Title: Planning AWS Platform Security Assessment ?

Name: Rajib Das

IOU: Cyber Security Practices

TCS Emp ID: 231462

Introduction

Now-a-days most of the customers are working in AWS platform or planning to migrate their existing physical Infrastructure to Cloud. AWS Cloud is the most popular among the Cloud vendors available in the market.

Once your Infrastructure migrated and settled as Business as Usual into Cloud then your next major concern is to complete security assessment for AWS ready Infrastructure. Assessors need not only to understand how the cloud works, but additionally how to leverage the power of cloud computing to their advantage while conducting assessments.

Security in the Cloud is the responsibility for customer. So you are responsible for

- Assets securities in the cloud
- Implementation of cloud security controls
- Compliance in the cloud (e.g- PCI-DSS, ISO 27018/27017/27001/9001, SOC)

Security of the Cloud is the responsibility of AWS. So AWS is responsible for

- Security of the cloud
- Host OS
- Virtualization Layer
- Physical security
- Compliance in the cloud

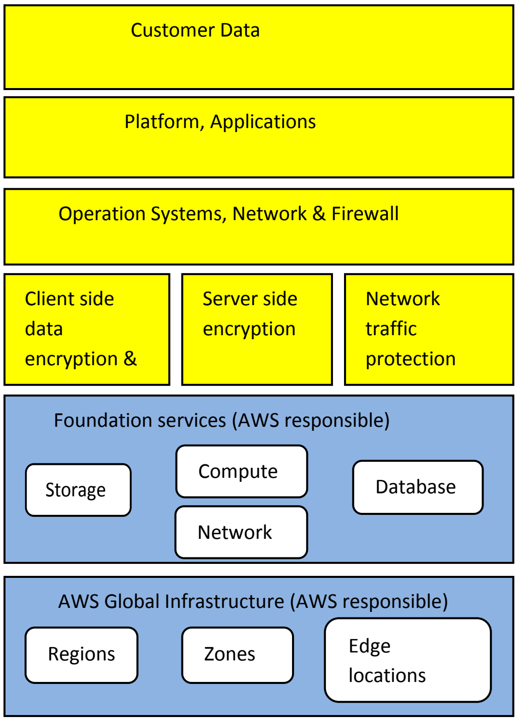
Customer Data
Platform, Applications
Operation Systems, Network & Firewall
Client side data encryption &
Server side encryption
Network traffic protection
Foundation services (AWS responsible)
Storage
Compute
Network
Database
AWS Global Infrastructure (AWS responsible)
Regions
Zones
Edge locations

Diagram 1: Shared Responsibility Model

Security assessment starts with identifying asset details.

- Instances
- Data Stores
- Applications
- Data

For AWS Infrastructure security assessment program security control objectives remains consistent.

- Pre assessment Tasks
  - Understanding AWS service uses within organization

    This include Interviewing IT department, Review expense reports and purchase order payments related to understand what services are in use

  - Determine AWS assessment objectives

    This includes review/modification of your assessment objectives to align with assessment program, plan and charter.

- Understanding AWS boundaries or review

  This includes your core business process alignment with IT, AWS services and business solution review obtain previous assessment report for remediation plan

- Pre-assessment tasks also include specific steps to risk assessment

  - Identify risk: This task determine whether risk assessment for the applicable already being performed.
  - Review risk & treatment plan: This task involves review of risk assessment report to determine residual risk in current environment. Also treatment plan and timeline should be reviewed against risk management policies and procedure.
  - Incorporate AWS in risk assessment: This include identification of business risk associate with AWS and business owners and key stake holders. Finally review and evaluation of overall risk factor for AWS review.

AWS Environment Security Assessment Checklist

Checklist Category	Description	Assessment Guideline
Logical access controls	AWS Cloud Trail review for unauthorized access. Cloud Watch logs monitoring for AWS resource monitoring Review of IAM Policies, S3 Bucket Policies, Security Groups, Network Access Control Lists, and Routing Table to identify unauthorized access. Review connectivity between organizations network and AWS along with VPN Connection between VPC and organizations network.	Ensure AWS assets are managed as per organizational policies, procedures. You can use AWS Trusted Advisor to validate IAM Users, Groups, and Role configurations details
Physical & Environmental Security Controls	AWS evidence details for the intrusion detection & protection of information processes must be reviewed which is managed by AWS physical security controls.	You need to evaluate third-party attestations like SOC certifications to gain reasonable design and operating effectiveness for this control.
Data encryption	Review of connection for AWS Console, management API, S3, RDS and Amazon EC2 VPN in terms of encryption. Ensure internal policies and procedures for key management for AWS services and EC2 Review AWS offered various encryption methods for key protection (KMS, CloudHSM etc)	Data at rest, at transit should be encrypted. Lack of proper data protection could create a security exposure. AWS trusted advisor can be used to verify permission for access data
Security logging and monitoring	Customer must use cloud watch & cloud trail For monitoring apps performance and assessment logs You must use IAM credentials report to identify unauthorized users Use VPC flow logs to identify accepted/rejected traffic Use ELB logging for load balancer logging AWS cloud front logging for logging of CDN distribution Review HIDS EC2 instances	Ensure assessment logging is being performed on the guest OS and critical applications installed on EC2 instances are in alignment with your policies and procedures.
Incident management & response	Ensure Cyber security plan & procedure must include AWS proper services to mitigate risks	You should understand incident response responsibilities by the use of existing security monitoring/alerting/assessment tools based and processes for their AWS resources. Security events should be monitored regardless of where ever assets resides

Disaster recovery	Ensure use of existing incident monitoring tools and use of AWS available To verify that Incident Response Plan goes through periodic review. Evaluate Incident Response Plan has notification procedures on and how the Customer addresses responsibility of losses associated with attacks.	Customer must ensure they must configure AWS services for high tolerance and high availability DR solution with minimum recovery time objective by using multiple zones and region based solutions. AWS trusted advisor services can be used for optimal performance and low cost solutions

AWS built-in Security Assessment Services

AWS built-in security assessment service	Features	Benefits
Amazon Inspector	Amazon Inspector provides built in engine for analysis of systems and resources configuration. It also incorporate built in library rules and best practices for meeting compliance standard and vulnerabilities.	It allows you to automate security assessment of your infrastructure. It produces findings of some real-time analysis of AWS resources configuration status which allow you to gain deeper understanding
Amazon WAF (web application firewall)	It is a web application firewall that allows you to monitor the HTTP/HTTPS requests traffic which are forwarded to Amazon Cloud Front. It also allows you to control access to your content based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings,	It can protect against web attacks by using conditions that you specify. You can filter based some characteristics • IP addresses request originate country, value in the request header and string • Presence of SQL code that may be malicious (known as SQL injection). • Presence of a script that may be malicious (known as cross-site scripting)
Amazon Macie	Amazon Macie is a security service automatically discovers, classify, and protect sensitive data in AWS. Macie recognizes identify data such as personally identifiable information (PII) or intellectual property (IP) and alert you for the visibility into how this data is being accessed or moved. Currently US East (Northern Virginia) & US West (Oregon) regions supported by this service	Identification & protection of PII, PHI, API keys, secret keys regulatory documents. Identification of access control and policy changes logs. Setup alert notification if data & account credentials cross protected zones Detection of data privacy content as per compliance requirement if a bulk quantities of business-critical documents needed to shared internally and externally
Amazon GuardDuty	It is continuous security monitoring tools to analyze VPC Flow Logs, AWS CloudTrail event logs, and DNS logs data sources. It can identify unexpected and unauthorized and malicious activity within your AWS	It can detect if EC2 instances compromised. GuardDuty also monitor AWS account access pattern for signs of compromise like unauthorized infrastructure deployments, or unusual API calls, like a password policy change to reduce password strength.

Conclusion: As AWS customers have complete control over their operating systems, network settings, storage and database part, so majority of existing platform in house tools can be utilized to assess services in AWS. Apart from the above security assessment services, AWS also introduced some built-in security services like AWS shield, AWS single sign-on, Amazon cognito, AWS directory services, AWS organizations, AWS Cloud HSM, AWS certificate manager and many more for security, risk and compliance assessment.

Reference:

1. https://aws.amazon.com/compliance/ (Amazon's Compliance program web document)

2. https://aws.amazon.com/products/security/?nc2=h_l3_db (Amazon's Security, Identity, and Compliance Products web document)

3. https://www.lynda.com/MyPlaylist/Watch/16009251/692285?autoplay=true (Lynda AWS security Video training module)