validates the design recommendations and best practices that make up the Architecture Framework. The team curates the Architecture Framework to reflect the expanding capabilities of Google Cloud, industry best practices, community knowledge, and feedback from you. For a summary of the significant changes, see What's new.

The design guidance in the Architecture Framework applies to applications built for the cloud and for workloads migrated from on-premises to Google Cloud, hybrid cloud deployments, and multi-cloud environments.



Security, privacy, and compliance
Overview
Security principles
Manage risks with controls
Manage your assets
Manage identity and access
Implement compute and container security
Secure your network
Implement data security
Deploy applications securely
Manage compliance obligations
Implement data residency and sovereignty
Implement privacy requirements
Implement logging and detective controls
Reliability

Use a single identity provider

Many of our customers have user accounts that are managed and provisioned by identity providers outside of Google Cloud. Google Cloud supports federation with most identity providers and with on-premises directories such as Active Directory.

Most identity providers let you enable single sign-on (SSO) for your users and groups. For applications that you deploy on Google Cloud and that use your external identity provider, you can extend your identity provider to Google Cloud. For more information, see Reference architectures and Patterns for authentication corporate users in a hybrid environment.

If you don't have an existing identity provider, you can use either Cloud Identity Premium or Google Workspace to manage identities for your employees.

Protect the super admin account

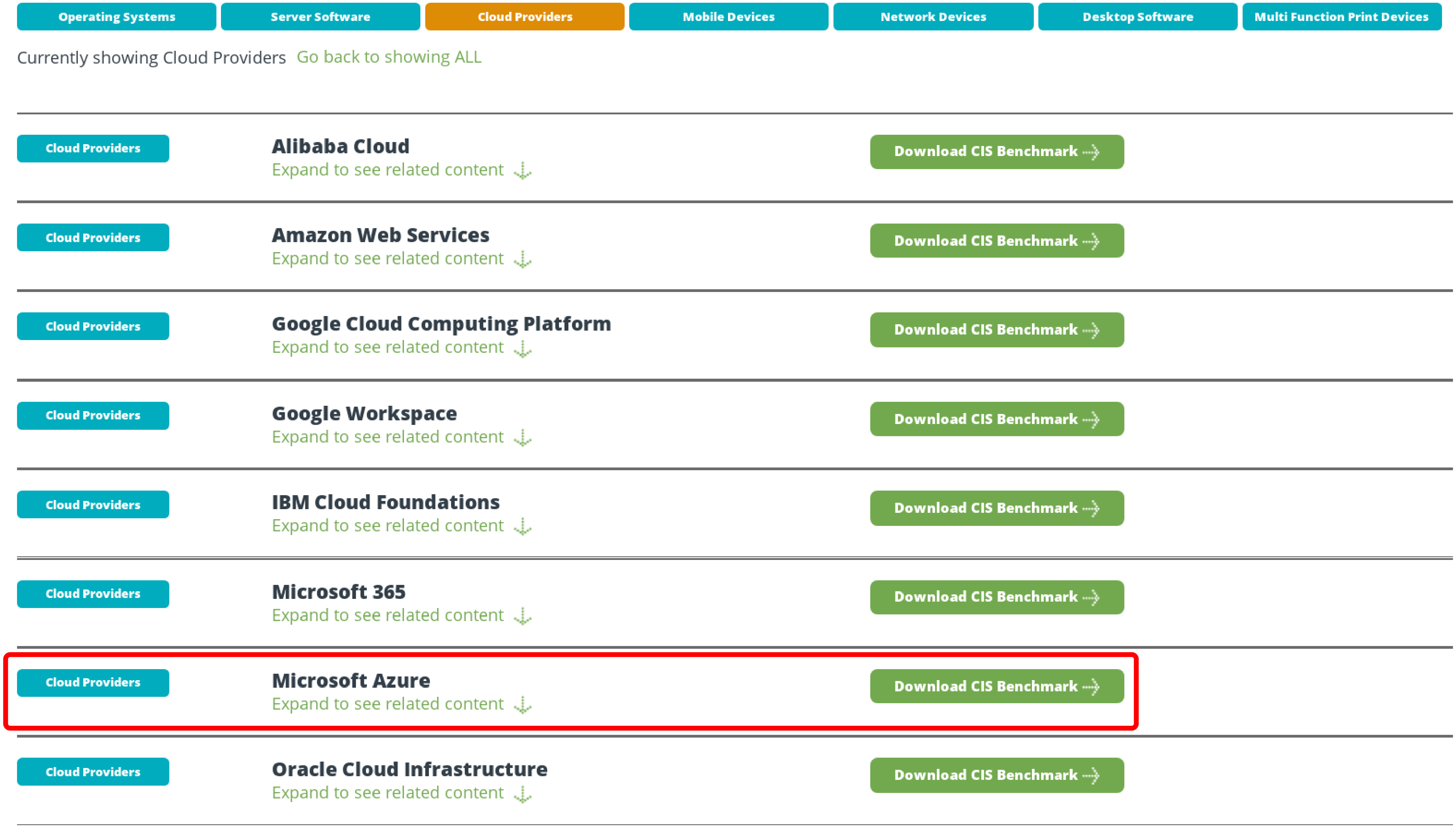
The super admin account (managed by Google Workspace or Cloud Identity) lets you create your

CIS®

Center for Internet Security®

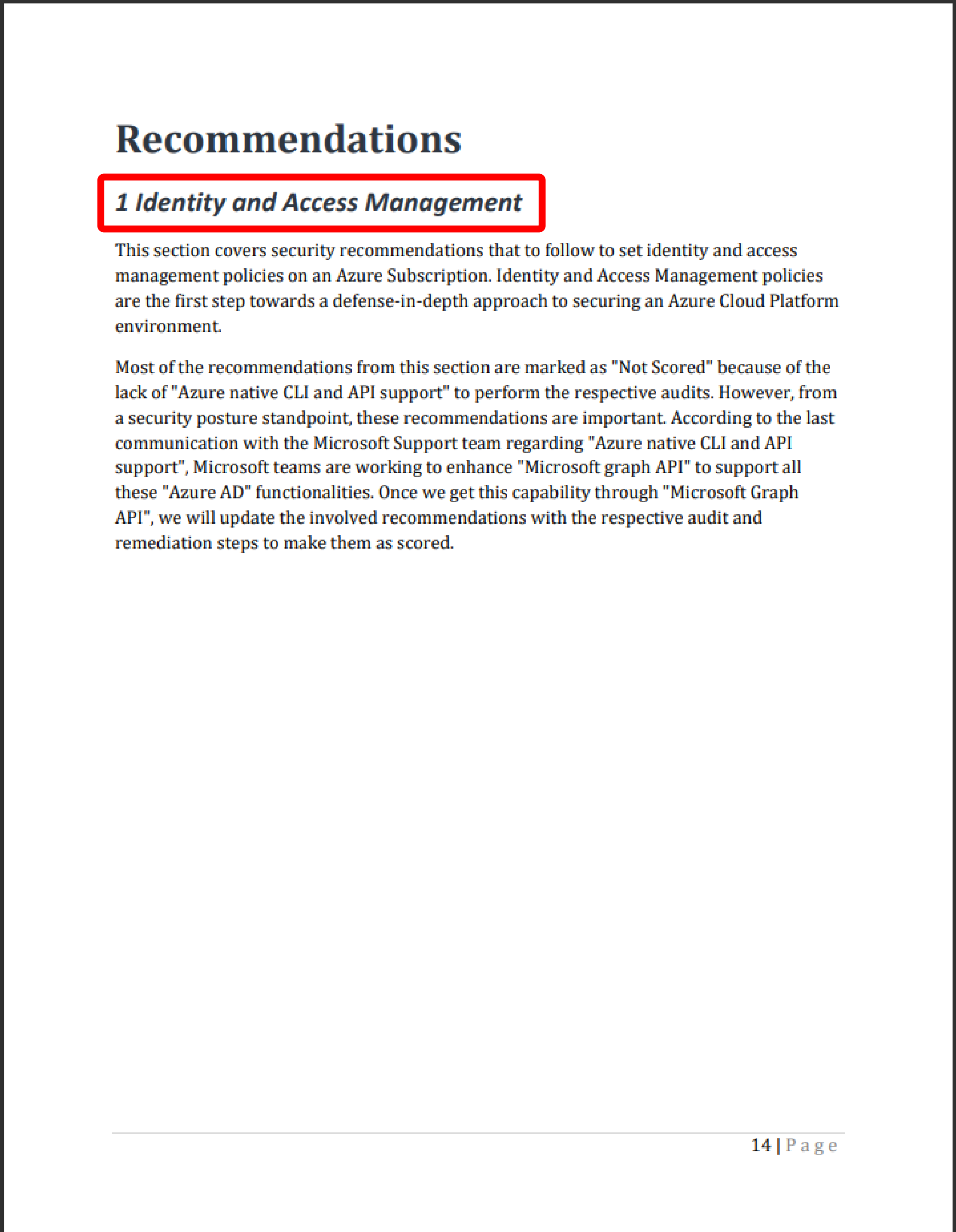
Creating Confidence in the Connected World.™

CIS Benchmarks



Currently showing Cloud Providers Go back to showing ALL

Cloud Providers	**Alibaba Cloud** Expand to see related content	Download CIS Benchmark
Cloud Providers	**Amazon Web Services** Expand to see related content	Download CIS Benchmark
Cloud Providers	**Google Cloud Computing Platform** Expand to see related content	Download CIS Benchmark
Cloud Providers	**Google Workspace** Expand to see related content	Download CIS Benchmark
Cloud Providers	**IBM Cloud Foundations** Expand to see related content	Download CIS Benchmark
Cloud Providers	**Microsoft 365** Expand to see related content	Download CIS Benchmark
Cloud Providers	**Microsoft Azure** Expand to see related content	Download CIS Benchmark
Cloud Providers	**Oracle Cloud Infrastructure** Expand to see related content	Download CIS Benchmark

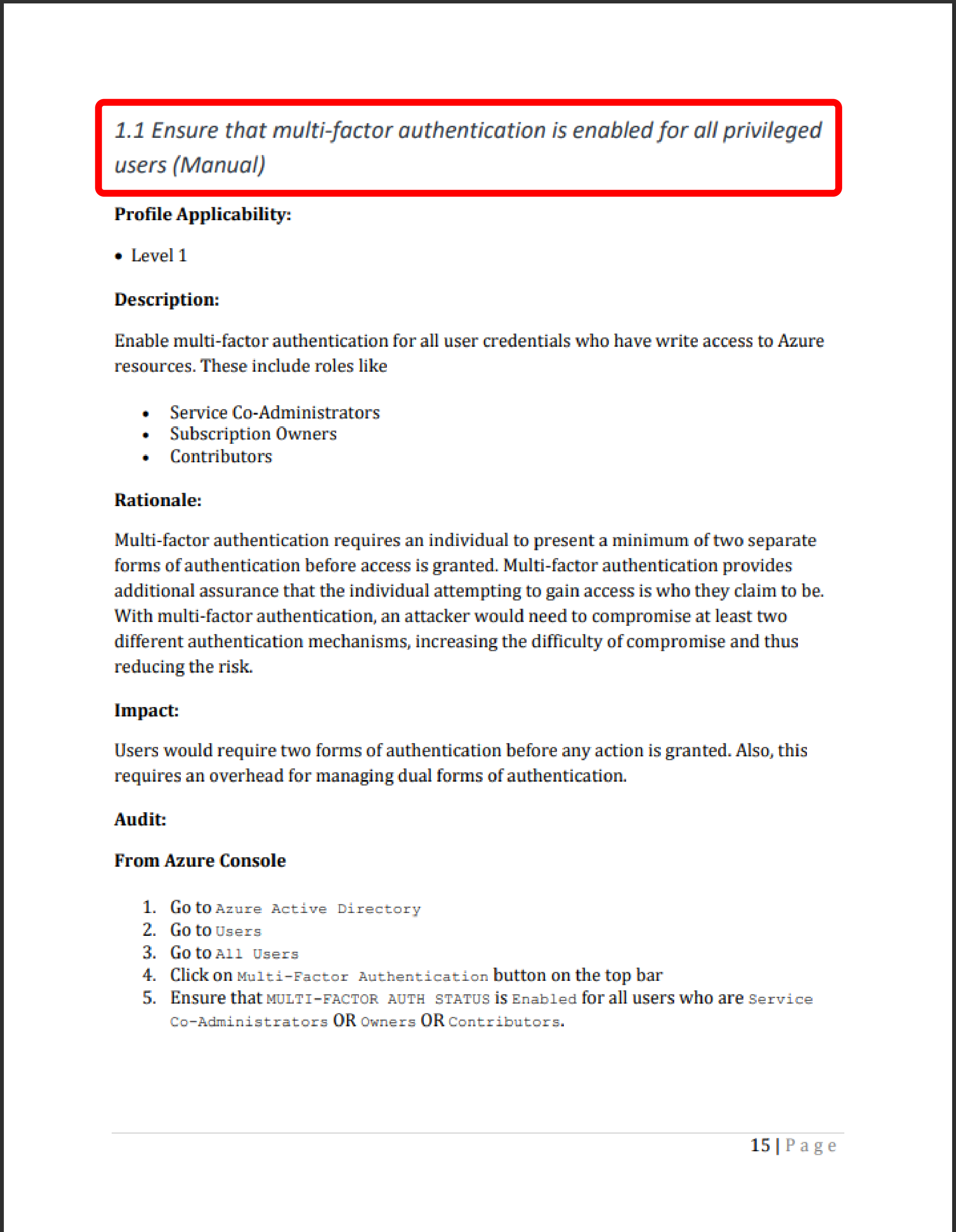


Recommendations

1 Identity and Access Management

This section covers security recommendations that to follow to set identity and access management policies on an Azure Subscription. Identity and Access Management policies are the first step towards a defense-in-depth approach to securing an Azure Cloud Platform environment.

Most of the recommendations from this section are marked as "Not Scored" because of the lack of "Azure native CLI and API support" to perform the respective audits. However, from a security posture standpoint, these recommendations are important. According to the last communication with the Microsoft Support team regarding "Azure native CLI and API support", Microsoft teams are working to enhance "Microsoft graph API" to support all these "Azure AD" functionalities. Once we get this capability through "Microsoft Graph API", we will update the involved recommendations with the respective audit and remediation steps to make them as scored.



1.1 Ensure that multi-factor authentication is enabled for all privileged users (Manual)

Profile Applicability:

- Level 1

Description:

Enable multi-factor authentication for all user credentials who have write access to Azure resources. These include roles like

- Service Co-Administrators
- Subscription Owners
- Contributors

Rationale:

Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

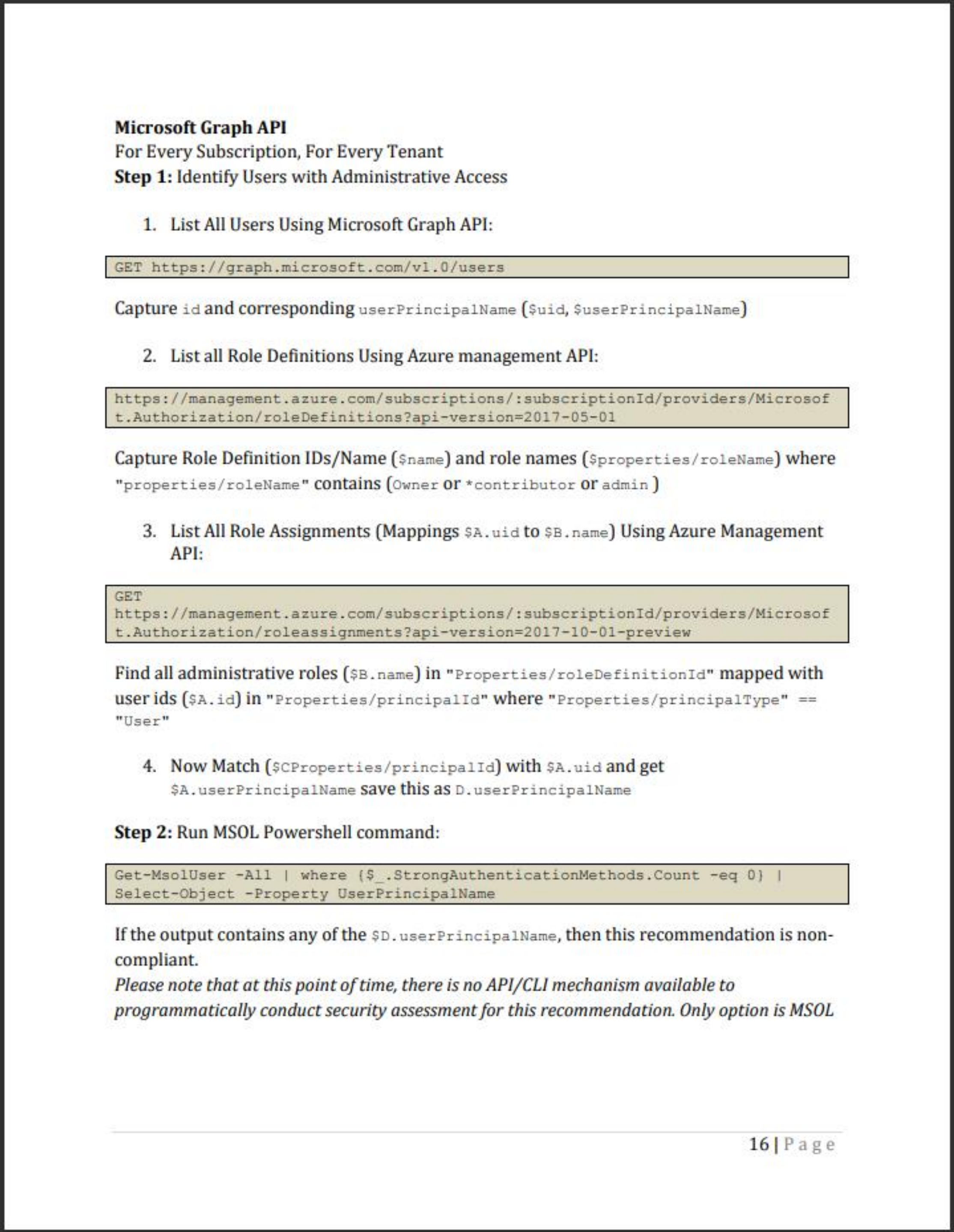
Impact:

Users would require two forms of authentication before any action is granted. Also, this requires an overhead for managing dual forms of authentication.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `All Users`
4. Click on `Multi-Factor Authentication` button on the top bar
5. Ensure that `MULTI-FACTOR AUTH STATUS` is `Enabled` for all users who are `Service Co-Administrators` OR `Owners` OR `Contributors`.



Microsoft Graph API
For Every Subscription, For Every Tenant
Step 1: Identify Users with Administrative Access

1. List All Users Using Microsoft Graph API:

```
GET https://graph.microsoft.com/v1.0/users
```

Capture `id` and corresponding `userPrincipalName` (`$uid`, `$userPrincipalName`)

2. List all Role Definitions Using Azure management API:

```
https://management.azure.com/subscriptions/:subscriptionId/providers/Microsof
t.Authorization/roleDefinitions?api-version=2017-05-01
```

Capture Role Definition IDs/Name (`$name`) and role names (`$properties/roleName`) where `"properties/roleName"` contains (`Owner` or `*contributor` or `admin`)

3. List All Role Assignments (Mappings `$A.uid` to `$B.name`) Using Azure Management API:

```
GET
https://management.azure.com/subscriptions/:subscriptionId/providers/Microsof
t.Authorization/roleassignments?api-version=2017-10-01-preview
```

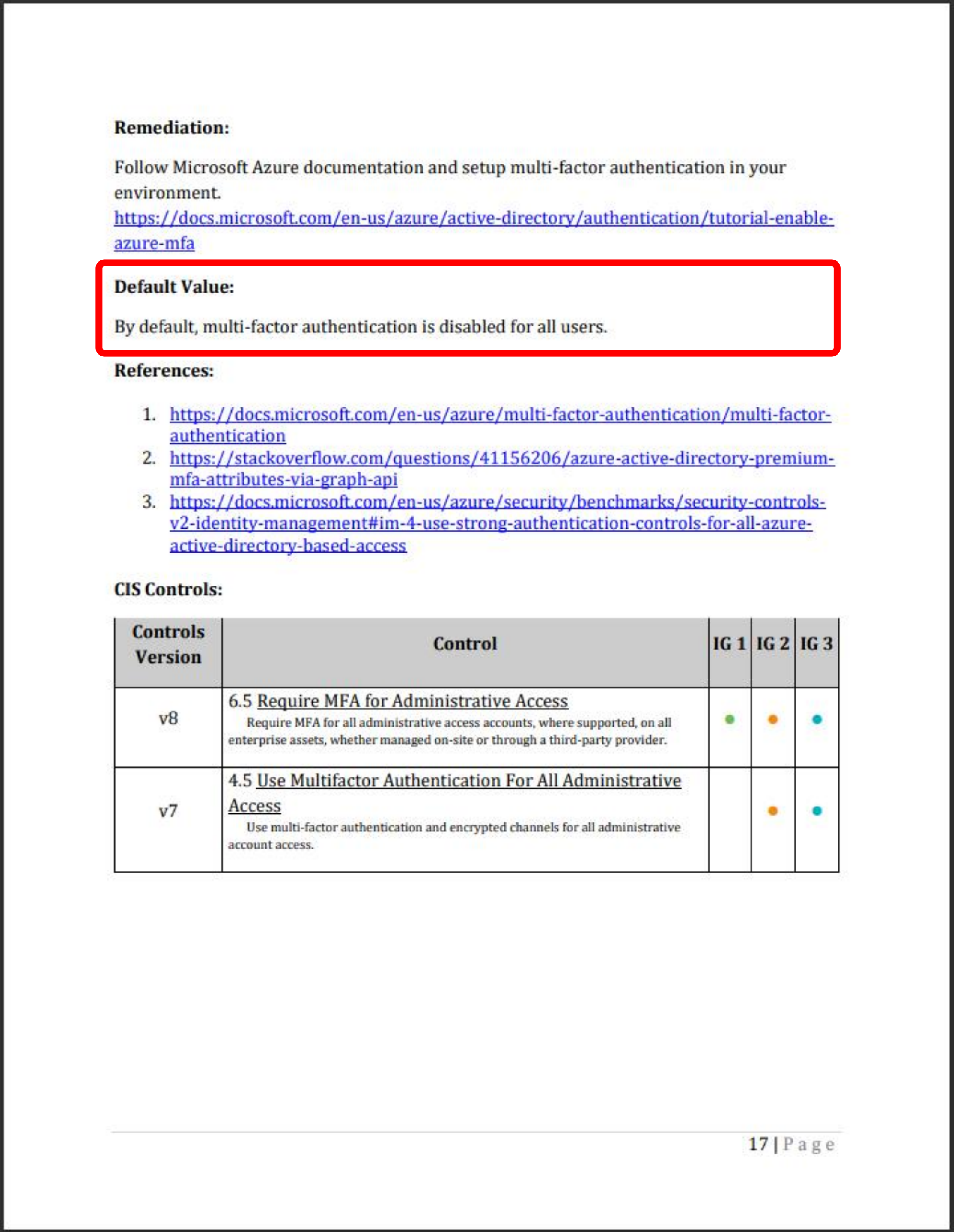
Find all administrative roles (`$B.name`) in `"Properties/roleDefinitionId"` mapped with user ids (`$A.id`) in `"Properties/principalId"` where `"Properties/principalType" == "User"`

4. Now Match (`$CProperties/principalId`) with `$A.uid` and get `$A.userPrincipalName` save this as `D.userPrincipalName`

Step 2: Run MSOL Powershell command:

```
Get-MsolUser -All | where {$_.StrongAuthenticationMethods.Count -eq 0} |
Select-Object -Property UserPrincipalName
```

If the output contains any of the `$D.userPrincipalName`, then this recommendation is non-compliant.
Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation. Only option is MSOL



Remediation:

Follow Microsoft Azure documentation and setup multi-factor authentication in your environment.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

Default Value:

By default, multi-factor authentication is disabled for all users.

References:

1. https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication
2. https://stackoverflow.com/questions/41156206/azure-active-directory-premium-mfa-attributes-via-graph-api
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

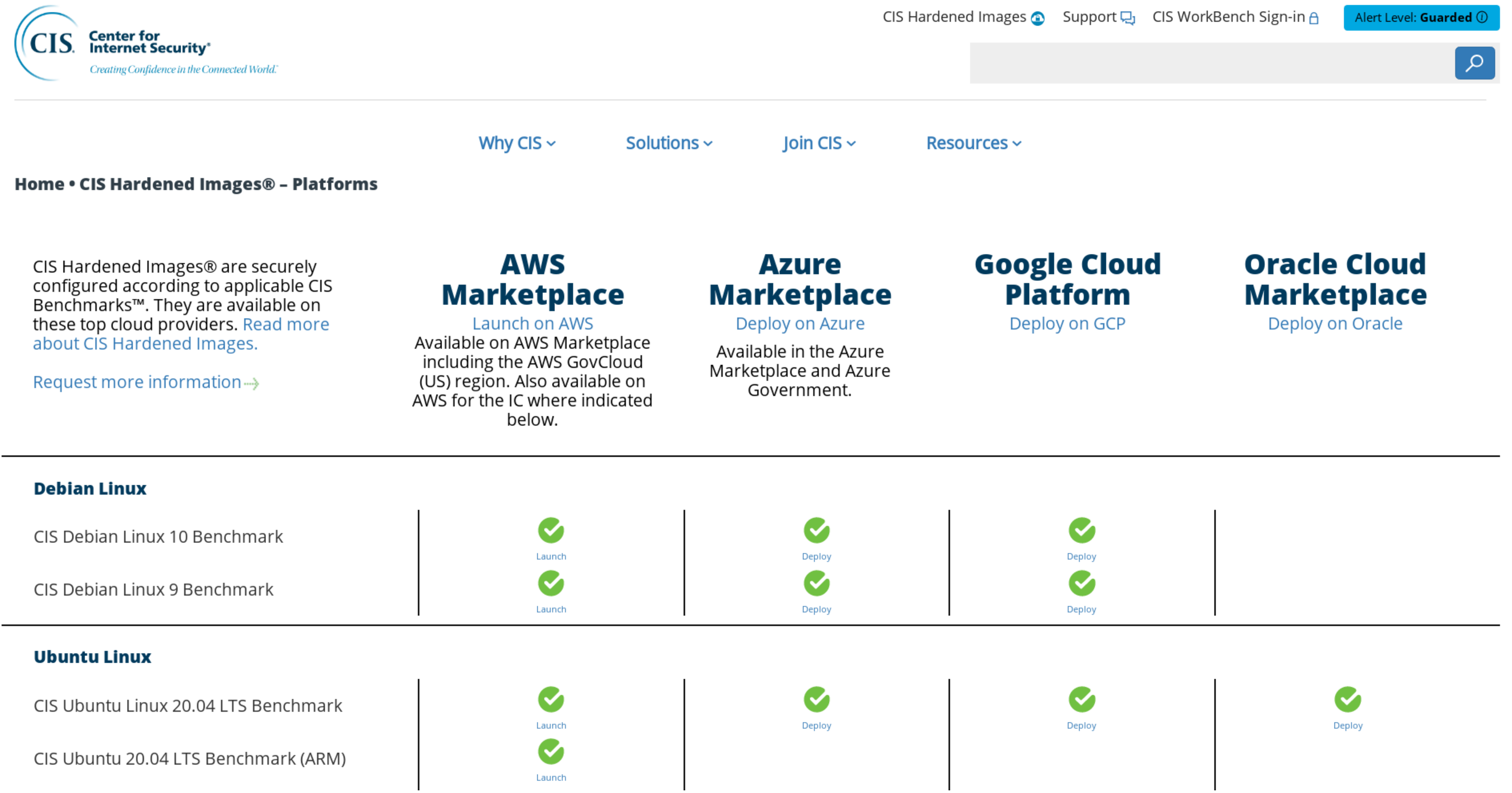
CIS Cloud Controls

CIS Controls Cloud Companion Guide

Download

In this document, we provide guidance on how to apply the security best practices found in CIS Controls Version 7 to any cloud environment from the consumer/customer perspective. For each top-level CIS Control, there is a brief discussion of how to interpret and apply the CIS Control in such environments, along with any unique considerations or differences from common IT environments.

CIS Hardened Images



CIS Center for Internet Security®
Creating Confidence in the Connected World.®

CIS Hardened Images Support CIS WorkBench Sign-in Alert Level: **Guarded**

Why CIS Solutions Join CIS Resources

Home • CIS Hardened Images® – Platforms

CIS Hardened Images® are securely configured according to applicable CIS Benchmarks™. They are available on these top cloud providers. Read more about CIS Hardened Images.

Request more information

AWS Marketplace

Launch on AWS

Available on AWS Marketplace including the AWS GovCloud (US) region. Also available on AWS for the IC where indicated below.

Azure Marketplace

Deploy on Azure

Available in the Azure Marketplace and Azure Government.

Google Cloud Platform

Deploy on GCP

Oracle Cloud Marketplace

Deploy on Oracle

Debian Linux

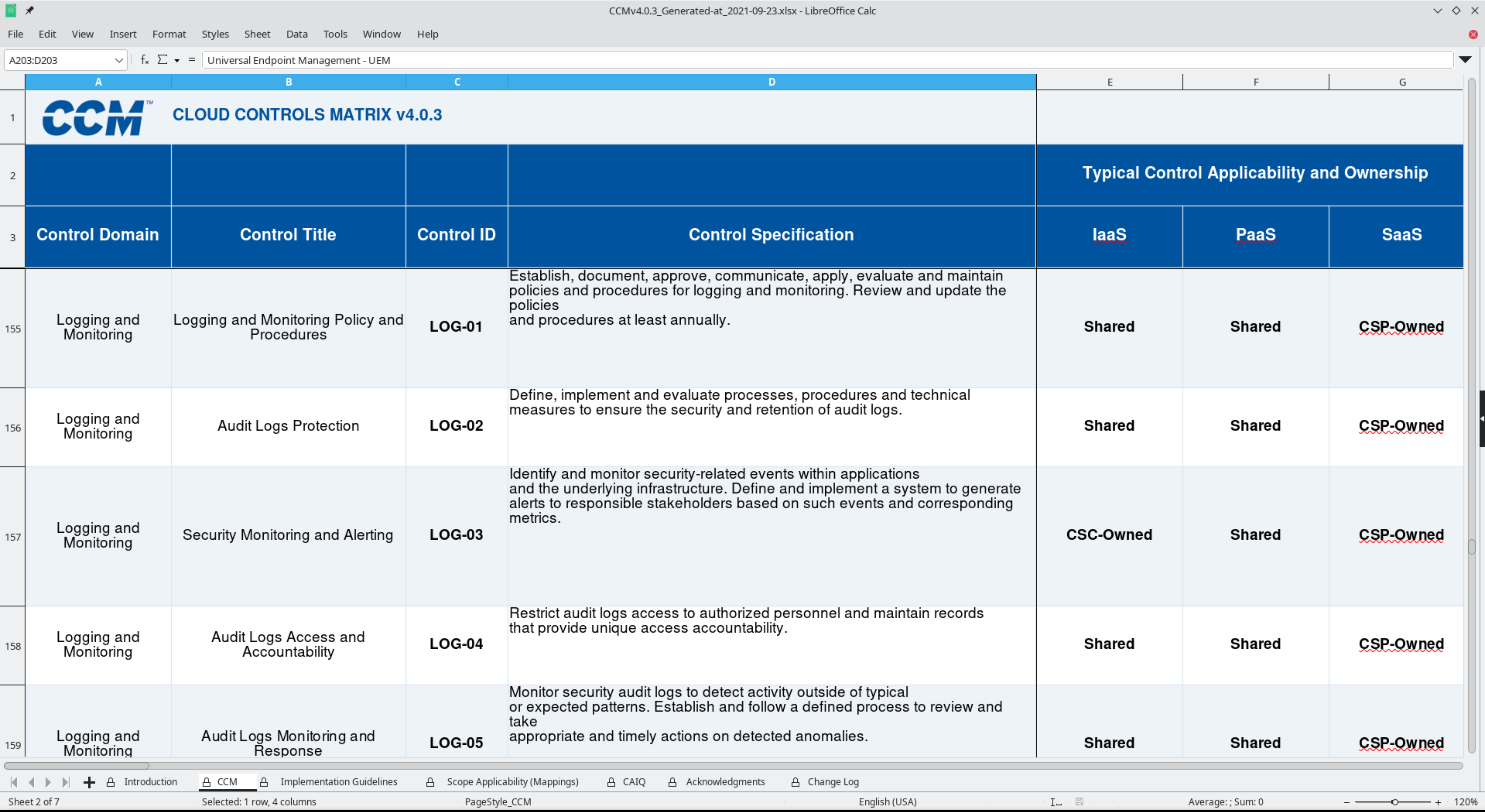
	AWS Marketplace	Azure Marketplace	Google Cloud Platform	Oracle Cloud Marketplace
CIS Debian Linux 10 Benchmark	✓ Launch	✓ Deploy	✓ Deploy	
CIS Debian Linux 9 Benchmark	✓ Launch	✓ Deploy	✓ Deploy	

Ubuntu Linux

	AWS Marketplace	Azure Marketplace	Google Cloud Platform	Oracle Cloud Marketplace
CIS Ubuntu Linux 20.04 LTS Benchmark	✓ Launch	✓ Deploy	✓ Deploy	✓ Deploy
CIS Ubuntu 20.04 LTS Benchmark (ARM)	✓ Launch			

CSA cloud security alliance®

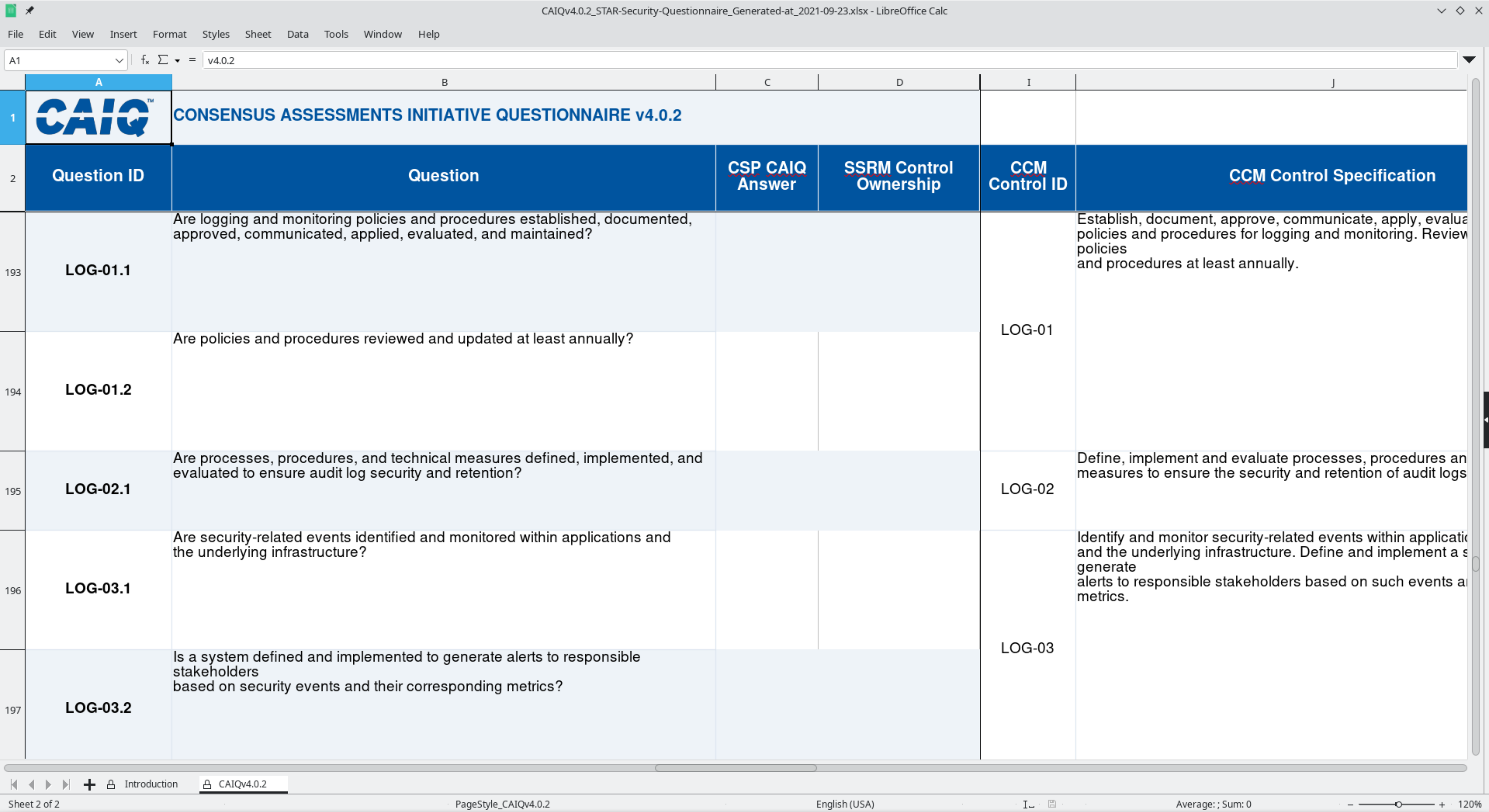
CSA Cloud Controls Matrix (CCM)


CCMv4.0.3_Generated-at_2021-09-23.xlsx - LibreOffice Calc
File
Edit
View
Insert
Format
Styles
Sheet
Data
Tools
Window
Help
A203:D203
Universal Endpoint Management - UEM
Introduction
CCM
Implementation Guidelines
Scope Applicability (Mappings)
CAIQ
Acknowledgments
Change Log
Sheet 2 of 7
Selected: 1 row, 4 columns
PageStyle_CCM
English (USA)
Average: ; Sum: 0
120%

CCM™ CLOUD CONTROLS MATRIX v4.0.3

Control Domain	Control Title	Control ID	Control Specification	Typical Control Applicability and Ownership		
				IaaS	PaaS	SaaS
Logging and Monitoring	Logging and Monitoring Policy and Procedures	LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Shared	Shared	CSP-Owned
Logging and Monitoring	Audit Logs Protection	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Shared	Shared	CSP-Owned
Logging and Monitoring	Security Monitoring and Alerting	LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	CSC-Owned	Shared	CSP-Owned
Logging and Monitoring	Audit Logs Access and Accountability	LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Shared	Shared	CSP-Owned
Logging and Monitoring	Audit Logs Monitoring and Response	LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Shared	Shared	CSP-Owned

CSA Consensus Assessment Initiative Questionnaire (CAIQ)



CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CCM Control ID	CCM Control Specification
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?			LOG-01	Establish, document, approve, communicate, apply, evalua policies and procedures for logging and monitoring. Review policies and procedures at least annually.
LOG-01.2	Are policies and procedures reviewed and updated at least annually?				
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?			LOG-02	Define, implement and evaluate processes, procedures an measures to ensure the security and retention of audit logs
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?			LOG-03	Identify and monitor security-related events within applicatio and the underlying infrastructure. Define and implement a s generate alerts to responsible stakeholders based on such events a metrics.
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?				

step four

Remediate & Repeat

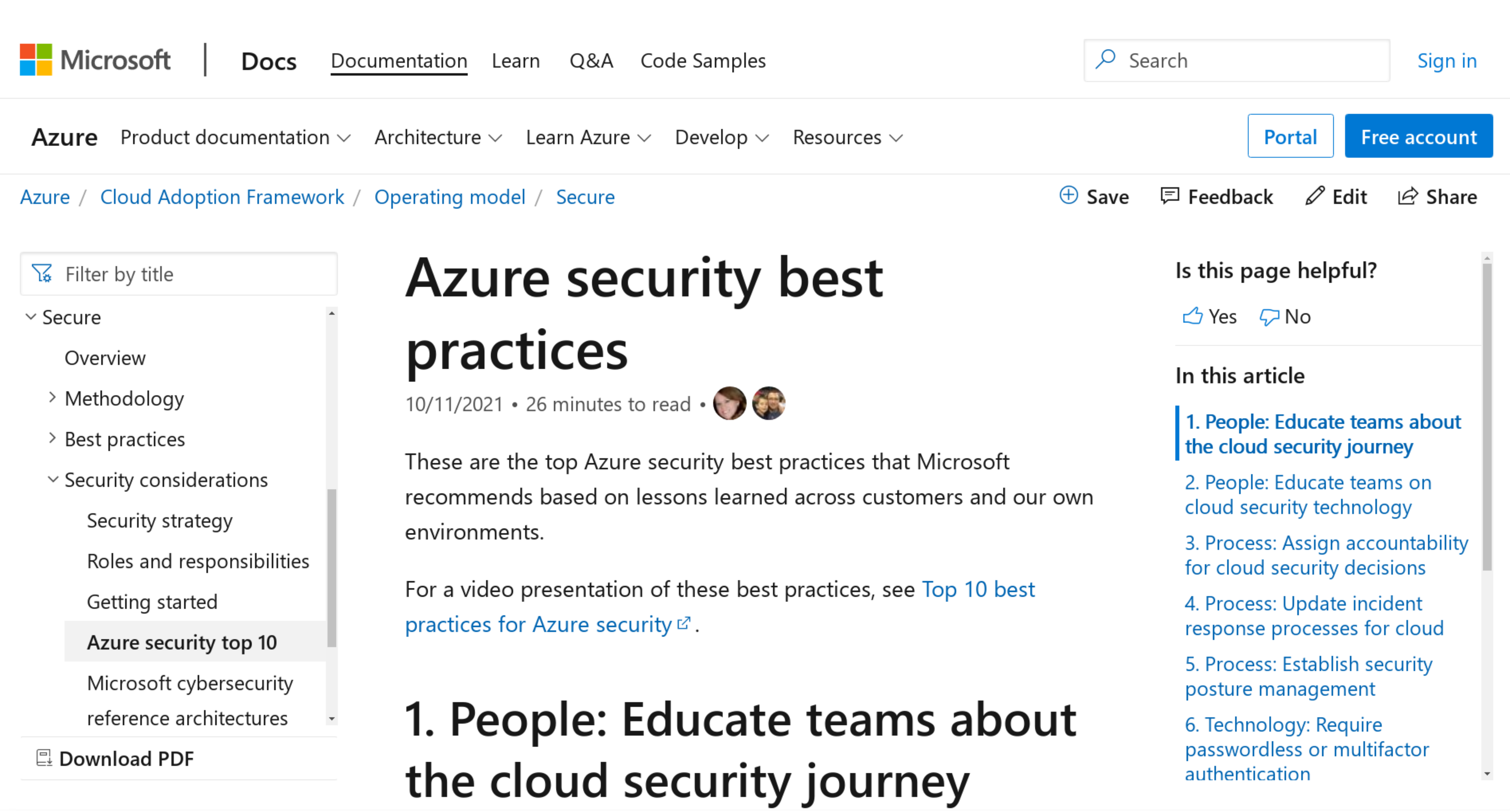
Best Practices

> “Security is not rocket science
> – Security is common sense!
>
> — Pete Finnigan

1. Enable multi-factor authentication
2. Follow the principle of least privilege
3. Separate development and production environments
4. Segment your network
5. Minimize the attack surface
6. Do not store application secrets in source code
7. Encrypt data at rest and in transit
8. Use a web application firewall (WAF)
9. Enable logging and monitor your logs
10. Make use of security tools provided by the CSP

What I didn‘t tell you...

- Security starts before your move to the cloud has begun
- A configuration review won‘t detect missing education practices
- A configuration review won‘t prevent vendor lock-in
- A configuration review won‘t provide business continuity and disaster recovery plans
- Not every reviewer will have knowledge about data protection laws / regulations with location-specific requirements



Microsoft | Docs Documentation Learn Q&A Code Samples Search Sign in

Azure Product documentation Architecture Learn Azure Develop Resources Portal Free account

Azure / Cloud Adoption Framework / Operating model / Secure Save Feedback Edit Share

Filter by title

- Secure
  - Overview
  - Methodology
  - Best practices
  - Security considerations
    - Security strategy
    - Roles and responsibilities
    - Getting started
    - Azure security top 10
    - Microsoft cybersecurity reference architectures

Download PDF

Azure security best practices

10/11/2021 • 26 minutes to read •

These are the top Azure security best practices that Microsoft recommends based on lessons learned across customers and our own environments.

For a video presentation of these best practices, see Top 10 best practices for Azure security.

1. People: Educate teams about the cloud security journey

Is this page helpful?

Yes No

In this article

1. People: Educate teams about the cloud security journey
2. People: Educate teams on cloud security technology
3. Process: Assign accountability for cloud security decisions
4. Process: Update incident response processes for cloud
5. Process: Establish security posture management
6. Technology: Require passwordless or multifactor authentication

Google Cloud security best practices center

- Best practices guides
- Deployable security blueprints and landing zones
- Security whitepapers and references
- Learning resources

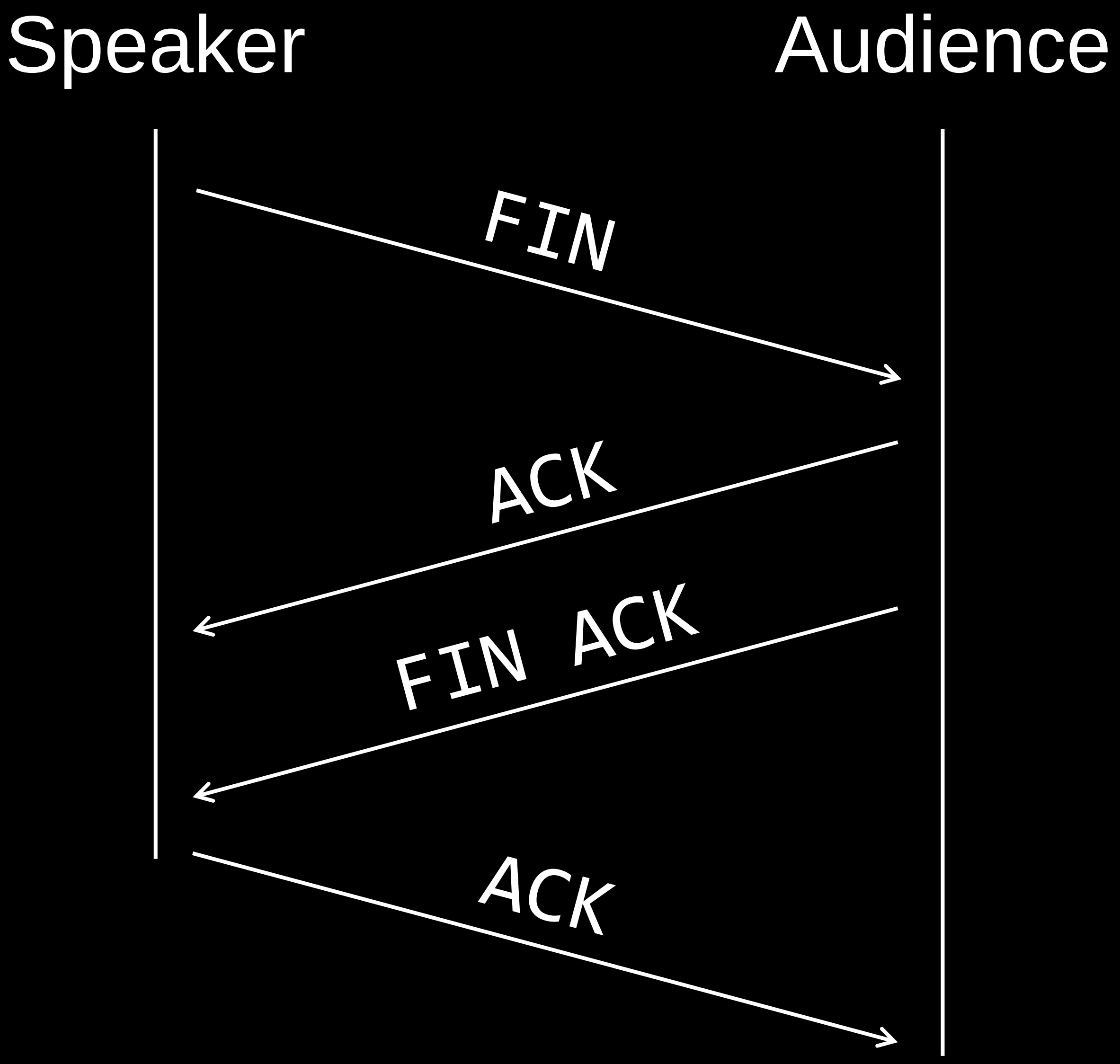
Google Cloud security best practices center

Explore these best practices for meeting your security and compliance objectives as you deploy workloads on Google Cloud.

Contact us

Best practices guides

Best practices guides provide specific, informed guidance on helping secure Google Cloud deployments and describe recommended configurations, architectures, suggested settings, and other operational



Speaker

Audience

FIN

ACK

FIN ACK

ACK