SOC 2 Audit for Amazon AWS Environments

With the migration to the cloud happening at record pace, thousands of companies are currently being needed to become SOC 2 compliant every year. In this blog, we will be touching upon the key areas and their importance from a SOC2 perspective related to Amazon Web Services (AWS) being used as a cloud platform.

SOC 2 Scoping & Readiness Assessment: Understanding scope and also the what business processes are to be enclosed inside your SOC 2 audit is important, and conjointly for mitigating any kind of scope related problems. Since you're hosting your services (i.e., your production environment) in AWS, it would have its own variety of advantages along with your SOC 2 audit.

- First, a wide range of the physical security controls are lined by AWS themselves as their personal information centers store your virtual server instances.

- Second, AWS incorporates a decent number of audit & compliance, and management tools & solutions that are straightforward to "spin up" in any surroundings, additional serving to compliance needs

Leverage AWS' SOC Reports for Scope Reduction: For the CPA firm you engaged with to perform your SOC 2 audit, they'll kindle you to get a replica of AWS' most current SOC 2 report, and for an obvious reason – scope reduction. A large range of the controls you'll want for SOC 2 compliance are literally lined by AWS' report. From physical and environmental controls –AWS' SOC 2 must be leveraged.

Utilize AWS's Security and Compliance Tools: CloudWatch logs reports on application logs, whereas CloudTrail Logs details on specific info on what occurred in your AWS account. These are simply some samples of the various tools that AWS has accessible for your growing security, governance, and regulative compliance desires.

Visit https://aws.amazon.com/products/security/ and you'll notice a list of tools and solutions for serving to meet growing regulative compliance desires for not solely SOC 2, but HIPAA, HITRUST, GDPR, PCI DSS, FISMA, and far a lot of. Here may be a sneak peek at the various tools accessible for from AWS in serving to with growing regulative compliance needs:

- **AWS object:** The AWS object portal provides on-demand access to AWS' security and compliance documents, conjointly referred to as audit artifacts.

- **AWS Certificate Manager:** AWS Certificate Manager may be a service that permits you to simply provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates.

- **AWS CloudHSM:** The AWS CloudHSM service helps you meet company, written agreement and regulative compliance needs for information security by mistreatment dedicated Hardware Security Module (HSM) appliances inside the AWS cloud.

- **Amazon Cognito:** Amazon Cognito permits you to add user sign-up/sign-in and access management to your net and mobile apps quickly and simply.

- **AWS Identity and Access Management (IAM)**: Use AWS Identity and Access Management (IAM) to regulate users' access to AWS services. Produce and manage users and teams, and grant or deny access.

There are more tools accessible from AWS once it involves security & compliance, therefore use them as required. They'll build life within the cloud and they'll build your SOC 2 audit much easier.

Implement the Tools: Sounds simple, however we'll got to with courtesy prompt you that simply knowing that such tools are accessible isn't enough, you would like to place them to smart use as auditors can wish to envision proof of such. If you're not aware of AWS in terms of their toolsets and offerings for regulative compliance, then it's necessary to search out for AWS security & compliance.

Develop AWS info Security Policies and Procedures: One among the foremost aspects of turning into SOC 2 criticism is developing all the specified info security policies and procedures. Specifically, SOC 2 is significant on documentation, and you'll have to be compelled to place in situ strong, literary InfoSec policies. However a lot of necessary, these policies have to be compelled to be written specifically for your surroundings inside AWS.

Here's simply a little sample of policy documents you'll want for turning into SOC 2 compliant:

- Access management
- Information backup
- Incident response
- Information retention and disposal
- Security and patch management – and many more.

Perform Essential Operational Initiatives: Four key operational initiatives that you simply should perform for SOC 2 compliance are:

- Perform annual risk assessment
- Check your incident response annually
- Implement security awareness coaching
- Conduct vulnerability scans periodically

The Audit Begins: The auditors are going to be inquiring for a wide range of evidences. Specifically, they'll be requesting documentation (i.e., policies and procedures), proof of varied system settings (this can are available the shape of screenshots), proof of operational measures undertaken, like security awareness coaching, risk assessments, and more. It's therefor essential to produce them with any and every one requests that return your means. In short, be clear along with your auditors.

We believe this the article would have enhances your understanding of AWS controls from a SOC2 perspective. Please reach out to us if you would like to know more about data security or need any help to perform a SOC/ GDPR certification for your organization.

Visit our website https://accorppartners.com/soc/index.php to read more articles related to SOC reporting.