## Lab Objective and Due Date:

Understand and implement cloud security governance best practices in an AWS environment. This lab assignment is due on **February 19, 2024.**

## Pre-Lab Setup:

1. AWS Account Setup
2. [Resource Allocation](https://aws.amazon.com/getting-started/hands-on/control-your-costs-free-tier-budgets/): Assign budget limits and monitor usage to prevent unexpected costs.

## Lab Exercise:

### Part 1: Understanding AWS Security and Compliance

1. Enable AWS Security Hub. **Provide a screenshot of Security Hub active in your environment.**

A screenshot of a computer

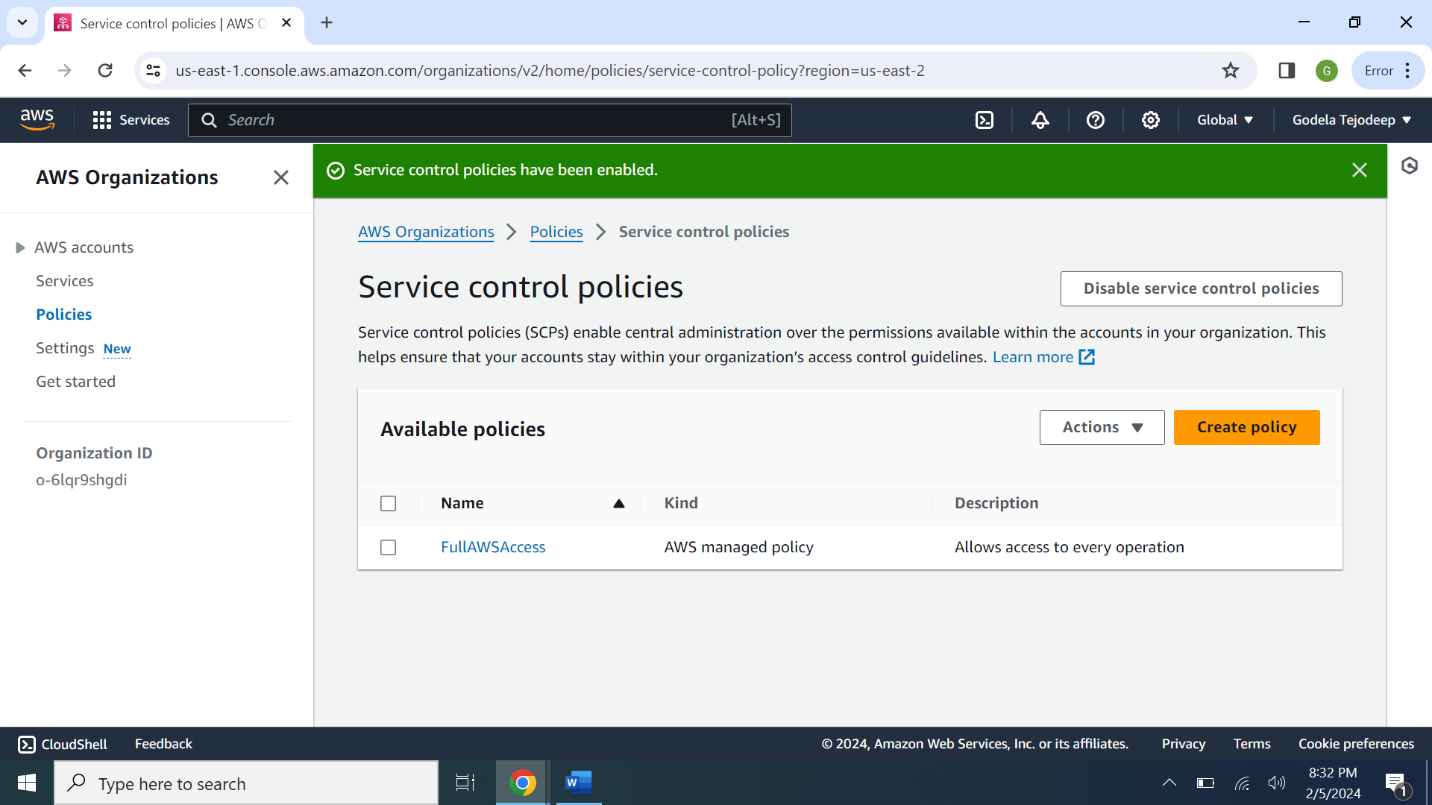
Description automatically generated

1. Create an AWS Service Control Policy that only allows users to create EC2 instances and S3 buckets in the US East 1 region.

A screenshot of a computer

Description automatically generated

1. Create a user that is able to set up EC2 instances. Log in as that user and create an EC2 instance. Provide a screenshot of **the user you created** and **the EC2 instance you created.**



A screenshot of a computer

Description automatically generated

1. Using that same user, switch to any region other than US East 1 and try to create an EC2 instance. **Provide a screenshot of the error you receive when you do this.**

A screenshot of a computer

Description automatically generated

1. Review AWS Artifact. **Provide a screenshot of the AWS Artifact interface.**

A screenshot of a computer

Description automatically generated

**Contd……..**

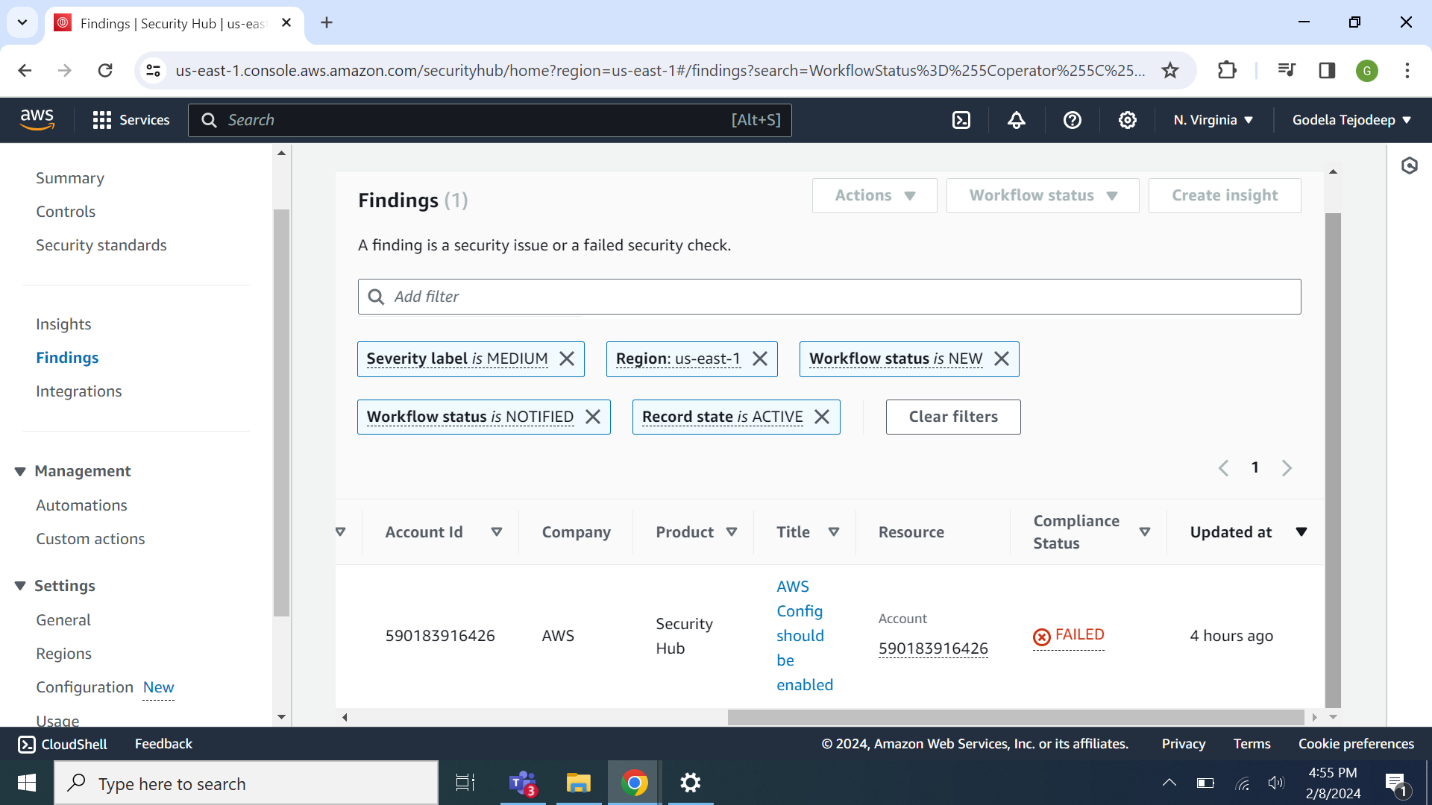
### Questions to Answer:

1. What is the benefit of AWS Security Hub? Why should companies enable this service?

**Answer:** Security standards enables the user to track your cloud security posture with a summary security score and standard security scores

In this lab we enforced 2 security standards namely

* **AWS Foundational Security Best Practices v1.0.0**
* **CIS AWS Foundations Benchmark v1.2.0**



In the above screenshot as I entered password incorrect you can see in compliance status and considered critical

A screenshot of a computer

Description automatically generated

1. What is the benefit of AWS Service Control Policies? How do they help companies manage governance and compliance?

**Answer:** AWS Organizations is a service for grouping and centrally managing multiple AWS accounts. A service control policy (SCP) limits permissions for entities in member accounts in AWS Organizations.

Basically creating a dashboard of services to the user working on a particular region enabling us to implement LPP[Least Privilege Policy] Access management. So the user can login from any part of the globe he can work on those services explicitly in that region like EC2 Instances,S3 Buckets

A screenshot of a computer

Description automatically generated

1. Why do companies use AWS Artifact?

**Answer:** Reports are documents that AWS has made available on-demand to the customers. Some reports are available to all customers while others are available only to select customers depending on need-to-know basis.

A screenshot of a computer

Description automatically generated

<https://docs.aws.amazon.com/artifact/latest/ug/what-is-aws-artifact.html>

A screenshot of a computer

Description automatically generated

An example like You can also use AWS Artifact to review, accept, and track the status of AWS agreements such as the Business Associate Addendum (BAA). A BAA typically is required for companies that are subject to the Health Insurance Portability and Accountability Act (HIPAA) to ensure that protected health information (PHI) is appropriately safeguarded.