# Cloud Audit and Assurance

**Dr. Lyron H. Andrews**

CISSP/CCSP/SSCP/CRISC/CISM/CCSK

https://www.profabula.com/whyprofabula

# Overview

Enumerate elements of attestations and certifications

Integrate audit of controls specific to cloud adaptation

Review published audit results of a CSP

# Provider Trust Then and Now

Past

**The client maintained a direct path of trust**

Present

**Pass-though trust through audit**

# Pass-through Trust from Audit

Top tier providers trust top tier audit firms

Audit firm maintains residence at client

Audit firm follows industry standards to maintain trust

# Primary Assurance and Trust Practices

**Attestation**

**Certification**

# Attestation for Technical and Financial Reporting Controls

# Service Organization Control Reports

SOC1-Financial

SOC2-Technical

SOC3-Summary

Consumer focus

Annual calendar

# SOC 1

Financial statements

ICOFR

Type I

Type II

# SOC 2

Trust Services Principles

Broad range of needs

Type I

Type II

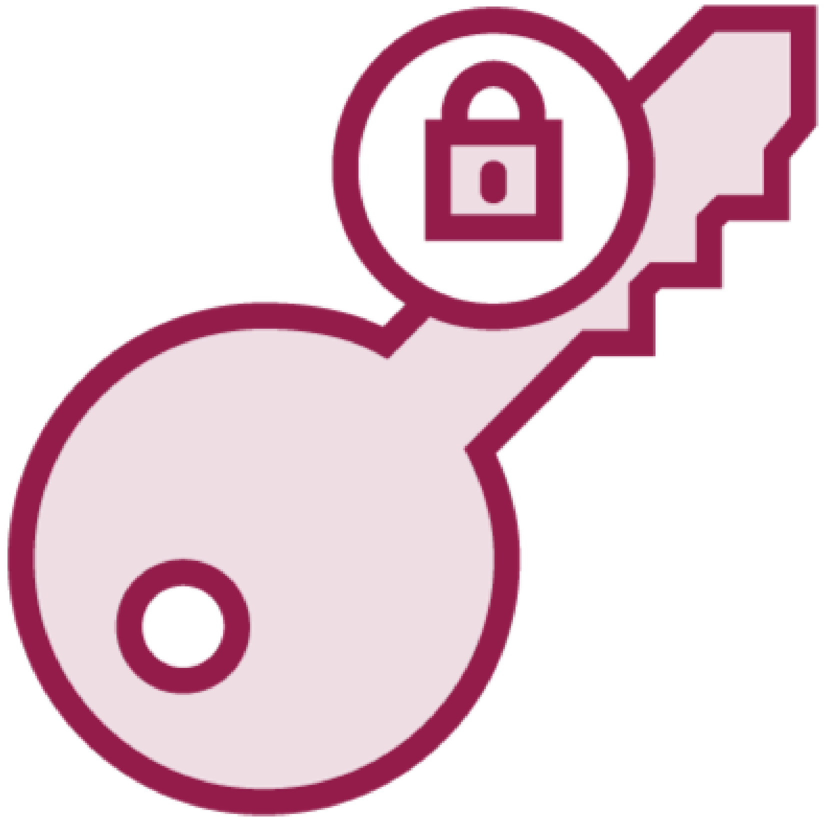
# SOC 3

Summary of SOC2

Auditor's opinion

Significant assurance

# SOC for Cybersecurity



Entity-wide assessment of cybersecurity

Holistic reporting framework

Tools to evaluate control effectiveness

# Certification for Information Security Management System (ISMS)

# ISMS Certification from ISO/IEC 27001:2013

SOC is for attestation
ISO/IEC 27001 is for certification

ISO/IEC 27001 designed for ISMS certification

Structured and measurable approach to risk

Top-down sponsorship imperative

# ISO/IEC 27001 Domains

Information Security Policies

Organization of Information Security

Human Resource Security

Asset Management

Access Control

Cryptography

Physical and Environmental Security

# ISO/IEC 27001 Domains

- Operations Security
- Communications Security
- System Acquisition, Development, and Maintenance
- Supplier Relationships
- Incident Management
- Business Continuity Management
- Compliance

# Code of Practice ISO/IEC 27002:2013

Guidelines for implementation

Works in concert with 27001

Lists control objectives

# Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds
# ISO/IEC 27018:2019

**Consent**

**Control**

**Transparency**

**Communication**

**Independent annual audit**

# Cloud Guidelines ISO/IEC 27017:2015

**Role delineation**

**Asset disposition**

**Customer isolation**

**VM configuration**

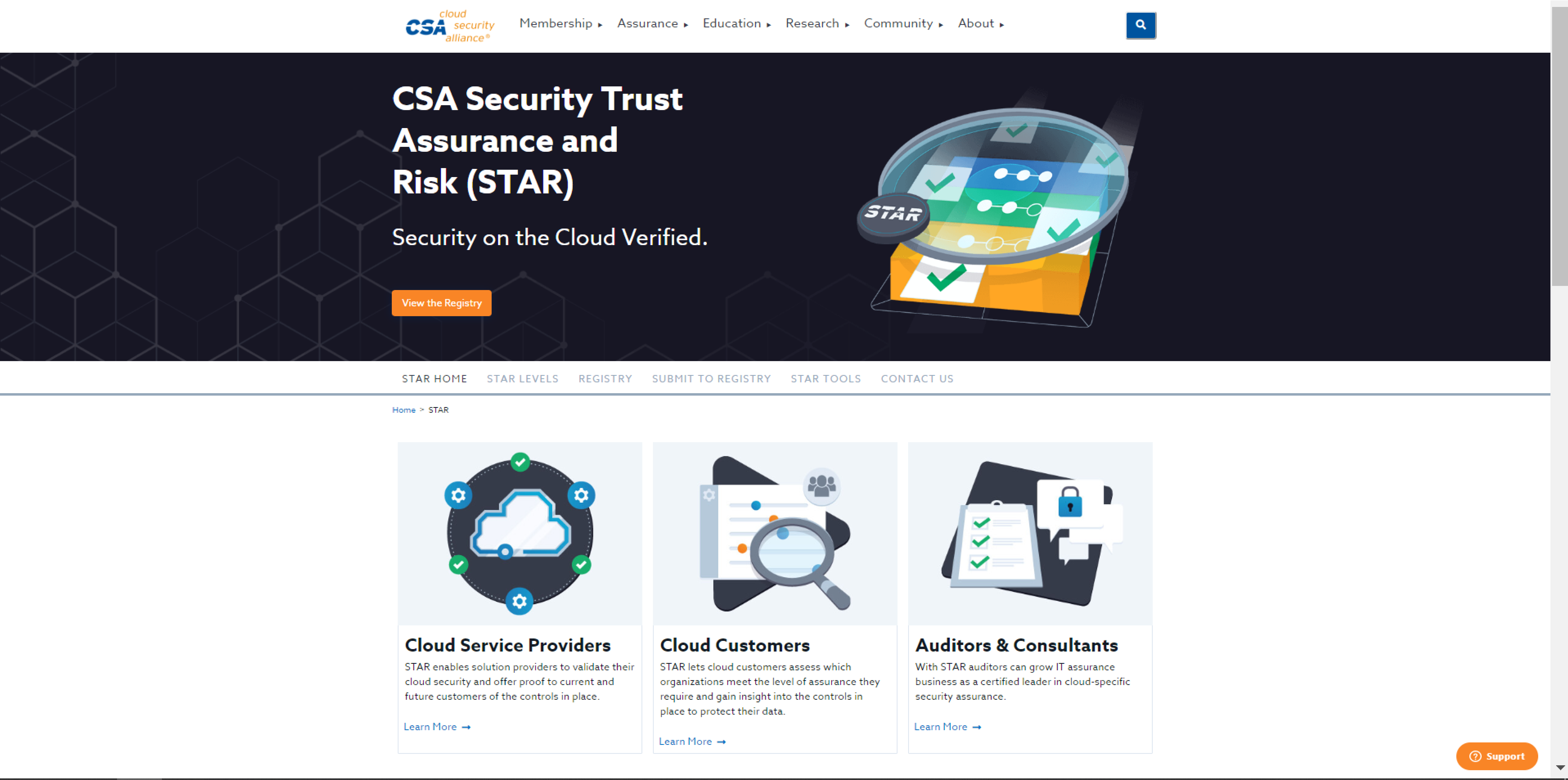
**Administrative procedures**

**Activity monitoring**

**Environment alignment**

# Cloud Specific Attestations and Certifications

# CSA Star Registry



CSA Security Trust Assurance and Risk (STAR)

Security on the Cloud Verified.

**Cloud Service Providers**

STAR enables solution providers to validate their cloud security and offer proof to current and future customers of the controls in place.

Learn More →

**Cloud Customers**

STAR lets cloud customers assess which organizations meet the level of assurance they require and gain insight into the controls in place to protect their data.

Learn More →

**Auditors & Consultants**

With STAR auditors can grow IT assurance business as a certified leader in cloud-specific security assurance.

Learn More →

# CSA STAR Level 1

**Self-assessment with CAIQ and CCM**

**GDPR Self-assessment**

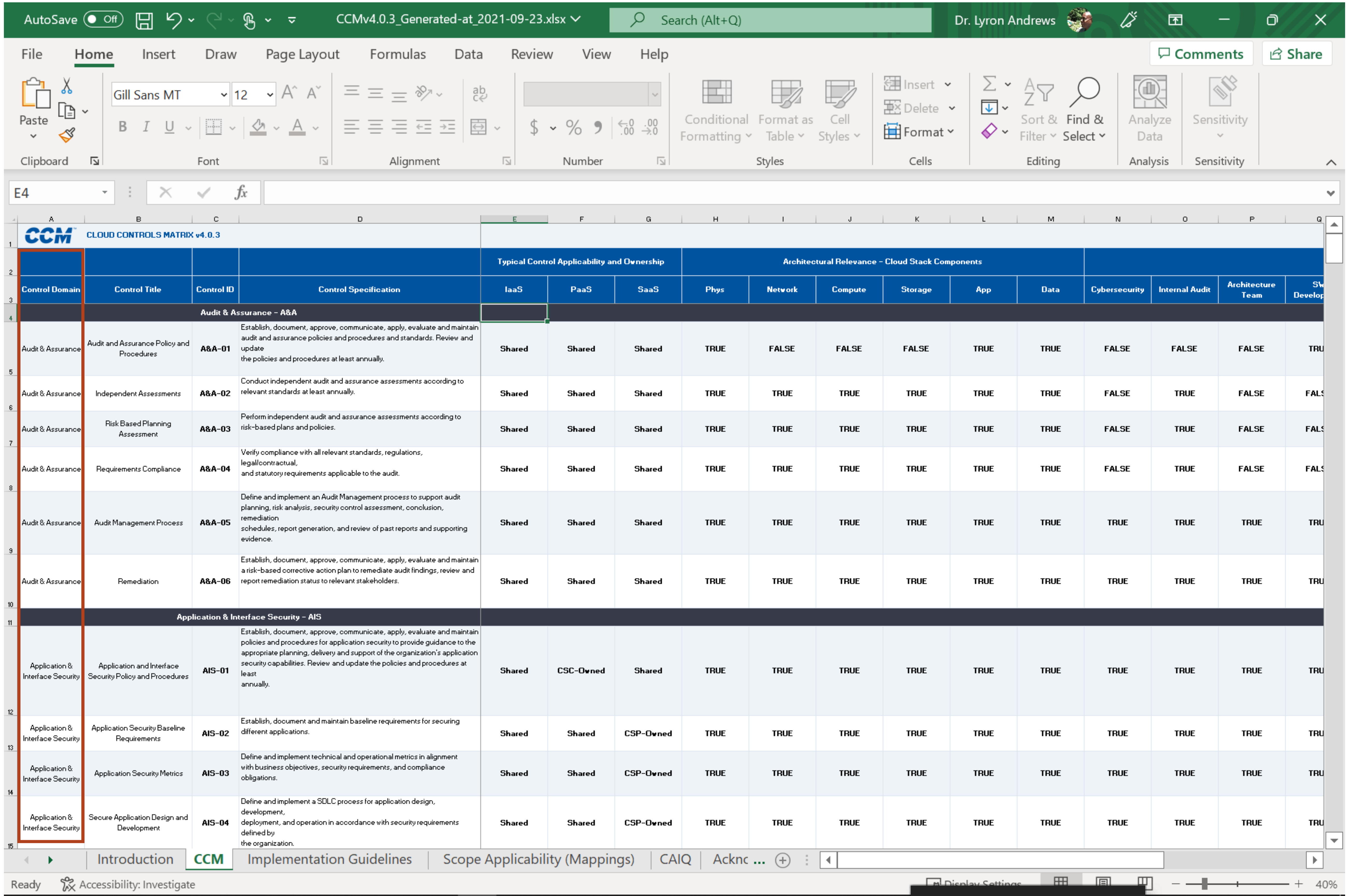
# CSA STAR

## Self-assessment

**Voluntary submission of documented cloud controls**

- Consensus Assessment Initiative Questionnaire (CAIQ)
- Cloud Controls Matrix (CCM)

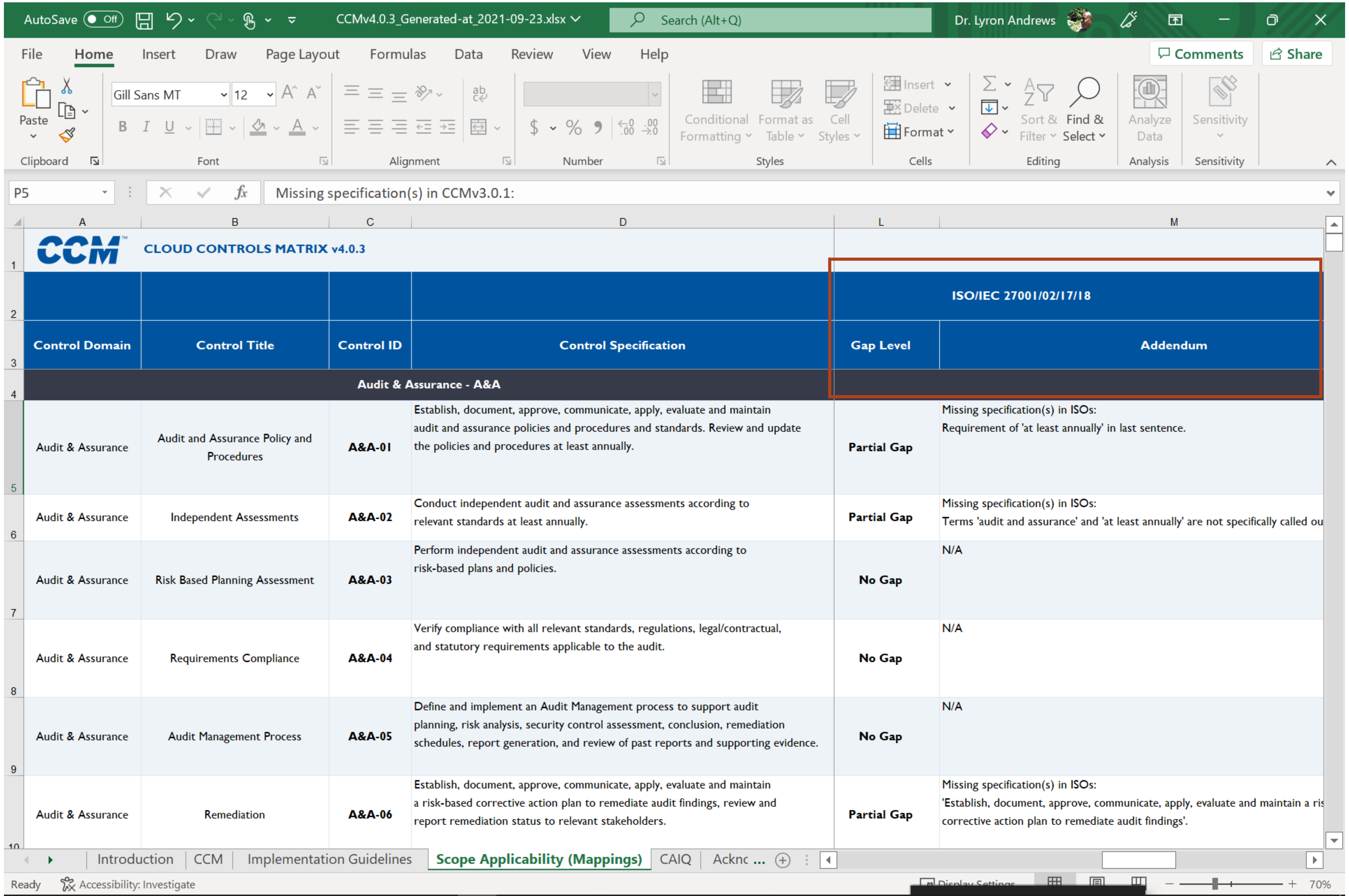
# Cloud Controls Matrix (CCM v4)



**CCM** CLOUD CONTROLS MATRIX v4.0.3

| | | | | Typical Control Applicability and Ownership | | | Architectural Relevance - Cloud Stack Components | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Control Domain | Control Title | Control ID | Control Specification | IaaS | PaaS | SaaS | Phys | Network | Compute | Storage | App | Data | Cybersecurity | Internal Audit | Architecture Team | SW Develop |
| | | | Audit & Assurance - A&A | | | | | | | | | | | | | |
| Audit & Assurance | Audit and Assurance Policy and Procedures | A&A-01 | Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually. | Shared | Shared | Shared | TRUE | FALSE | FALSE | FALSE | TRUE | TRUE | FALSE | FALSE | FALSE | TRU |
| Audit & Assurance | Independent Assessments | A&A-02 | Conduct independent audit and assurance assessments according to relevant standards at least annually. | Shared | Shared | Shared | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | FALSE | TRUE | FALSE | FALS |
| Audit & Assurance | Risk Based Planning Assessment | A&A-03 | Perform independent audit and assurance assessments according to risk-based plans and policies. | Shared | Shared | Shared | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | FALSE | TRUE | FALSE | FALS |
| Audit & Assurance | Requirements Compliance | A&A-04 | Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit. | Shared | Shared | Shared | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | FALSE | TRUE | FALSE | FALS |
| Audit & Assurance | Audit Management Process | A&A-05 | Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence. | Shared | Shared | Shared | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRU |
| Audit & Assurance | Remediation | A&A-06 | Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders. | Shared | Shared | Shared | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRU |
| | | | Application & Interface Security - AIS | | | | | | | | | | | | | |
| Application & Interface Security | Application and Interface Security Policy and Procedures | AIS-01 | Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually. | Shared | CSC-Owned | Shared | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRU |
| Application & Interface Security | Application Security Baseline Requirements | AIS-02 | Establish, document and maintain baseline requirements for securing different applications. | Shared | Shared | CSP-Owned | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRU |
| Application & Interface Security | Application Security Metrics | AIS-03 | Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations. | Shared | Shared | CSP-Owned | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRU |
| Application & Interface Security | Secure Application Design and Development | AIS-04 | Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization. | Shared | Shared | CSP-Owned | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRUE | TRU |

# Cloud Controls Matrix (CCM v4)

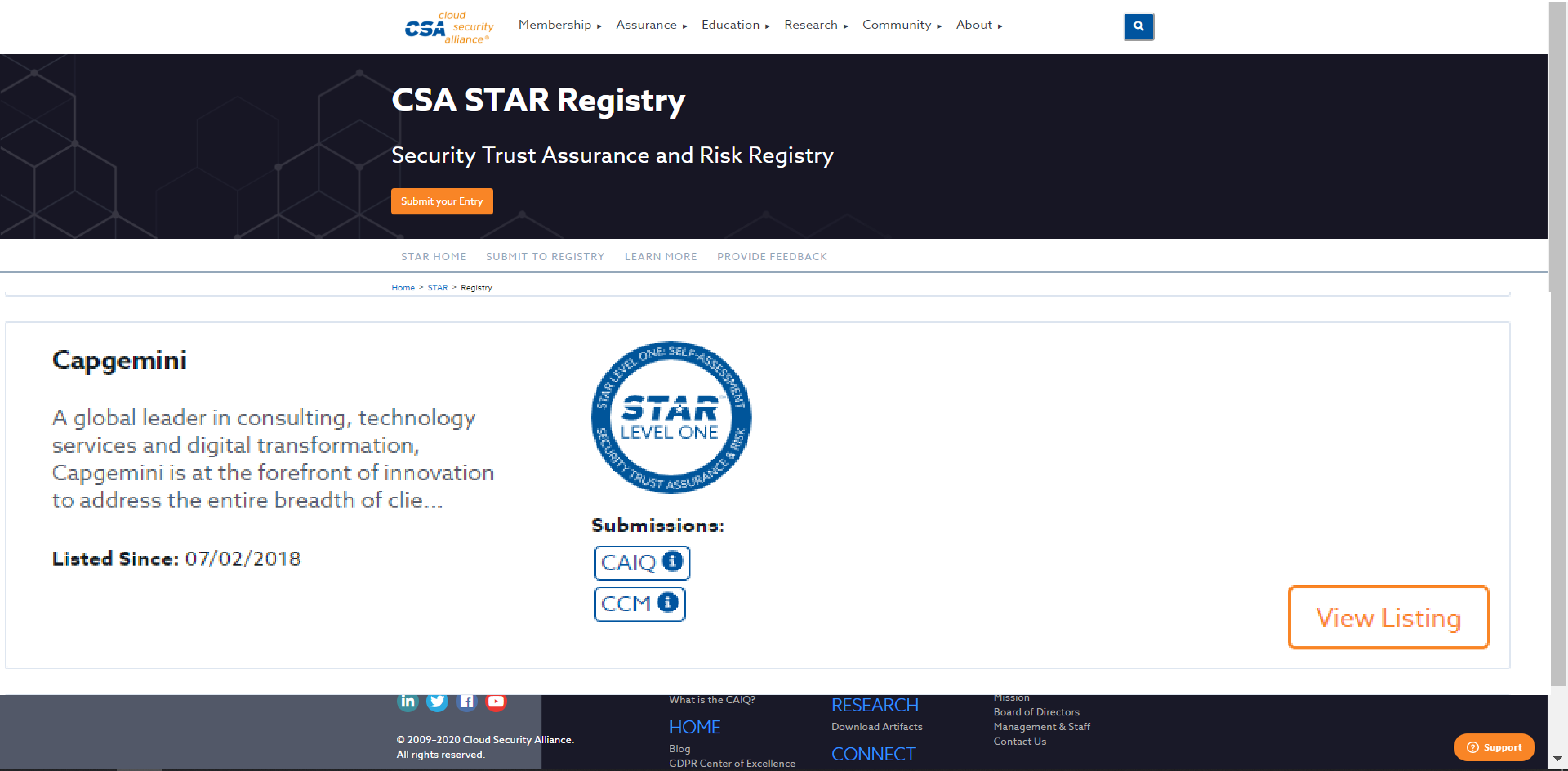


Missing specification(s) in CCMv3.0.1:

CCM CLOUD CONTROLS MATRIX v4.0.3

|  |  |  |  | ISO/IEC 27001/02/17/18 |  |
|---|---|---|---|---|---|
| **Control Domain** | **Control Title** | **Control ID** | **Control Specification** | **Gap Level** | **Addendum** |
| **Audit & Assurance - A&A** |  |  |  |  |  |
| Audit & Assurance | Audit and Assurance Policy and Procedures | **A&A-01** | Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually. | **Partial Gap** | Missing specification(s) in ISOs:<br>Requirement of 'at least annually' in last sentence. |
| Audit & Assurance | Independent Assessments | **A&A-02** | Conduct independent audit and assurance assessments according to relevant standards at least annually. | **Partial Gap** | Missing specification(s) in ISOs:<br>Terms 'audit and assurance' and 'at least annually' are not specifically called ou |
| Audit & Assurance | Risk Based Planning Assessment | **A&A-03** | Perform independent audit and assurance assessments according to risk-based plans and policies. | **No Gap** | N/A |
| Audit & Assurance | Requirements Compliance | **A&A-04** | Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit. | **No Gap** | N/A |
| Audit & Assurance | Audit Management Process | **A&A-05** | Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence. | **No Gap** | N/A |
| Audit & Assurance | Remediation | **A&A-06** | Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders. | **Partial Gap** | Missing specification(s) in ISOs:<br>'Establish, document, approve, communicate, apply, evaluate and maintain a ris corrective action plan to remediate audit findings'. |

# STAR Level 1



**CSA STAR Registry**

Security Trust Assurance and Risk Registry

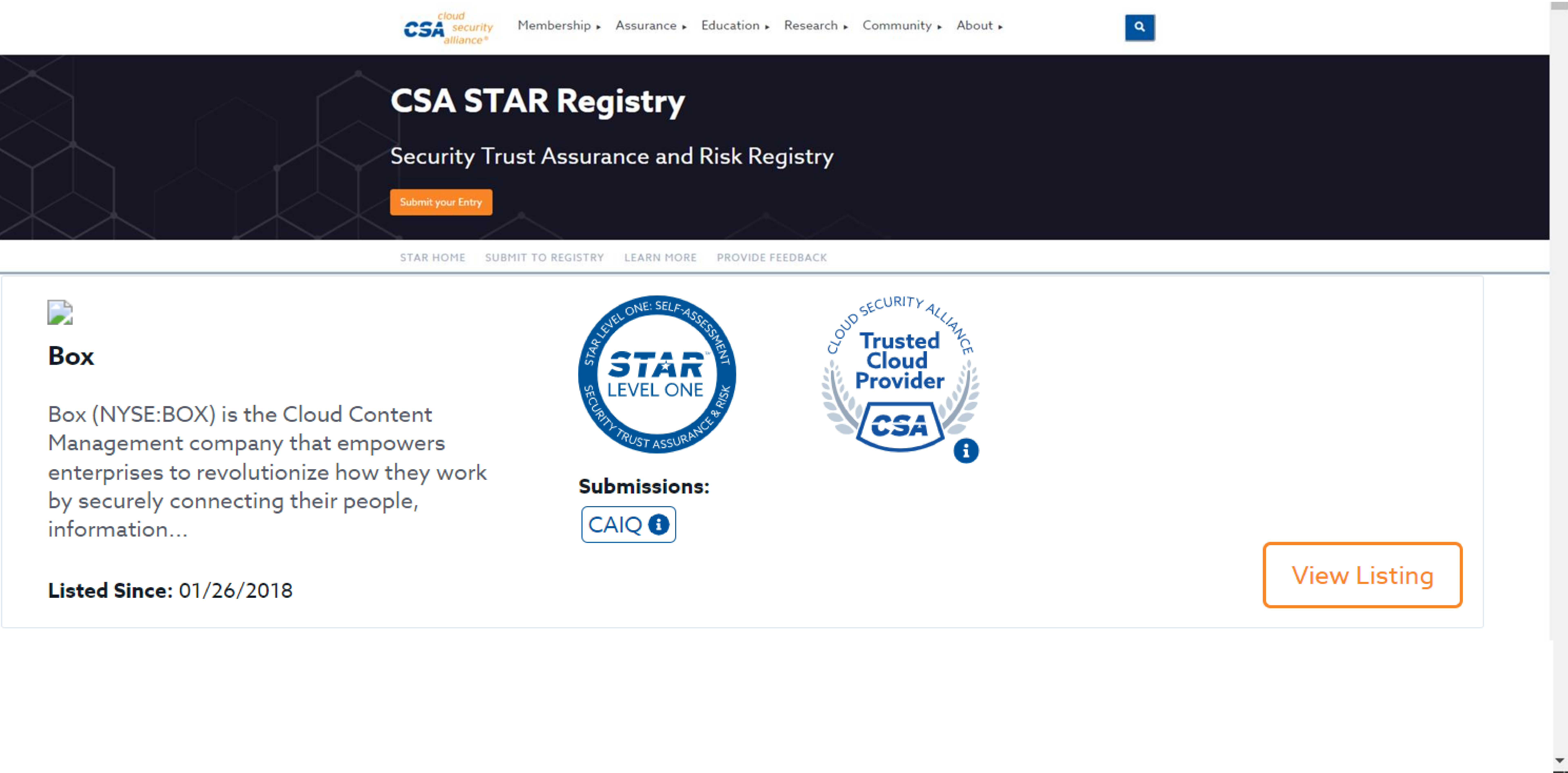
**Capgemini**

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clie...

**Listed Since:** 07/02/2018

**Submissions:**

# STAR Level 1



CSA STAR Registry

Security Trust Assurance and Risk Registry

**Box**

Box (NYSE:BOX) is the Cloud Content Management company that empowers enterprises to revolutionize how they work by securely connecting their people, information...

**Submissions:**

CAIQ

**Listed Since:** 01/26/2018

# STAR Level 2

**Third-party**

Attestation

Certification

# CSA STAR Certification

Third-party assessment tied to ISO 27001

Evaluates maturity of management capability

Evaluates organizational ISMS

# CSA STAR

## Certification Foundation

**ISO/IEC 17021:2011**

**ISO/IEC 27006:2011**

**ISO 19011**

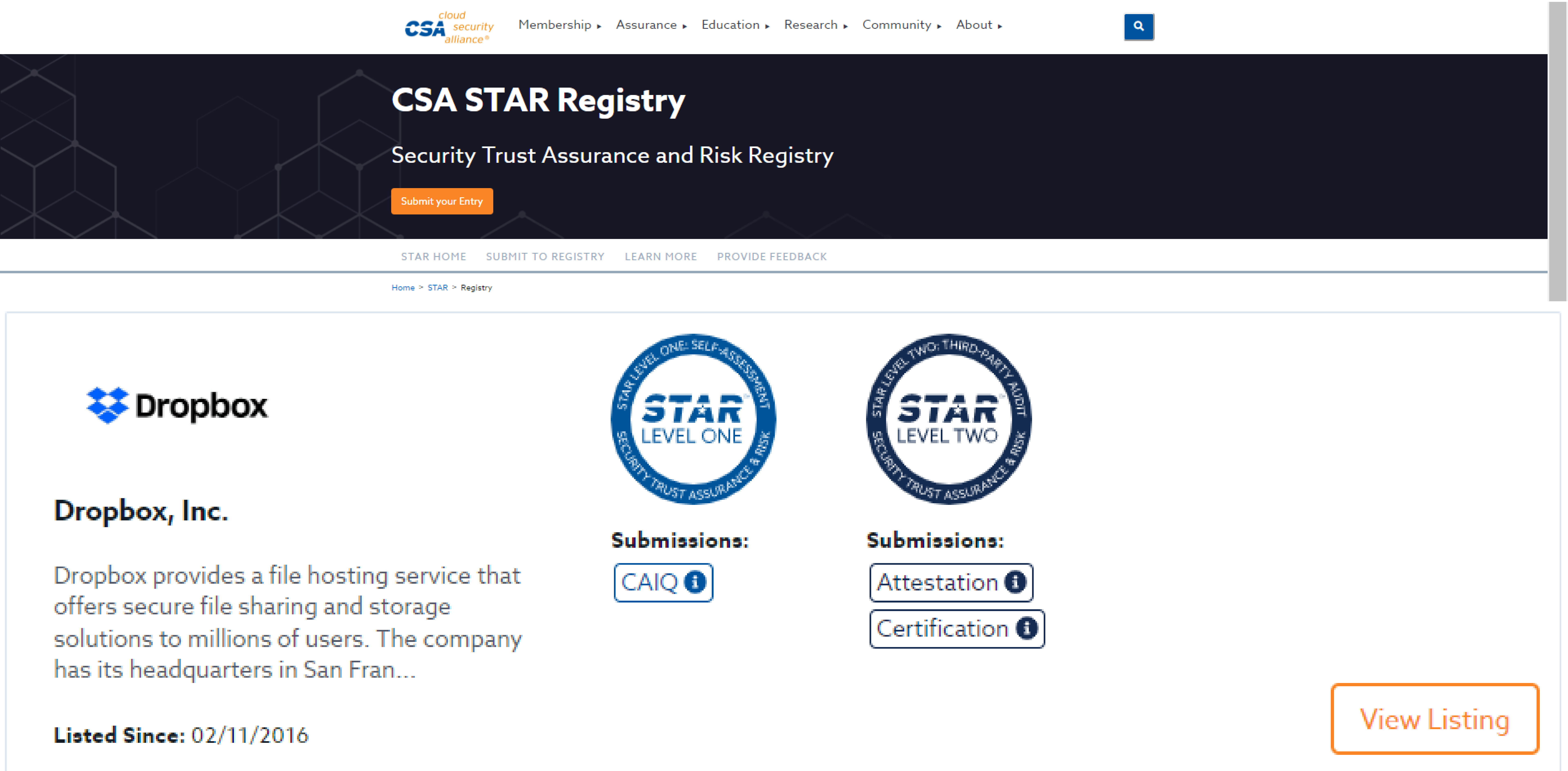
# CSA STAR Attestation

Third-party independent assessment of CSP security

Based upon SOC 2 type 1 or 2 attestations

Includes tests of controls

# CSA Star Level 2



## CSA STAR Registry

Security Trust Assurance and Risk Registry

**Dropbox, Inc.**

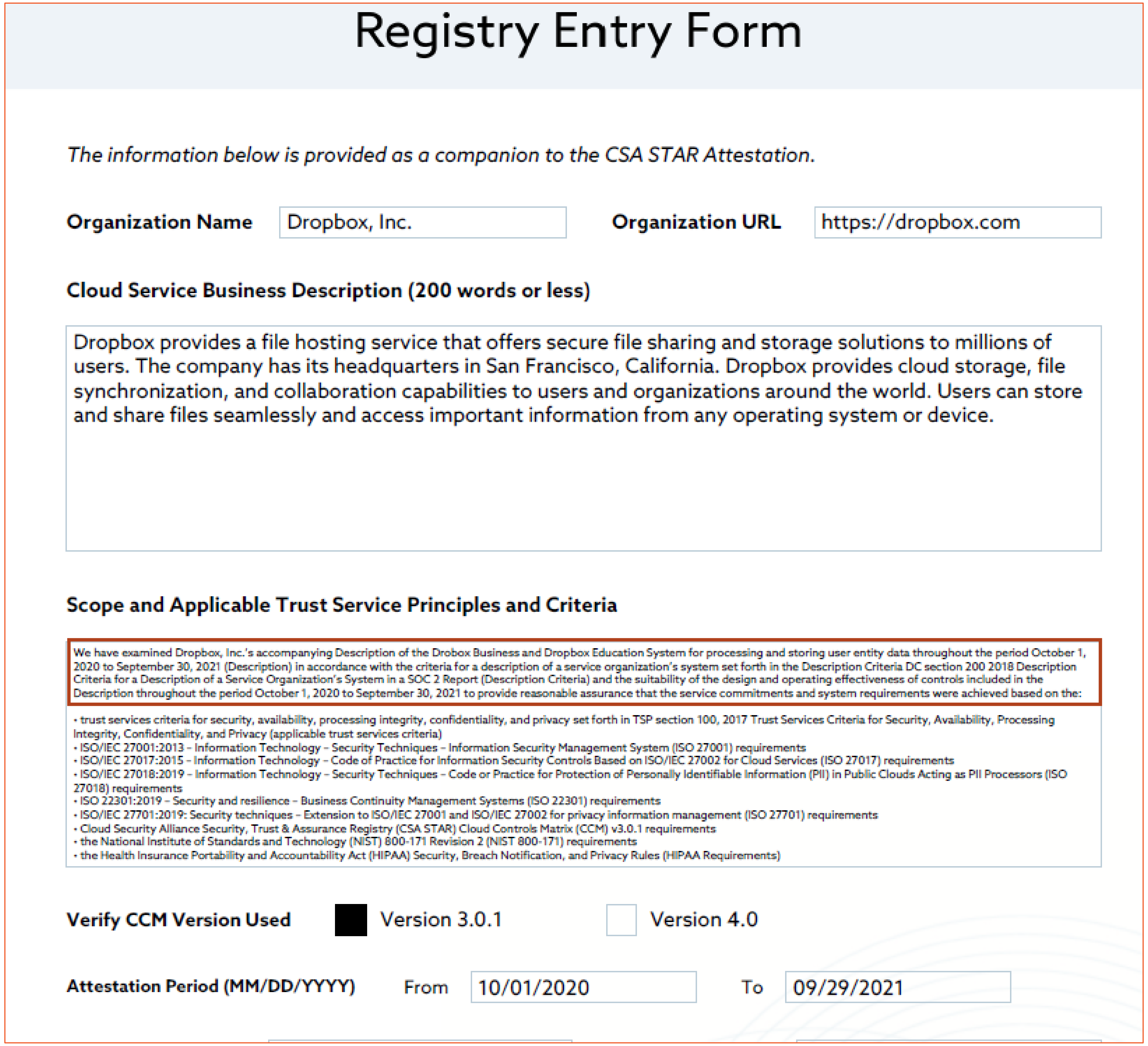
Dropbox provides a file hosting service that offers secure file sharing and storage solutions to millions of users. The company has its headquarters in San Fran...

**Submissions:**

**Submissions:**

**Listed Since:** 02/11/2016

# Cloud Controls Attestation



## Registry Entry Form

*The information below is provided as a companion to the CSA STAR Attestation.*

**Organization Name** Dropbox, Inc.

**Organization URL** https://dropbox.com

**Cloud Service Business Description (200 words or less)**

Dropbox provides a file hosting service that offers secure file sharing and storage solutions to millions of users. The company has its headquarters in San Francisco, California. Dropbox provides cloud storage, file synchronization, and collaboration capabilities to users and organizations around the world. Users can store and share files seamlessly and access important information from any operating system or device.

**Scope and Applicable Trust Service Principles and Criteria**

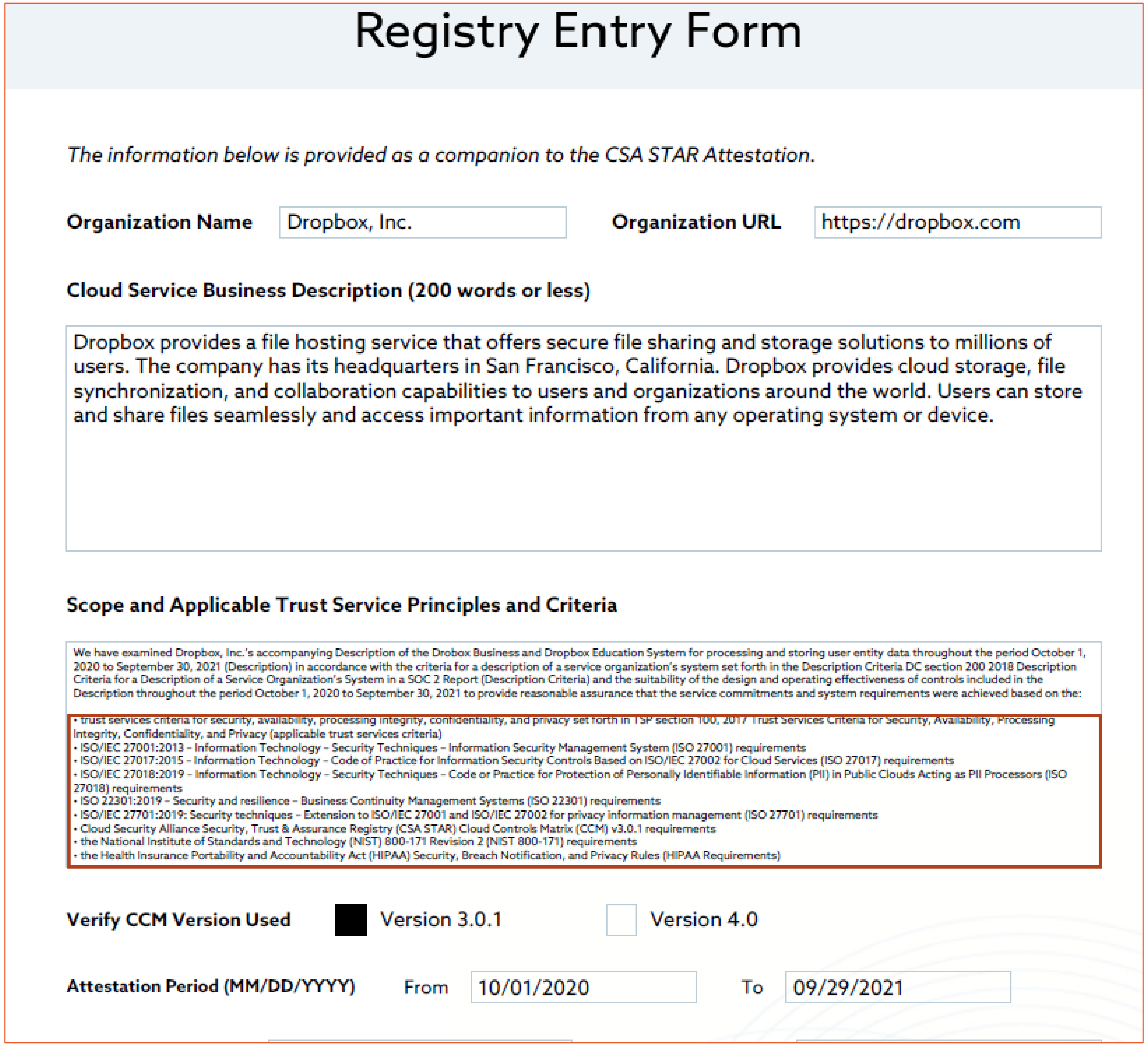
We have examined Dropbox, Inc.'s accompanying Description of the Drobox Business and Dropbox Education System for processing and storing user entity data throughout the period October 1, 2020 to September 30, 2021 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period October 1, 2020 to September 30, 2021 to provide reasonable assurance that the service commitments and system requirements were achieved based on the:

- trust services criteria for security, availability, processing integrity, confidentiality, and privacy set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria)
- ISO/IEC 27001:2013 – Information Technology – Security Techniques – Information Security Management System (ISO 27001) requirements
- ISO/IEC 27017:2015 – Information Technology – Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services (ISO 27017) requirements
- ISO/IEC 27018:2019 – Information Technology – Security Techniques – Code or Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors (ISO 27018) requirements
- ISO 22301:2019 – Security and resilience – Business Continuity Management Systems (ISO 22301) requirements
- ISO/IEC 27701:2019: Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management (ISO 27701) requirements
- Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR) Cloud Controls Matrix (CCM) v3.0.1 requirements
- the National Institute of Standards and Technology (NIST) 800-171 Revision 2 (NIST 800-171) requirements
- the Health Insurance Portability and Accountability Act (HIPAA) Security, Breach Notification, and Privacy Rules (HIPAA Requirements)

**Verify CCM Version Used** ■ Version 3.0.1 ☐ Version 4.0

**Attestation Period (MM/DD/YYYY)** From 10/01/2020 To 09/29/2021

# Cloud Controls Attestation



## Registry Entry Form

*The information below is provided as a companion to the CSA STAR Attestation.*

**Organization Name** Dropbox, Inc.

**Organization URL** https://dropbox.com

**Cloud Service Business Description (200 words or less)**

Dropbox provides a file hosting service that offers secure file sharing and storage solutions to millions of users. The company has its headquarters in San Francisco, California. Dropbox provides cloud storage, file synchronization, and collaboration capabilities to users and organizations around the world. Users can store and share files seamlessly and access important information from any operating system or device.

**Scope and Applicable Trust Service Principles and Criteria**

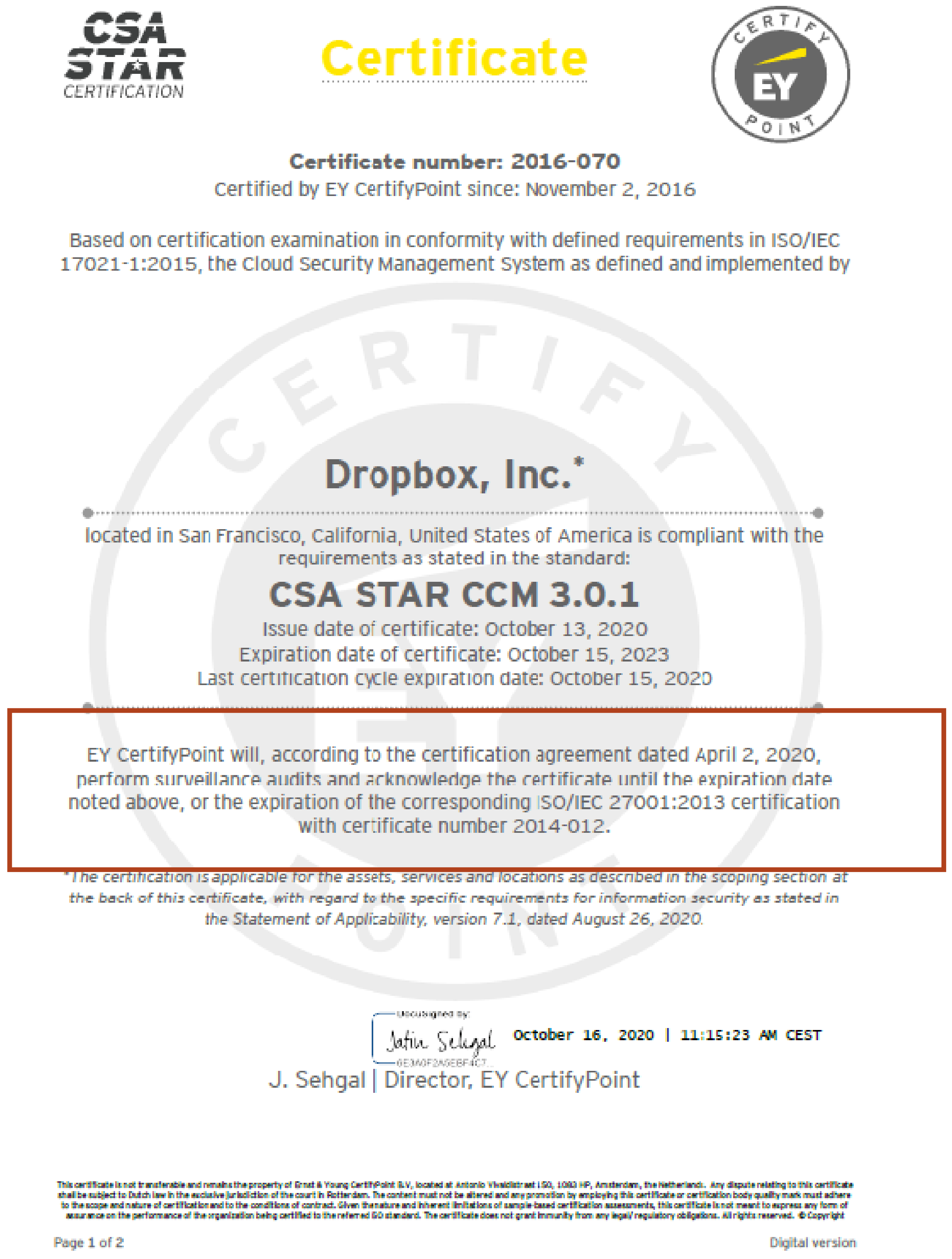
We have examined Dropbox, Inc.'s accompanying Description of the Drobox Business and Dropbox Education System for processing and storing user entity data throughout the period October 1, 2020 to September 30, 2021 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period October 1, 2020 to September 30, 2021 to provide reasonable assurance that the service commitments and system requirements were achieved based on the:

- trust services criteria for security, availability, processing integrity, confidentiality, and privacy set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria)
- ISO/IEC 27001:2013 – Information Technology – Security Techniques – Information Security Management System (ISO 27001) requirements
- ISO/IEC 27017:2015 – Information Technology – Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services (ISO 27017) requirements
- ISO/IEC 27018:2019 – Information Technology – Security Techniques – Code or Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors (ISO 27018) requirements
- ISO 22301:2019 – Security and resilience – Business Continuity Management Systems (ISO 22301) requirements
- ISO/IEC 27701:2019: Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management (ISO 27701) requirements
- Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR) Cloud Controls Matrix (CCM) v3.0.1 requirements
- the National Institute of Standards and Technology (NIST) 800-171 Revision 2 (NIST 800-171) requirements
- the Health Insurance Portability and Accountability Act (HIPAA) Security, Breach Notification, and Privacy Rules (HIPAA Requirements)

**Verify CCM Version Used** ☑ Version 3.0.1 ☐ Version 4.0

**Attestation Period (MM/DD/YYYY)** From 10/01/2020 To 09/29/2021

# Cloud Controls Certification



CSA STAR CERTIFICATION

**Certificate**

**Certificate number: 2016-070**

Certified by EY CertifyPoint since: November 2, 2016

Based on certification examination in conformity with defined requirements in ISO/IEC 17021-1:2015, the Cloud Security Management System as defined and implemented by

**Dropbox, Inc.***

located in San Francisco, California, United States of America is compliant with the requirements as stated in the standard:

**CSA STAR CCM 3.0.1**

Issue date of certificate: October 13, 2020
Expiration date of certificate: October 15, 2023
Last certification cycle expiration date: October 15, 2020

EY CertifyPoint will, according to the certification agreement dated April 2, 2020, perform surveillance audits and acknowledge the certificate until the expiration date noted above, or the expiration of the corresponding ISO/IEC 27001:2013 certification with certificate number 2014-012.

**The certification is applicable for the assets, services and locations as described in the scoping section at the back of this certificate, with regard to the specific requirements for information security as stated in the Statement of Applicability, version 7.1, dated August 26, 2020.*

DocuSigned by:
Jatin Sehgal
6E3A0F2A0EBF4C7...

October 16, 2020 | 11:15:23 AM CEST

J. Sehgal | Director, EY CertifyPoint

This certificate is not transferable and remains the property of Ernst & Young CertifyPoint B.V., located at Antonio Vivaldistraat 150, 1083 HP, Amsterdam, the Netherlands. Any dispute relating to this certificate shall be subject to Dutch law in the exclusive jurisdiction of the court in Rotterdam. The content must not be altered and any promotion by employing this certificate or certification body quality mark must adhere to the scope and nature of certification and to the conditions of contract. Given the nature and inherent limitations of sample-based certification assessments, this certificate is not meant to express any form of assurance on the performance of the organization being certified to the referred ISO standard. The certificate does not grant immunity from any legal/ regulatory obligations. All rights reserved. © Copyright

Page 1 of 2

Digital version

# Evaluating Cloud Service Providers by EuroCloud StarAudit

# EuroCloud StarAudit Program

**Global program**

**Facilitates innovation**

# StarAudit Activity Areas

Awareness Programs

Data Privacy Compliance

Knowledge Transfer

Start Up Encouragement

Standards and Interoperability

Legal Framework Harmonization

**Two-way trust**

**Assessments to establish transparency**

**Ubiquitous knowledge transfer**

# StarAudit Certification Scheme

# StarAudit Assessment Tool

**Self-assessment**

**Compliance checks**

**Gap analysis**

**Vendor comparison**

**Checklist development**

**Auditing-related work**

# StarAudit Vision

Tools selection

Reduce burden

Transparency

Knowledge transfer

# Reviewing Audit Practice Acceptability

# Audit Scope Restrictions

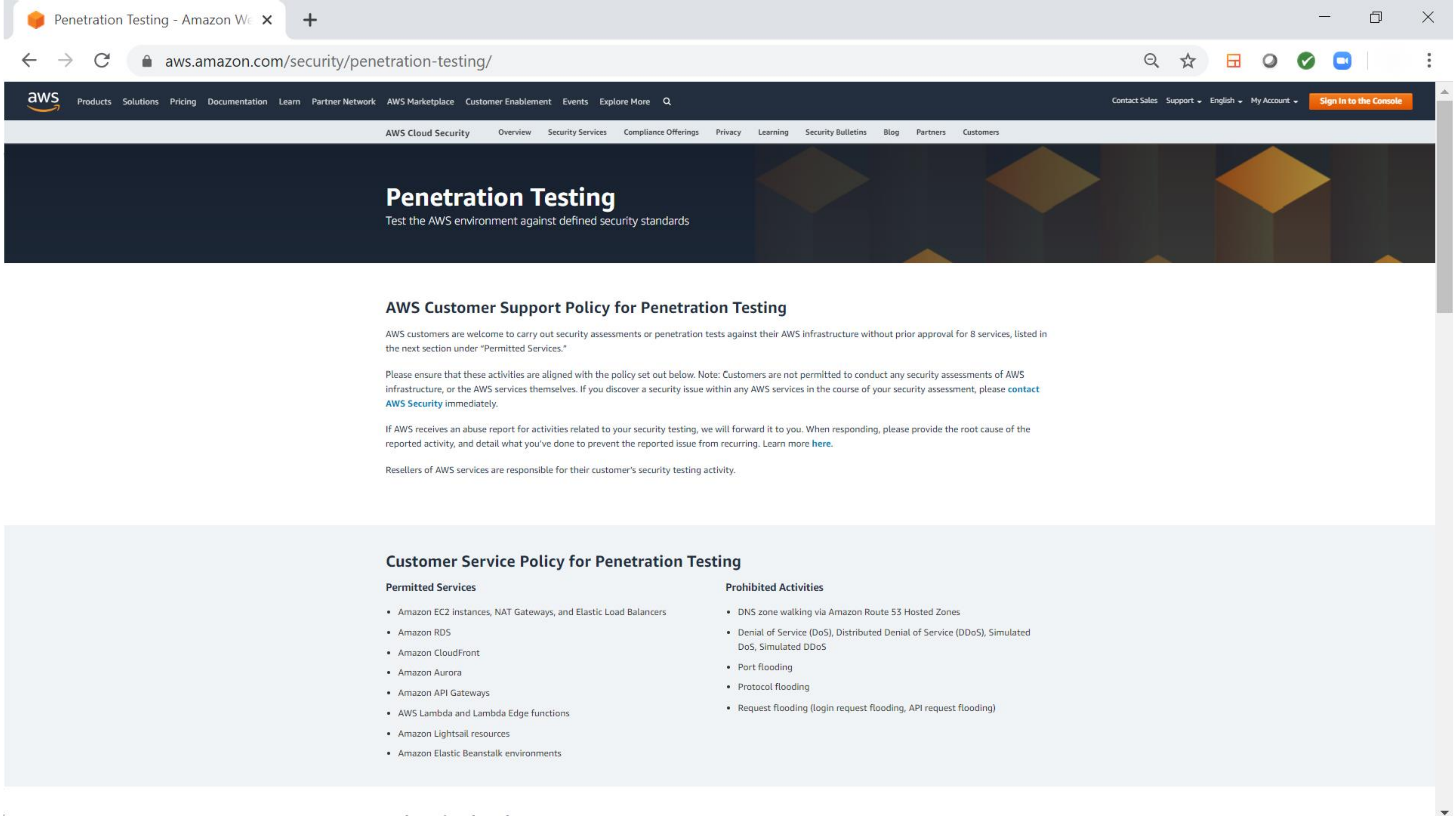
Proof of effectiveness through testing

Inform audit-ready environments

Used to ensure reduced impact

Some providers may not allow certain testing

# Amazon Penetration Testing Policy



## Penetration Testing

Test the AWS environment against defined security standards

### AWS Customer Support Policy for Penetration Testing

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services, listed in the next section under "Permitted Services."

Please ensure that these activities are aligned with the policy set out below. Note: Customers are not permitted to conduct any security assessments of AWS infrastructure, or the AWS services themselves. If you discover a security issue within any AWS services in the course of your security assessment, please **contact AWS Security** immediately.

If AWS receives an abuse report for activities related to your security testing, we will forward it to you. When responding, please provide the root cause of the reported activity, and detail what you've done to prevent the reported issue from recurring. Learn more **here**.

Resellers of AWS services are responsible for their customer's security testing activity.

### Customer Service Policy for Penetration Testing

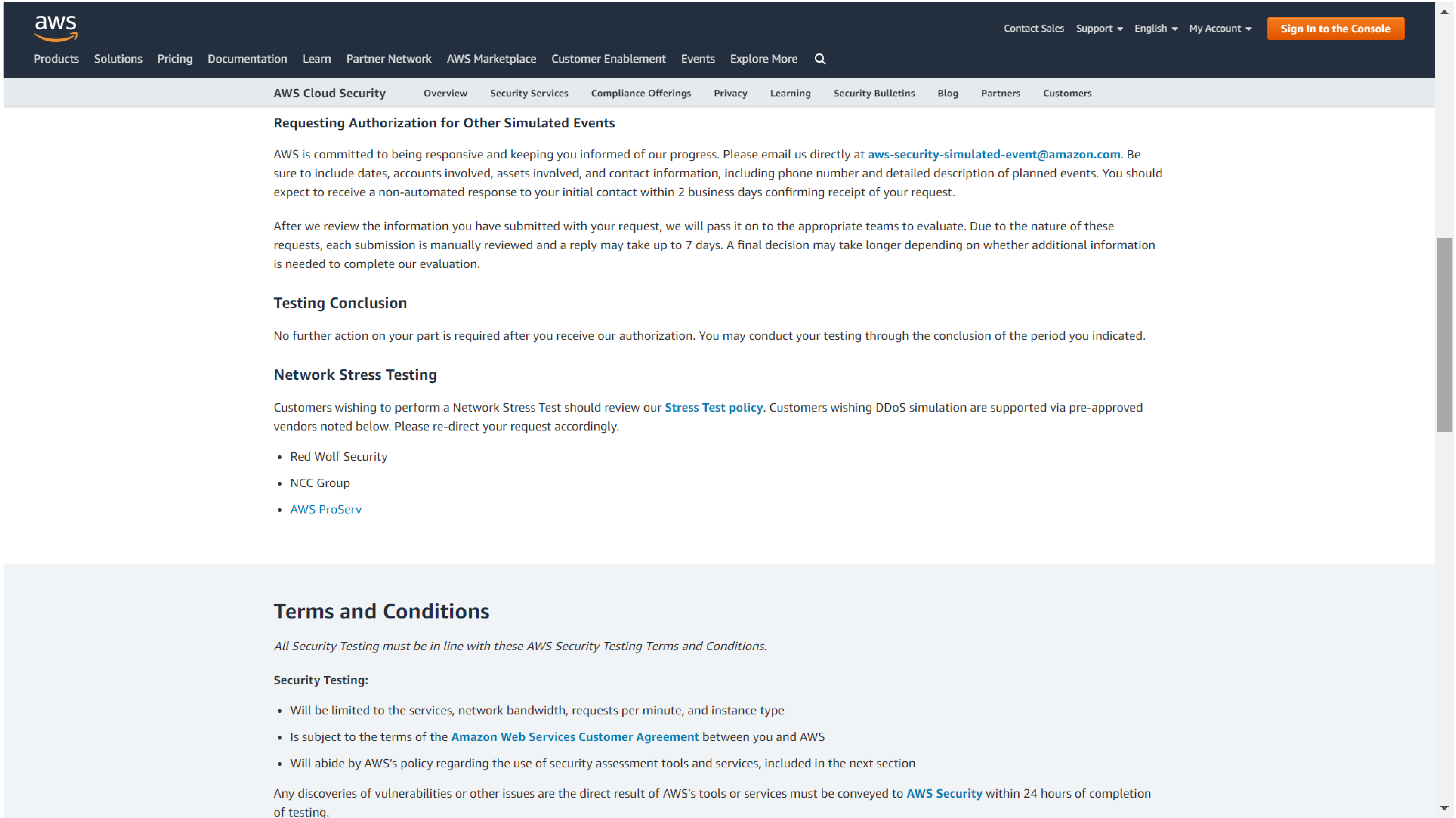
**Permitted Services**

- 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
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

# Amazon Penetration Testing Policy



**Requesting Authorization for Other Simulated Events**

AWS is committed to being responsive and keeping you informed of our progress. Please email us directly at **aws-security-simulated-event@amazon.com**. Be sure to include dates, accounts involved, assets involved, and contact information, including phone number and detailed description of planned events. You should expect to receive a non-automated response to your initial contact within 2 business days confirming receipt of your request.

After we review the information you have submitted with your request, we will pass it on to the appropriate teams to evaluate. Due to the nature of these requests, each submission is manually reviewed and a reply may take up to 7 days. A final decision may take longer depending on whether additional information is needed to complete our evaluation.

### Testing Conclusion

No further action on your part is required after you receive our authorization. You may conduct your testing through the conclusion of the period you indicated.

### Network Stress Testing

Customers wishing to perform a Network Stress Test should review our **Stress Test policy**. Customers wishing DDoS simulation are supported via pre-approved vendors noted below. Please re-direct your request accordingly.

- Red Wolf Security
- NCC Group
- AWS ProServ

## Terms and Conditions

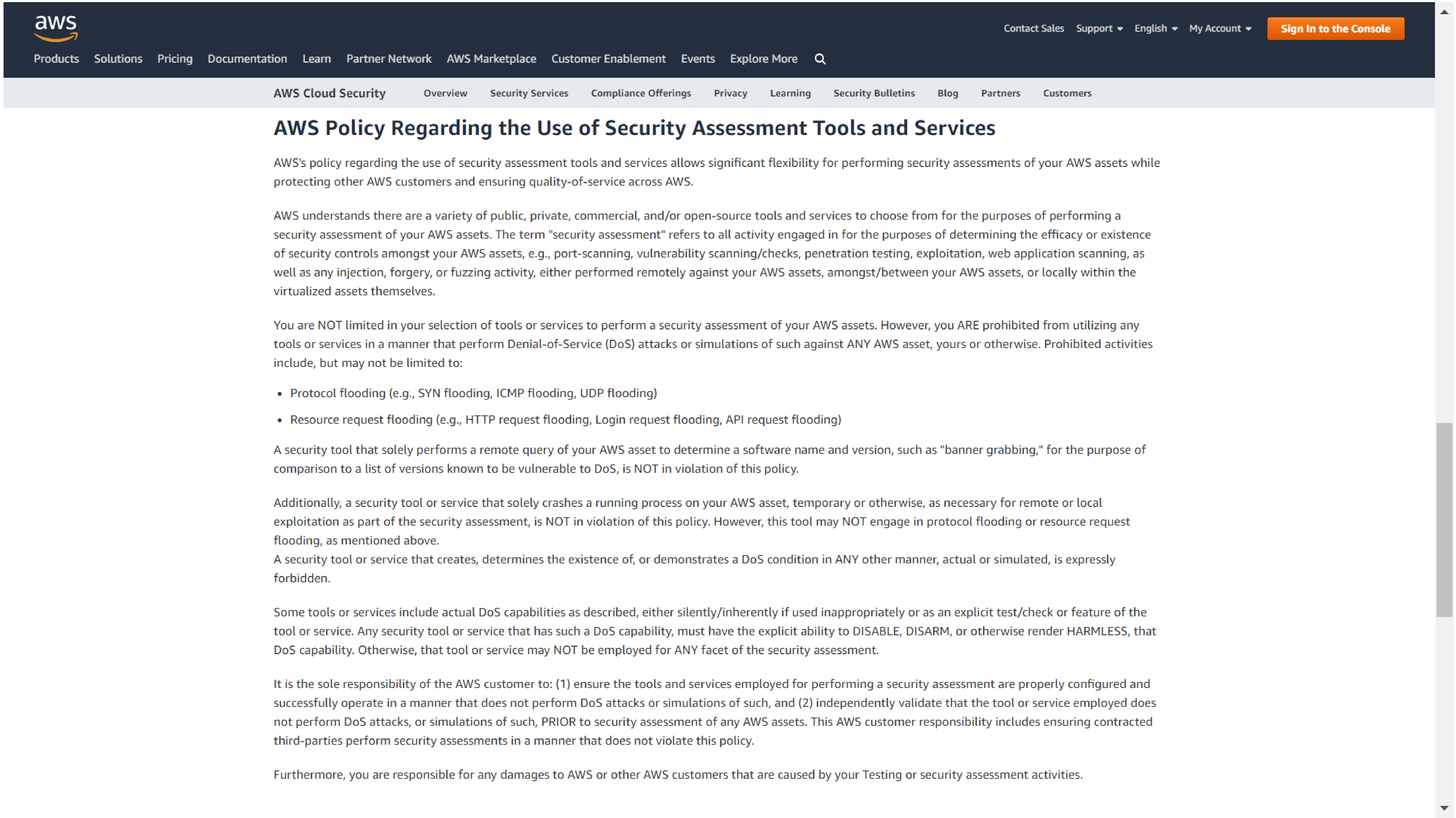
*All Security Testing must be in line with these AWS Security Testing Terms and Conditions.*

**Security Testing:**

- Will be limited to the services, network bandwidth, requests per minute, and instance type
- Is subject to the terms of the **Amazon Web Services Customer Agreement** between you and AWS
- Will abide by AWS's policy regarding the use of security assessment tools and services, included in the next section

Any discoveries of vulnerabilities or other issues are the direct result of AWS's tools or services must be conveyed to **AWS Security** within 24 hours of completion of testing.

# Amazon Penetration Testing Policy



## AWS Policy Regarding the Use of Security Assessment Tools and Services

AWS's policy regarding the use of security assessment tools and services allows significant flexibility for performing security assessments of your AWS assets while protecting other AWS customers and ensuring quality-of-service across AWS.

AWS understands there are a variety of public, private, commercial, and/or open-source tools and services to choose from for the purposes of performing a security assessment of your AWS assets. The term "security assessment" refers to all activity engaged in for the purposes of determining the efficacy or existence of security controls amongst your AWS assets, e.g., port-scanning, vulnerability scanning/checks, penetration testing, exploitation, web application scanning, as well as any injection, forgery, or fuzzing activity, either performed remotely against your AWS assets, amongst/between your AWS assets, or locally within the virtualized assets themselves.

You are NOT limited in your selection of tools or services to perform a security assessment of your AWS assets. However, you ARE prohibited from utilizing any tools or services in a manner that perform Denial-of-Service (DoS) attacks or simulations of such against ANY AWS asset, yours or otherwise. Prohibited activities include, but may not be limited to:

- Protocol flooding (e.g., SYN flooding, ICMP flooding, UDP flooding)
- Resource request flooding (e.g., HTTP request flooding, Login request flooding, API request flooding)

A security tool that solely performs a remote query of your AWS asset to determine a software name and version, such as "banner grabbing," for the purpose of comparison to a list of versions known to be vulnerable to DoS, is NOT in violation of this policy.

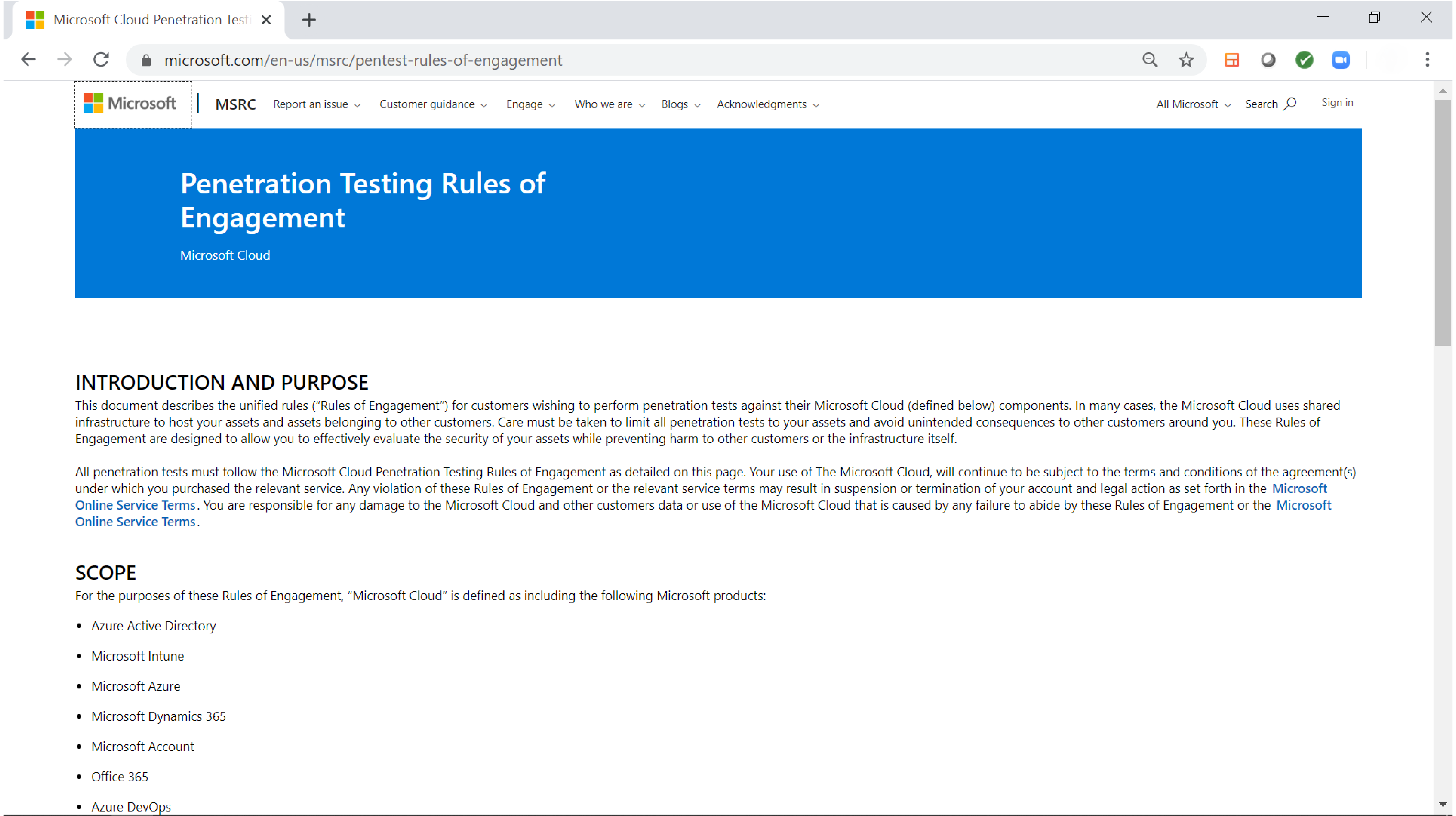
Additionally, a security tool or service that solely crashes a running process on your AWS asset, temporary or otherwise, as necessary for remote or local exploitation as part of the security assessment, is NOT in violation of this policy. However, this tool may NOT engage in protocol flooding or resource request flooding, as mentioned above.
A security tool or service that creates, determines the existence of, or demonstrates a DoS condition in ANY other manner, actual or simulated, is expressly forbidden.

Some tools or services include actual DoS capabilities as described, either silently/inherently if used inappropriately or as an explicit test/check or feature of the tool or service. Any security tool or service that has such a DoS capability, must have the explicit ability to DISABLE, DISARM, or otherwise render HARMLESS, that DoS capability. Otherwise, that tool or service may NOT be employed for ANY facet of the security assessment.

It is the sole responsibility of the AWS customer to: (1) ensure the tools and services employed for performing a security assessment are properly configured and successfully operate in a manner that does not perform DoS attacks or simulations of such, and (2) independently validate that the tool or service employed does not perform DoS attacks, or simulations of such, PRIOR to security assessment of any AWS assets. This AWS customer responsibility includes ensuring contracted third-parties perform security assessments in a manner that does not violate this policy.

Furthermore, you are responsible for any damages to AWS or other AWS customers that are caused by your Testing or security assessment activities.

# Azure Penetration Testing Policy



## Penetration Testing Rules of Engagement

Microsoft Cloud

## INTRODUCTION AND PURPOSE

This document describes the unified rules ("Rules of Engagement") for customers wishing to perform penetration tests against their Microsoft Cloud (defined below) components. In many cases, the Microsoft Cloud uses shared infrastructure to host your assets and assets belonging to other customers. Care must be taken to limit all penetration tests to your assets and avoid unintended consequences to other customers around you. These Rules of Engagement are designed to allow you to effectively evaluate the security of your assets while preventing harm to other customers or the infrastructure itself.

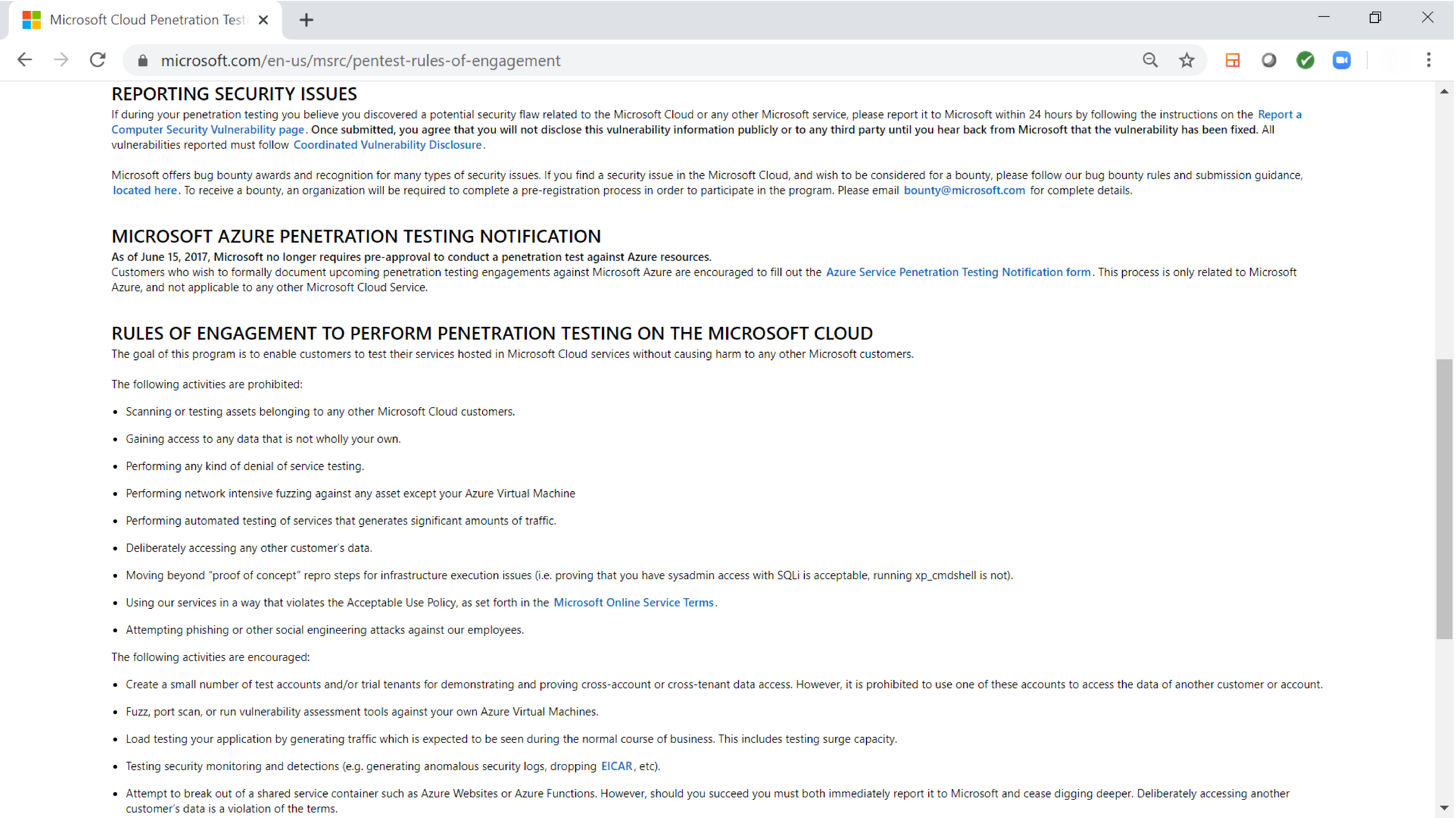
All penetration tests must follow the Microsoft Cloud Penetration Testing Rules of Engagement as detailed on this page. Your use of The Microsoft Cloud, will continue to be subject to the terms and conditions of the agreement(s) under which you purchased the relevant service. Any violation of these Rules of Engagement or the relevant service terms may result in suspension or termination of your account and legal action as set forth in the Microsoft Online Service Terms. You are responsible for any damage to the Microsoft Cloud and other customers data or use of the Microsoft Cloud that is caused by any failure to abide by these Rules of Engagement or the Microsoft Online Service Terms.

## SCOPE

For the purposes of these Rules of Engagement, "Microsoft Cloud" is defined as including the following Microsoft products:

- Azure Active Directory
- Microsoft Intune
- Microsoft Azure
- Microsoft Dynamics 365
- Microsoft Account
- Office 365
- Azure DevOps

# Azure Policy


Microsoft Cloud Penetration Test
microsoft.com/en-us/msrc/pentest-rules-of-engagement

## REPORTING SECURITY ISSUES

If during your penetration testing you believe you discovered a potential security flaw related to the Microsoft Cloud or any other Microsoft service, please report it to Microsoft within 24 hours by following the instructions on the Report a Computer Security Vulnerability page. **Once submitted, you agree that you will not disclose this vulnerability information publicly or to any third party until you hear back from Microsoft that the vulnerability has been fixed.** All vulnerabilities reported must follow Coordinated Vulnerability Disclosure.

Microsoft offers bug bounty awards and recognition for many types of security issues. If you find a security issue in the Microsoft Cloud, and wish to be considered for a bounty, please follow our bug bounty rules and submission guidance, located here. To receive a bounty, an organization will be required to complete a pre-registration process in order to participate in the program. Please email bounty@microsoft.com for complete details.

## MICROSOFT AZURE PENETRATION TESTING NOTIFICATION

**As of June 15, 2017, Microsoft no longer requires pre-approval to conduct a penetration test against Azure resources.**
Customers who wish to formally document upcoming penetration testing engagements against Microsoft Azure are encouraged to fill out the Azure Service Penetration Testing Notification form. This process is only related to Microsoft Azure, and not applicable to any other Microsoft Cloud Service.

## 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.

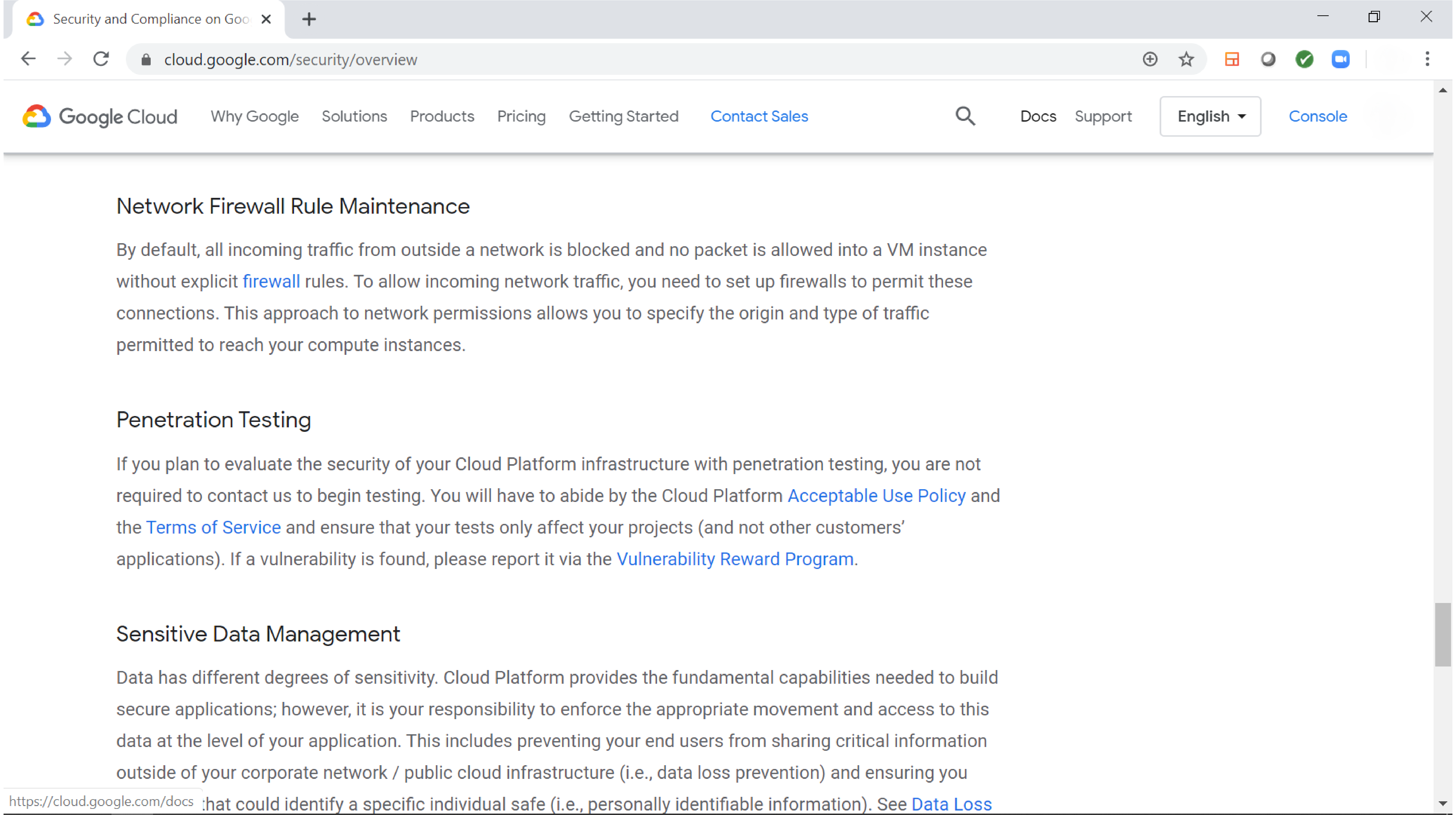
The following activities are prohibited:

- 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.

The following activities are encouraged:

- Create a small number of test accounts and/or trial tenants for demonstrating and proving cross-account or cross-tenant data access. However, it is prohibited to use one of these accounts to access the data of another customer or account.
- Fuzz, port scan, or run vulnerability assessment tools against your own Azure Virtual Machines.
- Load testing your application by generating traffic which is expected to be seen during the normal course of business. This includes testing surge capacity.
- Testing security monitoring and detections (e.g. generating anomalous security logs, dropping EICAR, etc).
- Attempt to break out of a shared service container such as Azure Websites or Azure Functions. However, should you succeed you must both immediately report it to Microsoft and cease digging deeper. Deliberately accessing another customer's data is a violation of the terms.

# Google Penetration Testing Policy



## Network Firewall Rule Maintenance

By default, all incoming traffic from outside a network is blocked and no packet is allowed into a VM instance without explicit firewall rules. To allow incoming network traffic, you need to set up firewalls to permit these connections. This approach to network permissions allows you to specify the origin and type of traffic permitted to reach your compute instances.

## Penetration Testing

If you plan to evaluate the security of your Cloud Platform infrastructure with penetration testing, you are not required to contact us to begin testing. You will have to abide by the Cloud Platform Acceptable Use Policy and the 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.

## Sensitive Data Management

Data has different degrees of sensitivity. Cloud Platform provides the fundamental capabilities needed to build secure applications; however, it is your responsibility to enforce the appropriate movement and access to this data at the level of your application. This includes preventing your end users from sharing critical information outside of your corporate network / public cloud infrastructure (i.e., data loss prevention) and ensuring you :hat could identify a specific individual safe (i.e., personally identifiable information). See Data Loss

# Summary

What specific confidence or assurance does your business require?

How will you get the level of assurance needed?

Why is it important for a CSP to have an established audit program?