PRJ-SEC-011: Compliance Automation & Continuous Auditing

Author: Mo Suleiman | **Project:** PRJ-SEC-011 | **Certification:** AWS Certified Security – Specialty

1. Project Overview

This project implements a powerful, automated framework for continuous compliance monitoring and auditing. Manual compliance checks are slow, error-prone, and cannot keep up with the dynamic nature of the cloud. This project demonstrates how to codify your compliance requirements and automate their enforcement and reporting.

We use **AWS Config** as the core engine to track resource configurations and evaluate them against desired policies. We deploy a **Conformance Pack** for a standard framework (CIS AWS Foundations Benchmark) to quickly establish a baseline. For non-compliant resources, we use **AWS Systems Manager Automation** documents to perform automated remediation. Finally, we integrate with **AWS Security Hub** for unified dashboarding and **AWS Audit Manager** to continuously collect evidence and generate audit-ready reports.

GRC Mapping

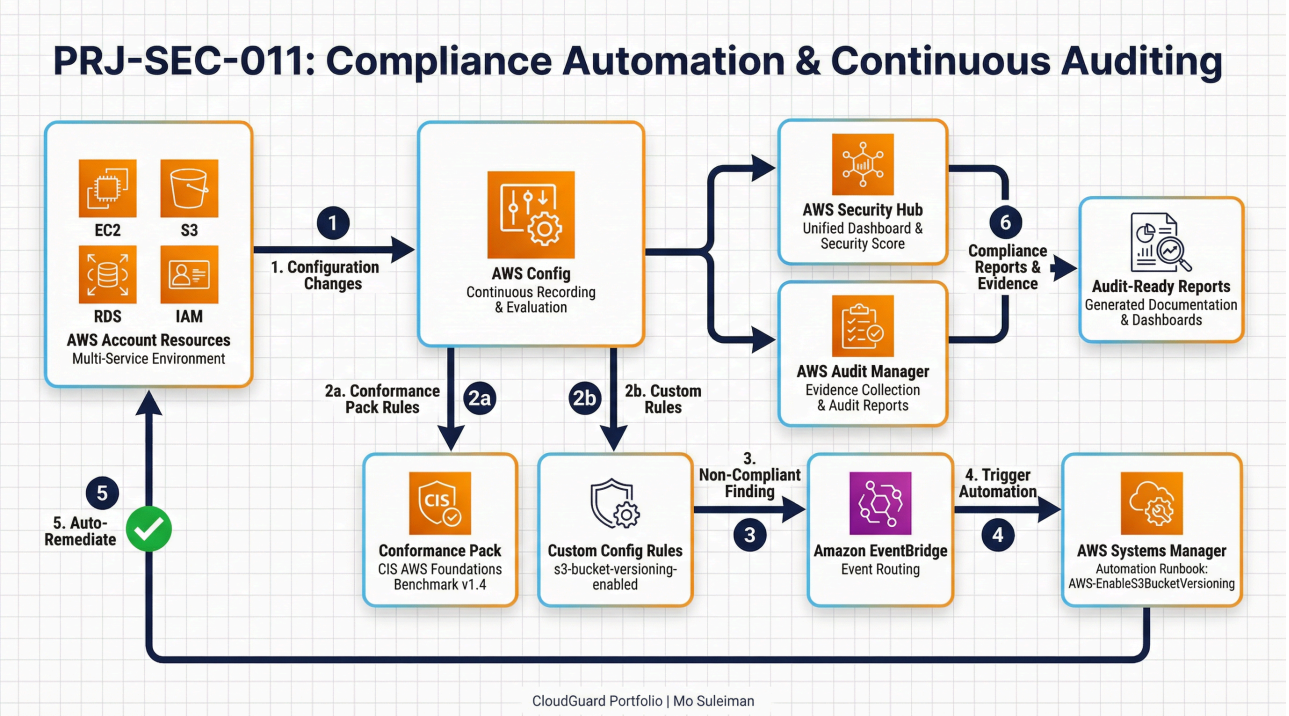
Framework	Control	Description
CIS Benchmark	v1.4.0	Establishes secure configuration baselines for AWS services.
PCI-DSS	Req. 10.2	Implement automated audit trails for all system components.
HIPAA	§ 164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity.
NIST CSF	DE.CM-8	Vulnerability scans are performed, and configuration management is automated.
ISO 27001	A.12.4.1	Event logging and monitoring of user activities, exceptions, and faults.
Business Value	—	Eliminates manual audit preparation, reduces non-compliance windows from months to minutes, and provides a real-time view of organizational security posture.

Architecture Components

Component	Service	Purpose
Configuration Tracking	AWS Config	Continuously monitors and records AWS resource configurations.
Compliance Baseline	AWS Config Conformance Pack	Evaluates resources against the CIS AWS Foundations Benchmark.
Automated Remediation	AWS Systems Manager	Executes Automation Runbooks to fix non-compliant resources.
Event Routing	Amazon EventBridge	Triggers SSM Automation when Config detects non-compliance.
Unified Dashboard	AWS Security Hub	Aggregates compliance findings and calculates a security score.
Evidence Collection	AWS Audit Manager	Automates evidence gathering and generates audit-ready reports.

---

2. Architecture Diagram



Workflow Steps:

1. **Continuous Monitoring:** AWS Config continuously discovers and records configuration changes for all supported AWS resources.
2. **Evaluation:** AWS Config evaluates changes against the deployed Conformance Pack (CIS Benchmark) and custom rules (e.g., S3 versioning).
3. **Flag Non-Compliance:** When a resource is non-compliant, AWS Config flags it and generates an EventBridge event.
4. **Automated Remediation:** EventBridge triggers an AWS Systems Manager Automation document (e.g., `AWS-EnableS3BucketVersioning`).
5. **Auto-Remediate:** The Automation document executes API calls to fix the non-compliant resource automatically.
6. **Auditing and Reporting:** AWS Security Hub provides a consolidated dashboard, while AWS Audit Manager continuously collects evidence to generate one-click audit reports.

---

3. Prerequisites

Before starting, confirm the following:

- You are logged into the AWS Console with an IAM user or role that has `AdministratorAccess`.
- You have permissions to manage AWS Config, Systems Manager, EventBridge, Security Hub, Audit Manager, and IAM.
- Your region is set to **us-east-1**.
- You have enabled AWS Organizations (recommended for Security Hub and Audit Manager centralized management, though not strictly required for a single-account lab).

---

4. Step-by-Step Deployment Guide

Step 4.1: Enable AWS Config and Security Hub

1. **Enable AWS Config:**
    - Navigate to the **AWS Config** console.
    - If it's your first time, click **1-click setup**. This creates a configuration recorder, a delivery channel, and an S3 bucket.
    - Ensure that **Include global resources (e.g., IAM resources)** is checked.
    - *Note: If creating the S3 bucket manually, it must follow standard S3 naming conventions and have a bucket policy allowing Config to write to it.*
2. **Enable AWS Security Hub:**
    - Navigate to the **AWS Security Hub** console and click **Enable Security Hub**.
    - Under **Security standards**, ensure **CIS AWS Foundations Benchmark v1.4.0** is enabled.
    - In **Settings -> Integrations**, ensure that `AWS Config` is enabled as a provider (this usually happens automatically).

Step 4.2: Deploy a Conformance Pack

1. Go to **AWS Config -> Conformance packs -> Deploy conformance pack**.
2. Choose the **CIS AWS Foundations Benchmark v1.4.0** template.
3. **Conformance pack name:** `CIS-Benchmark-Pack`.
4. Click **Next** and **Deploy**.
5. AWS Config will deploy dozens of rules. This takes 15-20 minutes. You can view the compliance status on the pack's detail page.

Step 4.3: Create a Custom Config Rule

1. Go to **AWS Config -> Rules -> Add rule**.
2. In the filter box, type `s3-bucket-versioning-enabled` and select the AWS-managed rule.
3. Review the details and click **Next** then **Add rule**.

Step 4.4: Configure Automated Remediation via Systems Manager

1. Go to **AWS Config -> Rules** and select the `s3-bucket-versioning-enabled` rule.
2. Click **Actions -> Manage remediation**.
3. **Remediation method:** Automatic remediation.
4. **Remediation action:** Choose `AWS-EnableS3BucketVersioning`.
5. **Resource ID parameter:** `BucketName`.
6. **Parameters:**
    - `BucketName`: Leave blank (auto-filled by the finding).
    - `AutomationAssumeRole`: You must provide the ARN of an IAM role that allows SSM to enable S3 versioning.
        - *To create this role:* Go to IAM -> Roles -> Create Role. Select **Systems Manager** as the trusted entity. Attach the `AmazonS3FullAccess` policy (or a custom policy scoped to `s3:PutBucketVersioning`). Copy the Role ARN and paste it into the `AutomationAssumeRole` field in Config.
7. Click **Save changes**.

Step 4.5: Test the Remediation

1. Go to the **S3 console** and create a new bucket named `test-compliance-remediation-<your-initials>`.
2. **Do not enable versioning** during creation.
3. Wait 5-10 minutes. AWS Config will detect the non-compliant bucket.
4. The Config rule will trigger the Systems Manager Automation document.
5. Refresh the S3 console properties for your bucket — **Bucket Versioning** will now be enabled.
6. View the execution history in **Systems Manager -> Automation**.

Step 4.6: Automate Evidence Collection with AWS Audit Manager

1. Go to the **AWS Audit Manager** console and complete the one-time setup.
2. Go to **Framework library** and select **CIS AWS Foundations Benchmark v1.4.0**.
3. Click **Create assessment from this framework**.
4. **Name:** `CIS-Quarterly-Assessment`.
5. **AWS accounts:** Select your account.
6. **AWS services:** Leave the pre-selected in-scope services. Click **Next**.
7. **Audit owners:** Select your IAM user. Click **Create assessment**.
8. Audit Manager will continuously collect evidence. Wait up to 24 hours for initial data.
9. To generate a report: Open your assessment, review the control sets, and click **Generate assessment report**. This creates a zip file with a summary PDF and all evidence.

---

5. Cleanup

To avoid ongoing charges, delete the resources in this order:

1. **S3:** Delete the `test-compliance-remediation` bucket.

2. **AWS Config:** Go to the `s3-bucket-versioning-enabled` rule and remove the remediation action, then delete the rule.
3. **AWS Config:** Delete the `CIS-Benchmark-Pack` Conformance Pack.
4. **AWS Config:** Stop the configuration recorder in Settings.
5. **Audit Manager:** Delete the assessment and disable Audit Manager in Settings.
6. **Security Hub:** Disable Security Hub in Settings.
7. **IAM:** Delete the AutomationAssumeRole you created.