Compliance Automation Framework using AWS Config and Systems Manager (SSM)

# Project Objective

The goal of this project is to build a Compliance Automation Framework using AWS Config and Systems Manager (SSM) that not only detects policy violations but also remediates them automatically using SSM automation runbooks—securely, reliably, and with traceability. The framework also includes alerting, auditing, and weekly compliance reporting.

# What We Did in This Project

1. Created test resources (EC2 instances, S3 buckets, IAM policies) to simulate compliance violations.

2. Enabled AWS Config to continuously monitor resources for compliance.

3. Created IAM roles with necessary permissions for automation and reporting.

4. Built SSM Automation runbooks in YAML for auto-remediation of violations.

5. Linked AWS Config rules with SSM runbooks to remediate violations automatically.

6. Set up Amazon SNS for compliance alerts.

7. Built a Lambda function for weekly compliance reports and scheduled it with EventBridge.

8. Validated the framework with five compliance scenarios.

# AWS Services Used

Amazon EC2: Used to create instances and test compliance scenarios (open SSH, missing tags).

Amazon S3: Stores AWS Config logs, CloudTrail logs, compliance reports, and test for unencrypted bucket scenario.

AWS Config: Detects resource compliance violations continuously based on managed rules.

AWS Systems Manager (SSM): Hosts Automation Documents (runbooks) to remediate violations automatically.

AWS Lambda: Generates weekly compliance reports and stores them in S3.

Amazon SNS: Sends alerts and notifications when remediations occur.

AWS CloudTrail: Provides audit logs and traceability of all API calls.

# Steps Followed

**Step 1:** Create baseline resources

* EC2 instances (one with missing tags, one normal)
* S3 bucket
* CloudTrail trail (logs to S3)
* SNS topic for alerts.

**Step 2:** Enable AWS Config

* Record all resources.
* Store snapshots in S3.
* Send notifications to SNS.

**Step 3:** Create IAM roles

* **SSM Automation Role** → used by runbooks.
* **Config Remediation Role** → triggers automation.
* **Lambda Report Role** → generates compliance reports.

**Step 4:** Build SSM runbooks (Automation Documents)

* Scenario 1: Remove open SSH from Security Groups.
* Scenario 2: Enable default encryption on S3.
* Scenario 3: Add missing EC2 tags.
* Scenario 4: Ensure CloudTrail is logging.
* Scenario 5: Quarantine over-permissive IAM policies (approval required).

**Step 5:** Create AWS Config rules + remediation

* Link each **managed rule** with its corresponding SSM runbook.
* Map parameters (e.g., SecurityGroupId, BucketName).
* Enable auto-remediation.

**Step 6:** Build compliance reporting

* Lambda function generates weekly compliance reports.
* Stores reports in S3, sends alerts via SNS.
* EventBridge schedules weekly execution.

**Step 7:** Test scenarios

* Open SSH → auto-removed.
* Unencrypted S3 → encryption enabled.
* Missing EC2 tags → tags added.
* CloudTrail stopped → restarted automatically.
* Over-permissive IAM policy → detached after approval.

# References

• AWS Config Documentation: https://docs.aws.amazon.com/config/

• AWS Systems Manager Documentation: https://docs.aws.amazon.com/systems-manager/

• AWS Lambda Documentation: https://docs.aws.amazon.com/lambda/

• Amazon SNS Documentation: https://docs.aws.amazon.com/sns/

• AWS CloudTrail Documentation: https://docs.aws.amazon.com/cloudtrail/

# Screenshots (Sample)



