Accessing AWS Compliance Reports

In this activity you will access AWS Artifact and download a compliance report and work through guidance on how to interpret the report. This activity is a great place to start if you are new to AWS, it mixes a bit of hands-on with supporting theory.

Learning Outcomes

This activity provides an introduction to compliance at AWS including the Shared Responsibility Model. When you have completed this activity, you will be: familiar with the Shared Responsibility Model, and be able to access AWS' security and compliance reports.

Target Audience

This activity has been developed specifically with the risk, compliance, and controls assurance community in mind, but anyone interested in understanding how to evidence AWS controls will benefit.

Prerequisites

To complete this activity, you will need a .pdf reader, other than that there are no prerequisites and no assumed AWS knowledge for this activity. This is a great place to start for those new to AWS.

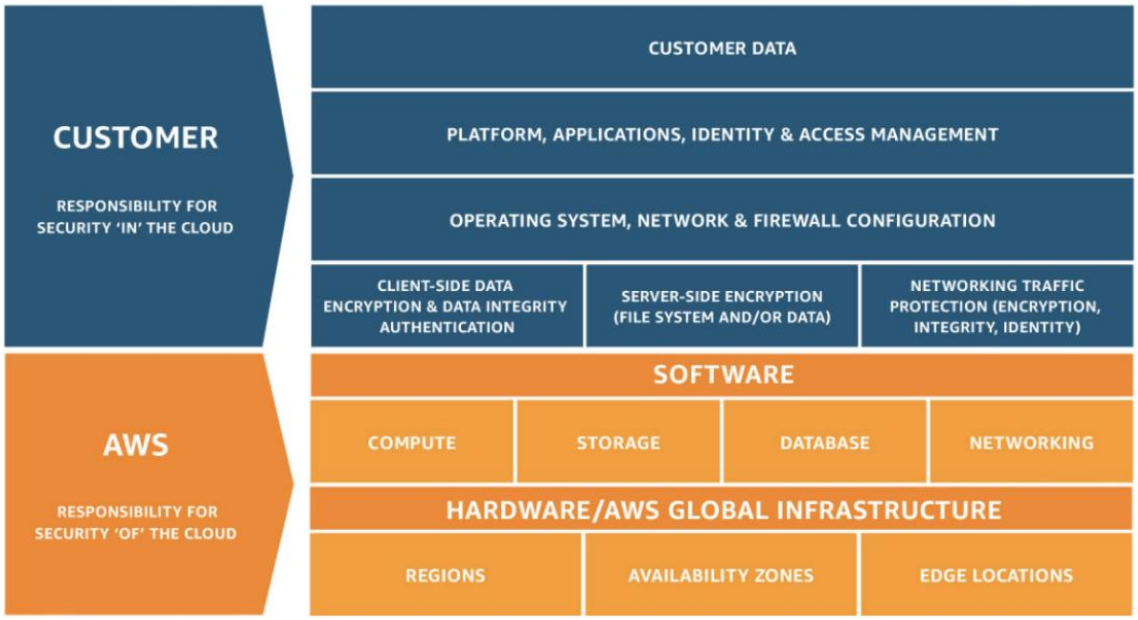
Steps

- Shared Responsibility
- Access a report
- Interpreting the results
- Deep Dive: Shared Responsibility

Shared Responsibility

Compliance is a Shared Responsibility

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall.



See the [Shared Responsibility Model] for more.

This activity focuses on introducing [AWS Artifact] and how customers can perform due-diligence using AWS' auditor issued reports. AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements.

Access a report

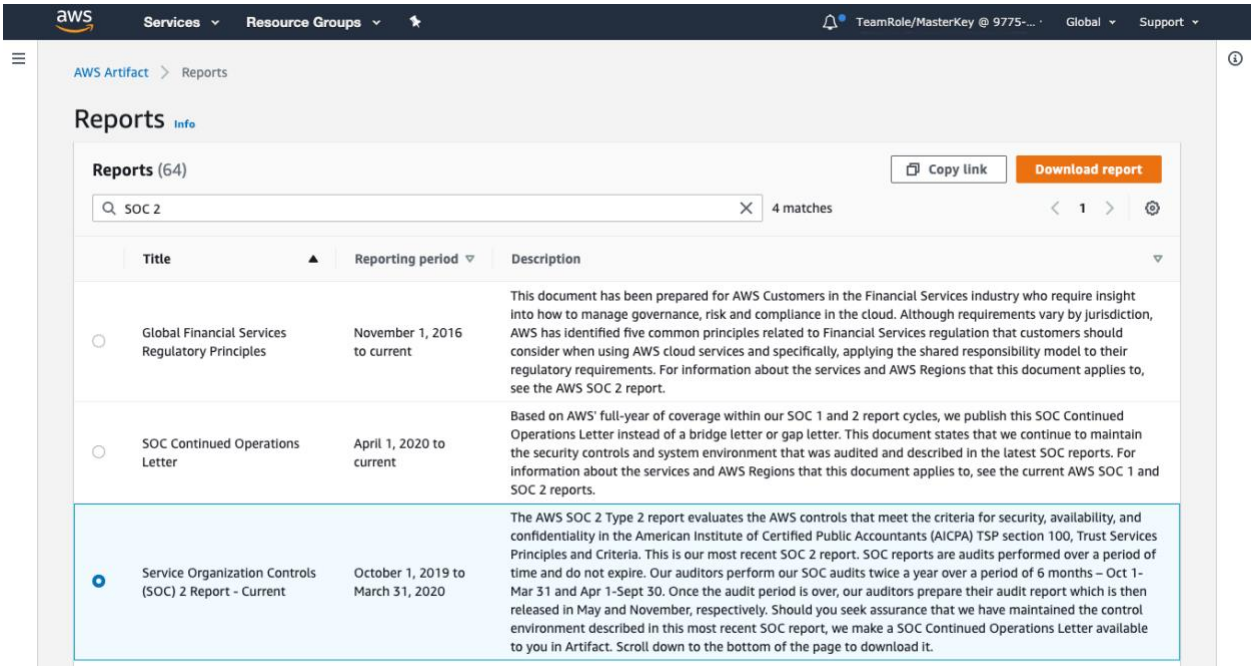
1. Access the AWS Artifact Console

From the Console, select the Services dropdown and **Artifact** under **Security, Identity, & Compliance**.

Click **View reports**

2. Download the SOC 2 Report

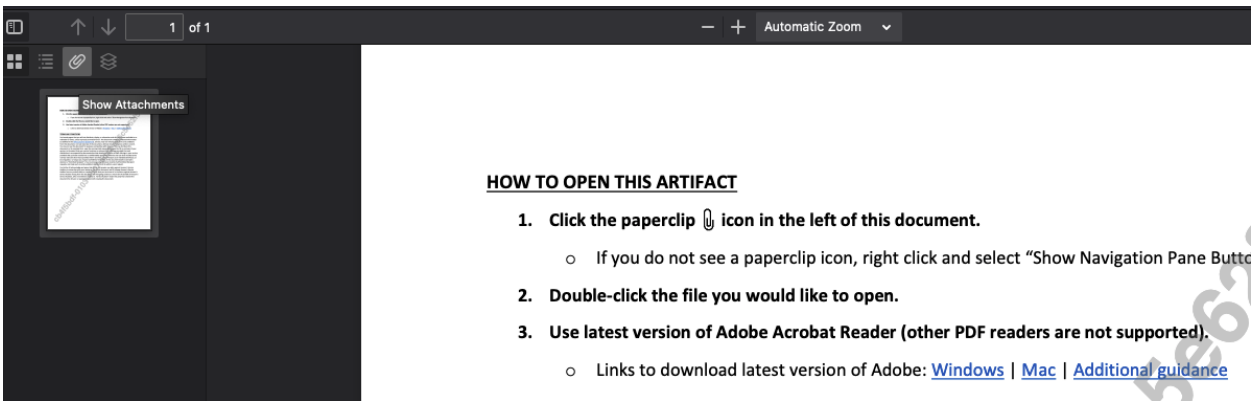
In this step we'll look at the Service Organization Controls (SOC) 2 Report.
As you can see reports available include our Service Organization Control (SOC), International Organization for Standardization (ISO), Payment Card Industry (PCI), and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

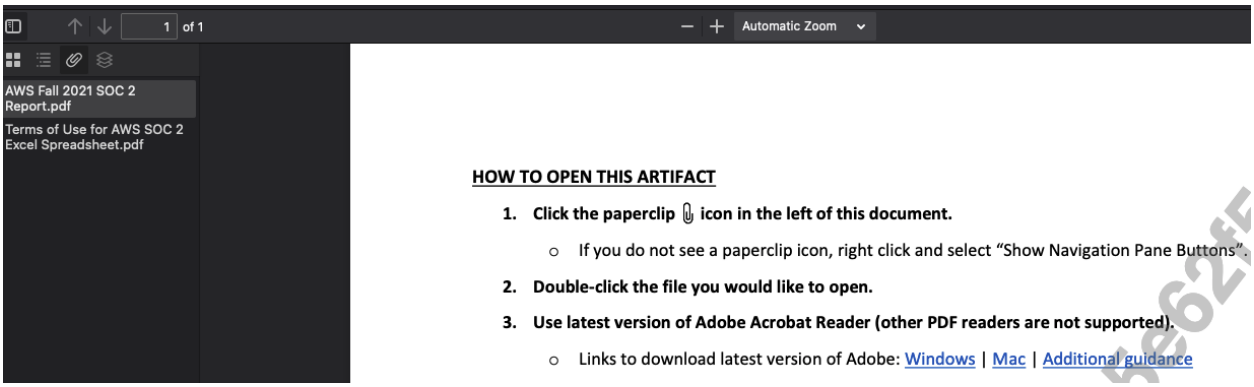


Enter "SOC 2" into the search and select SOC 2 Report - Current, then select **Download report**.
Read and accept the Non-disclosure Agreement (NDA).

3. Open the Report

Open your downloads folder and open the file
Review the Terms and Conditions of the artifact and click the paperclip icon to display the attachments on top left of PDF:





Open the first file in the list, the AWS SOC 2 Report.

The dates in the file name are the in-scope dates for the report.

SOC reports are audits performed over a period of time and do not expire. Our auditors perform our SOC audits twice a year over a period of 6 months: Oct 1 to Mar 31 and Apr 1 to Sept 30. Once the audit period is over, our auditors prepare their audit report which is then released in May and November, respectively. Should you seek assurance that we have maintained the control environment described in this most recent SOC report, we make a SOC Continued Operations Letter available to you in Artifact.

4. Review the Report

Take some time to review these independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives.

More information on our SOC compliance can be found at SOC Compliance

Interpreting the results

Now that you have a few minutes to review have the report, let's take a deeper look. First, we need to understand what the report covers, the overall conclusion, and the detailed results.

1. Completeness check

Under the *Scope* heading of *SECTION II – Independent Service Auditor's Assurance Report* there is a list of the AWS Services and Global Infrastructure Locations which are considered in scope, this can be used to validate that the services you use are in scope for the report.

2. Auditor opinion

Review the *Opinion* in *SECTION II – Independent Service Auditor's Assurance Report* which provides the Auditor opinion of the report.

3. The detailed results

SECTION IV – Description of Criteria, AWS Controls, Tests and Results of Tests contains tables mapping the Auditors Control Criteria to the AWS Control Activities (AWSCA) with the control assurance results. Readers can map these results to their own control requirements.

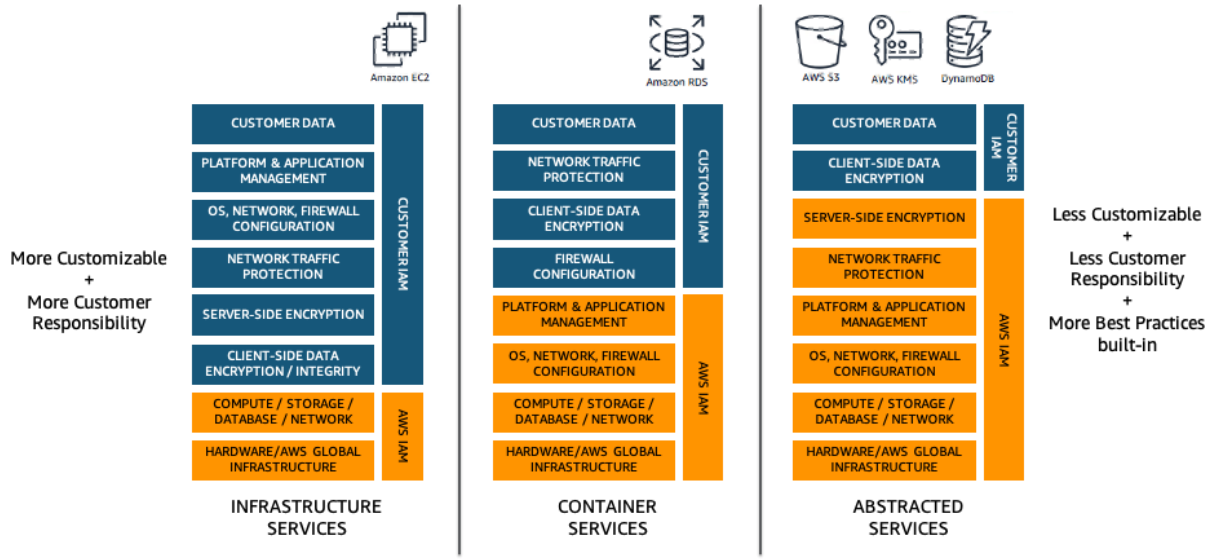
Congratulations!

You have accessed AWS Artifact, downloaded a SOC 2 Type 2 Report, and reviewed the results to confirm the controls that AWS operates on your behalf.

Deep Dive: Shared Responsibility

AWS groups services into three main categories: infrastructure, container, and abstracted. Each category comes with a slightly different security ownership model based on how customers interact and access the functionality. Customer responsibility is determined by the AWS Cloud

services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities.



Take advantage of AWS controls

Customers can take advantage of more abstracted services and shifting management of certain IT controls to AWS. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification as required.

Infrastructure Services

Services such as Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Virtual Private Cloud (Amazon VPC) are categorized as Infrastructure Services and, as such, require the customer to perform the necessary security configuration and management tasks. If a customer deploys an Amazon EC2 instance, they are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

Container Services

Container Services not 'Containers'

'Container services' is not to be mistaken with container technologies like Docker or Kubernetes.

Services in this category typically run separately on Amazon EC2 or other infrastructure instances, but sometimes customers are not required to manage the operating system or the platform layer. AWS provides a managed service for these application “containers”. Customers are responsible for setting up and managing network controls, such as firewall rules, and for

managing platform-level identity and access management separately from IAM. Examples of container services include Amazon Relational Database Services (Amazon RDS), Amazon Elastic Map Reduce (Amazon EMR) and AWS Elastic Beanstalk.

Abstracted Services

This category includes high-level storage, database, and messaging services, such as Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon DynamoDB, Amazon Simple Queuing Service (Amazon SQS), and Amazon Simple Email Service (Amazon SES). These services abstract the platform or management layer on which the customers can build and operate cloud applications. The customers access the endpoints of these abstracted services using AWS APIs, and AWS manages the underlying service components or the operating system on which they reside.

More Information

For more information refer to the Best Practices for Security, Identity, & Compliance page.

AWS also publishes security blogs related to best practices that covers best practices around using AWS services.