



Secure AWS Multi-Account Baseline

***Terraform +
Policy-as-Code***

***Portfolio
by Amina Jiyu An
Github:***

<https://github.com/amina0806>

Executive Summary

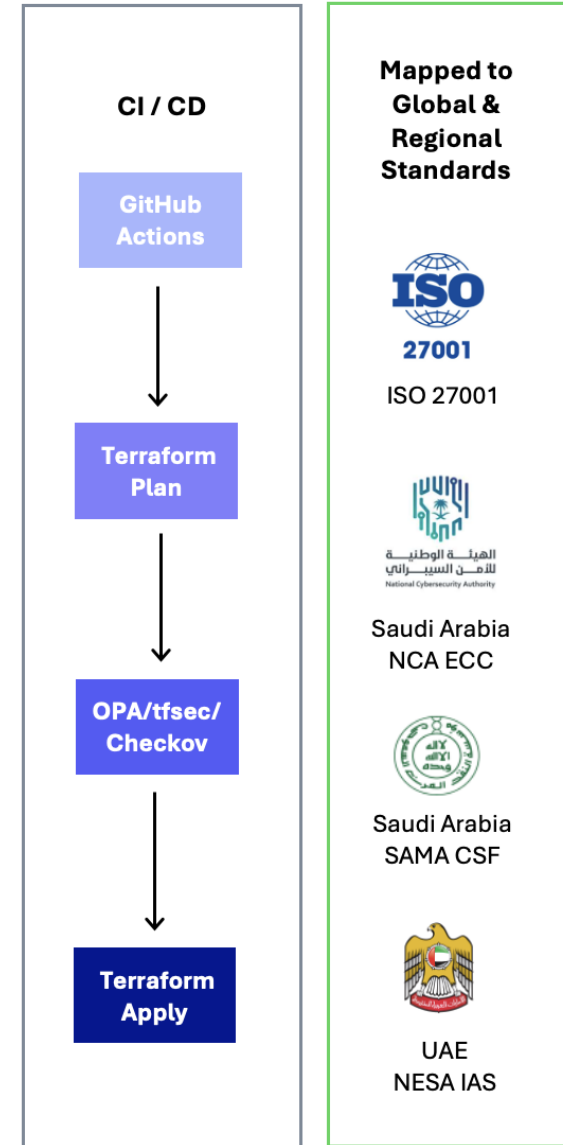
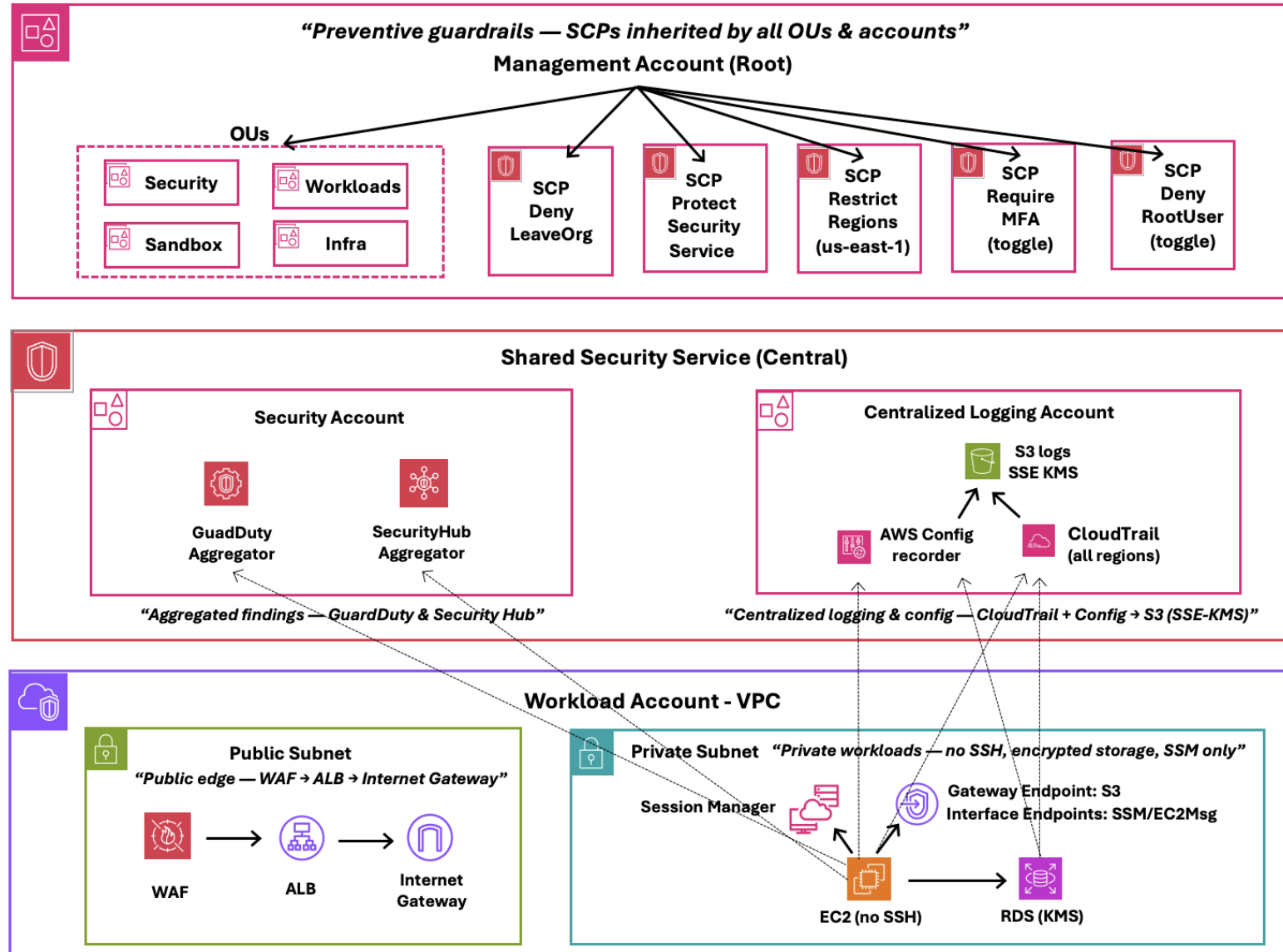
Enterprise AWS Secure Baseline (Terraform + Policy-as-Code)

“This is not theory. Every slide is a proof I built, validated, and enforced in AWS.”

This portfolio demonstrates how I designed and enforced a secure AWS environment at **enterprise scale**, combining preventive, detective, and governance controls. Every component is mapped to **international and regional compliance frameworks** (ISO/IEC 27001, Saudi NCA ECC, Saudi SAMA CSF, UAE NESAS IAS), proving awareness of both global standards and local regulatory requirements.

Multi-account Governance	Centralized Logging Encryption	Compliance Mapping	Threat detection & CSPM	Policy-as-Code (OPA,tfsec,Checkov)
Multi-account governance with AWS Orgs & SCPs) → ISO 27001 A.5.1, NCA GOV-02, NESAS GOV-01.	CloudTrail + S3/KMS logs → ISO 27001 A.12.4/8.15 NCA LGM-02 NESAS MON-01	AWS Config Conformance Packs → ISO 27001 A.12.1/5.14 NCA CC-06 NESAS AUD-02	GuardDuty + Security Hub → ISO 27001 A.12.6/8.8 NCA D5.5 NESAS MON-05	Enforce encryption & IAM boundaries → ISO 27001 A.14.2/8.28 NCA D3.2 NESAS DEV-01

Architecture Diagram



Preventive = SCPs • Detective = CloudTrail/Config/GD/SecHub • Foundational = VPC+Encryption+SSM • Governance = Terraform+OPA

Validated against
ISO 27001, Saudi NCA, SAMA CSF, UAE NESAS controls

Step1: State Backend

What this proves

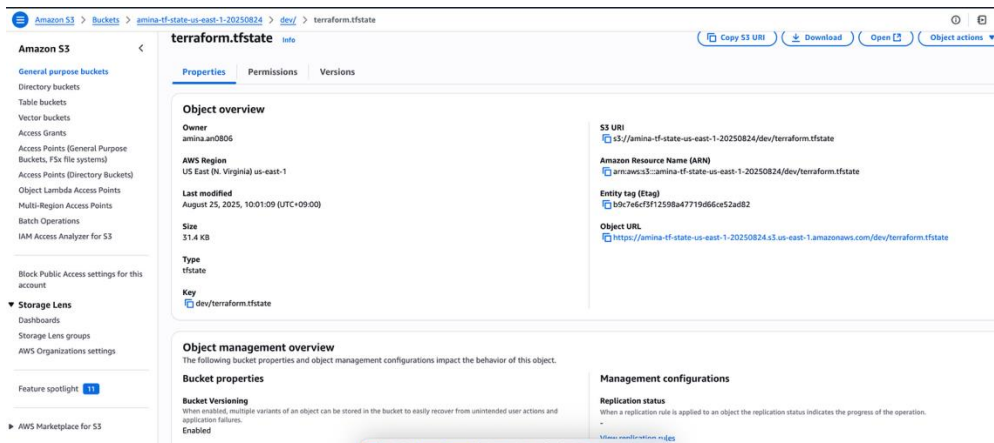
- Secure Terraform state management across accounts.
- **Encryption (SSE-KMS)** protects state confidentiality.
- DynamoDB locking prevents concurrent writes / corruption.

Controls

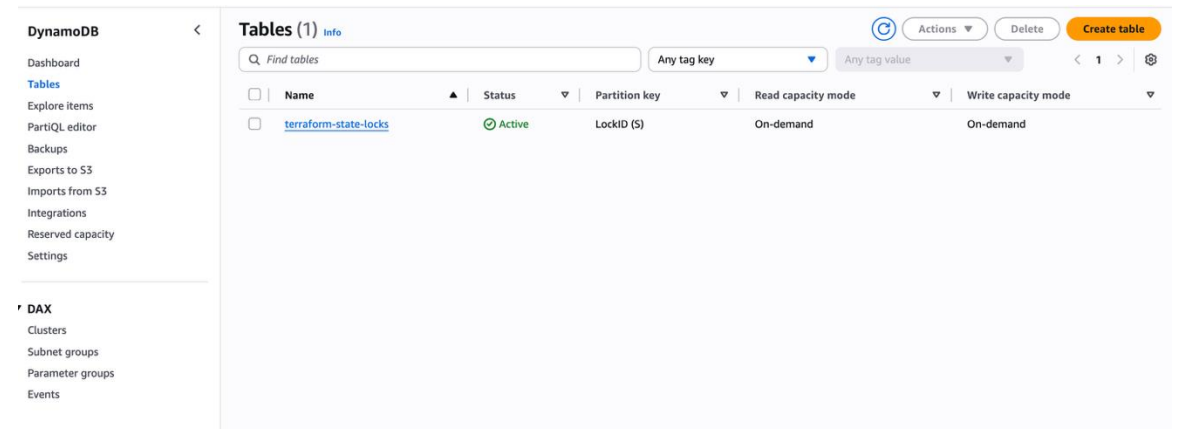
- **ISO 27001:** A.8.20, A.8.23, A.8.16 → 2022: 8.24, 5.23, 5.15

Proofs / Screenshots

S3 bucket (SSE-KMS enabled)



DynamoDB state locking



Note: Ensures **tamper-resistant, segregated state** → critical for enterprise IaC.

Step2: Centralized Logging

What this proves

- Enterprise-wide **visibility** into all AWS activity.
- CloudTrail & AWS Config logs are **centralized, encrypted, immutable**.
- S3 bucket with **KMS CMK + versioning** → no accidental/intentional log deletion.

Controls

- **ISO 27001:** A.12.4 → 2022: 8.15
- **Saudi NCA:** D1 Logging & CC-06 Compliance
- **SAMA CSF:** LOG (Logging & Monitoring), COM (Compliance)
- **UAE NES:** MON-01

Proofs / Screenshots

Log bucket encryption (SSE-KMS)

The screenshot shows the Amazon S3 console interface for a bucket's 'Default encryption' settings. The 'Encryption type' is set to 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)'. The 'Encryption key ARN' is displayed as `arn:aws:kms:us-east-1:958006149724:key/mrk-27d3409cf7c04b4ea998f16c7ae654a0`. The 'Bucket Key' is also shown as 'Enabled'. Below this, there are 'Intelligent-Tiering Archive configurations (0)' with buttons for 'View details', 'Edit', 'Delete', and 'Create configuration'. A search bar for configurations is also visible.

CloudTrail Logs in S3

The screenshot shows the 'Objects (21)' view in the Amazon S3 console. It displays a list of objects, including CloudTrail logs. The table has columns for Name, Type, Last modified, Size, and Storage class. Three objects are visible:

Name	Type	Last modified	Size	Storage class
958006149724_CloudTrail_us-east-1_20250825T0105Z_hvMrzlypfEgwlOKR.json.gz	gz	August 25, 2025, 10:07:27 (UTC+09:00)	2.1 KB	Standard
958006149724_CloudTrail_us-east-1_20250825T0105Z_kmnUHK4lmQeRaj.json.gz	gz	August 25, 2025, 10:06:53 (UTC+09:00)	6.0 KB	Standard
958006149724_CloudTrail_us-east-1_20250825T0105Z_LsIX	gz	August 25, 2025, 10:07:40 (UTC+09:00)	893.0 B	Standard

Note: Logging is the foundation for monitoring & audit evidence.

Step3: AWS Config & Conformance Packs

What this proves

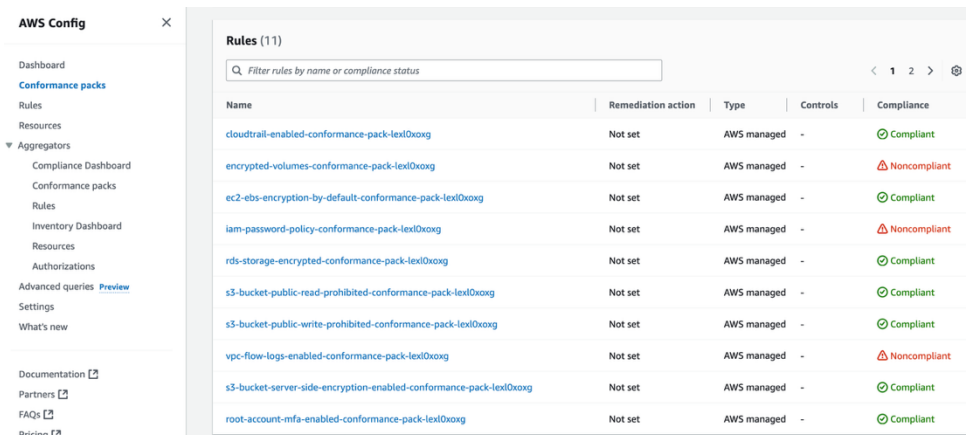
- **Detects misconfigurations** → flags non-compliance in near real-time.
- Conformance Pack with 11 security baseline rules (passwords, MFA, encryption, logs)

Controls

- **ISO 27001:** A.12.1, A.18.2.2 → 2022: 5.14, 5.36
- **Saudi NCA ECC:** OAM-06 (config mgmt.)
- **UAE NESIA IAS:** Secure baseline, data protection, audit & accountability

Proofs / Screenshots

Config Rules Evaluations



Name	Remediation action	Type	Controls	Compliance
cloudtrail-enabled-conformance-pack-lexl0xoxg	Not set	AWS managed	-	Compliant
encrypted-volumes-conformance-pack-lexl0xoxg	Not set	AWS managed	-	Noncompliant
ec2-ebs-encryption-by-default-conformance-pack-lexl0xoxg	Not set	AWS managed	-	Compliant
iam-password-policy-conformance-pack-lexl0xoxg	Not set	AWS managed	-	Noncompliant
rds-storage-encrypted-conformance-pack-lexl0xoxg	Not set	AWS managed	-	Compliant
s3-bucket-public-read-prohibited-conformance-pack-lexl0xoxg	Not set	AWS managed	-	Compliant
s3-bucket-public-write-prohibited-conformance-pack-lexl0xoxg	Not set	AWS managed	-	Compliant
vpc-flow-logs-enabled-conformance-pack-lexl0xoxg	Not set	AWS managed	-	Noncompliant
s3-bucket-server-side-encryption-enabled-conformance-pack-lexl0xoxg	Not set	AWS managed	-	Compliant
root-account-mfa-enabled-conformance-pack-lexl0xoxg	Not set	AWS managed	-	Compliant

CLI Conformance Pack

```
janes-MacBook-Pro:~ janeahn$ aws configservice describe-conformance-packs --conformance-pack-names starter-dev
{
  "ConformancePackDetails": [
    {
      "ConformancePackName": "starter-dev",
      "ConformancePackArn": "arn:aws:config:us-east-1:958006149724:conformance-pack/starter-dev/conformance-pack-lexl0xoxg",
      "ConformancePackId": "conformance-pack-lexl0xoxg",
      "DeliveryS3Bucket": "awsconfigconforms-baseline-958006149724-us-east-1",
      "DeliveryS3KeyPrefix": "artifacts",
      "ConformancePackInputParameters": [],
      "LastUpdateRequestedTime": "2025-08-26T21:27:59.086000+09:00"
    }
  ]
}
```

Note: Provides ongoing evidence for audits. Moves from reactive audits → proactive continuous compliance

Step4: Security Hub & GuardDuty

What this proves

- Unified **threat detection + compliance aggregation**.
- Security Hub consolidates findings (CIS, PCI DSS).
- GuardDuty detects **anomalous network and account behavior**.

Controls

- ISO 27001:** A.12.6, A.16.1 → 2022: 8.8, 5.25
- Saudi NCA:** D5.5 Threat Detection
- SAMA CSF: TVM (Threat & Vulnerability Management), LOG (Logging & Monitoring)

Proofs / Screenshots

Security Hub Summary

The screenshot displays the AWS Security Hub console. On the left, a sidebar shows navigation options: Security Hub CSPM, Summary, Controls, Security standards, Insights, Findings, Integrations, Management (Automations, Custom actions), and Settings (General, Regions, Configuration, Usage). The main content area is divided into two panels. The left panel, titled 'Security standards', shows a 'Security score' of 79% (282 of 356 controls passed) and a table of standards. The right panel, titled 'Assets with the most findings', shows a table of resources with their respective finding counts.

Standard	Passed	Failed	Score
CIS AWS Foundations Benchmark v1.4.0	0	0	0%
NIST Special Publication 800-53 Revision 5	0	0	0%
AWS Foundational Security Best Practices v1.0.0	279	49	85%
AWS Resource Tagging Standard v1.0.0			Enable
CIS AWS Foundations Benchmark v1.2.0			Enable
CIS AWS Foundations Benchmark v3.0.0			Enable
NIST Special Publication 800-171 Revision 2			Enable

Resources	By severity	By resource type	Total findings
arn:aws:rdc:us-east-1:958006149724:db:secure-db	<div><div></div></div>	<div><div></div></div>	9
arn:aws:s3::aws-cloudtrail-logs-958006149724-329023c8	<div><div></div></div>	<div><div></div></div>	9
arn:aws:s3::aws-cloudtrail-logs-958006149724-665bb401	<div><div></div></div>	<div><div></div></div>	9
arn:aws:s3::aws-cloudtrail-logs-958006149724-7a7f55bf	<div><div></div></div>	<div><div></div></div>	9

GuardDuty Detector ON

The screenshot displays the AWS GuardDuty console. On the left, a sidebar shows navigation options: Summary, Findings, EC2 malware scans, Protection plans (S3 Protection, EKS Protection, Extended Threat Detection, Runtime Monitoring, Malware Protection for EC2, Malware Protection for S3, RDS Protection, Lambda Protection), Accounts, Settings, and Lists. The main content area is titled 'Malware Protection for EC2' and shows the status of the 'GuardDuty-initiated malware scan'. The status is 'GuardDuty-initiated malware scan is enabled' with a 'Free trial: 30 day' badge. There is a 'Disable' button. Below this, there is a section for 'On-demand malware scan' with a 'Start scan' button.

Note: Provides central view of risk posture across all accounts

Step5: Policy-as-Code (OPA, tfsec, Checkov)

What this proves

- **Automated governance** before provisioning.
- Prevents deployment of insecure resources (unencrypted S3, missing MFA, etc.).
- CI/CD gate → code must pass tfsec, Checkov, OPA rules **before** apply.

Controls

- **ISO 27001:** A.14.2, A.12.1.2, A.18.2.3 → 2022: 8.28, 5.14, 5.35
- **CIS AWS Foundations:** enforced via Hub CIS subscription
- **SAMA CSF:** SSA (Secure Systems & Applications), ACC (Identity & Access Management), COM (Compliance)

Proofs / Screenshots

✗ OPA eval fail (GuardDuty missing)

```
Janes-MacBook-Pro:tf-aws-secure-baseline janeahn$ cat > plan-no-guardduty.json <<'EOF'
> {
>   "resource_changes": []
> }
> EOF
Janes-MacBook-Pro:tf-aws-secure-baseline janeahn$ opa eval -d policies-as-code/opa -i plan-no-guardduty.json 'data.terraform.security.m
tty
{
  "GuardDuty is not being enabled in this plan (missing aws_guardduty_detector).",

```

✓ OPA eval pass (all checks)

```
Janes-MacBook-Pro:tf-aws-secure-baseline janeahn$ opa eval -d policies-as-code/opa -i plan-pass.json 'data.terraform.security.result' -f pretty
{
  "count": 0,
  "messages": [],
  "passed": true
}
Janes-MacBook-Pro:tf-aws-secure-baseline janeahn$
```

✓ OPA unit tests pass

```
Janes-MacBook-Pro:tf-aws-secure-baseline janeahn$ opa test policies-as-code/opa -v
policies-as-code/opa/policies_test.rego:
data.terraform.security.test_guardduty_missing_detector_denies: PASS (2.876834ms)
data.terraform.security.test_iam_group_missing_boundary_denies: PASS (3.512292ms)
data.terraform.security.test_guardduty_disabled_denies: PASS (3.549917ms)
data.terraform.security.test_securityhub_both_missing_denies: PASS (3.554584ms)
data.terraform.security.test_securityhub_account_only_denies_subscription: PASS (3.612166ms)
data.terraform.security.test_iam_role_missing_boundary_denies: PASS (3.591125ms)
data.terraform.security.test_iam_user_missing_boundary_denies: PASS (3.576917ms)
data.terraform.security.test_s3_requires_sse_denies: PASS (626.75µs)
data.terraform.security.test_s3_with_sse_allows: PASS (4.415333ms)
data.terraform.security.test_guardduty_enabled_allows: PASS (1.988041ms)
-----
PASS: 10/10
```

Note: Shifts compliance left → security embedded in development pipeline.

Step6: Organizations & SCPs

What this proves

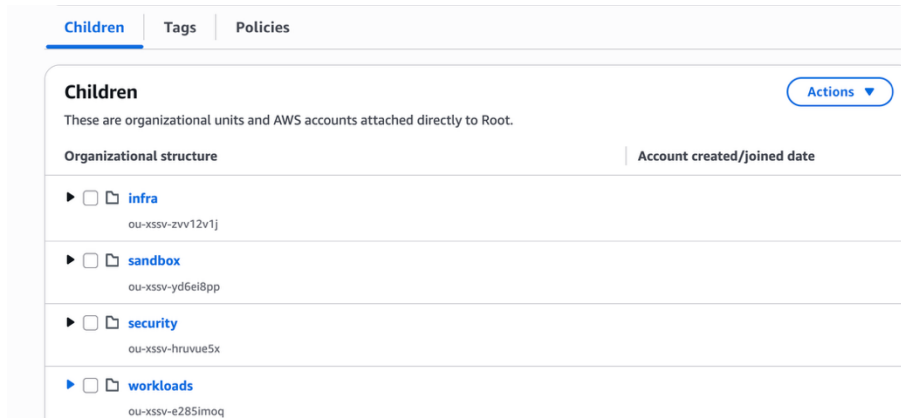
- **Preventive guardrails** enforced Org-wide.
- **SCPs restrict dangerous actions:** Deny leaving Org , Protect CloudTrail/Config/SecHub/GD , Restrict regions (only us-east-1), Require MFA for IAM writes, Deny root user access (toggle)

Controls

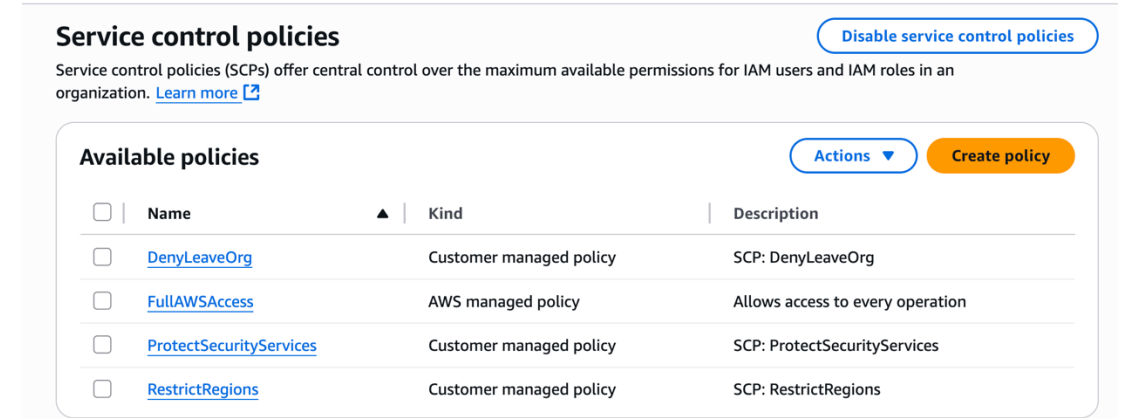
- **ISO 27001:** A.5.1.1, A.9.2.3, A.9.2.1 → 2022: 5.1, 5.18, 5.17
- **Saudi NCA:** GOV-02
- **UAE NESA:** GOV-01
- **SAMA CSF:** GOV (Leadership & Governance), ACC (Identity & Access Management)

Proofs / Screenshots

Org OUs (security, infra, workloads, sandbox)



Root with SCPs Attached



Note: These guardrails prevent violations at source — stronger than detective controls.

Compliance Mapping

Full Compliance Mapping (Audit-Ready Version)

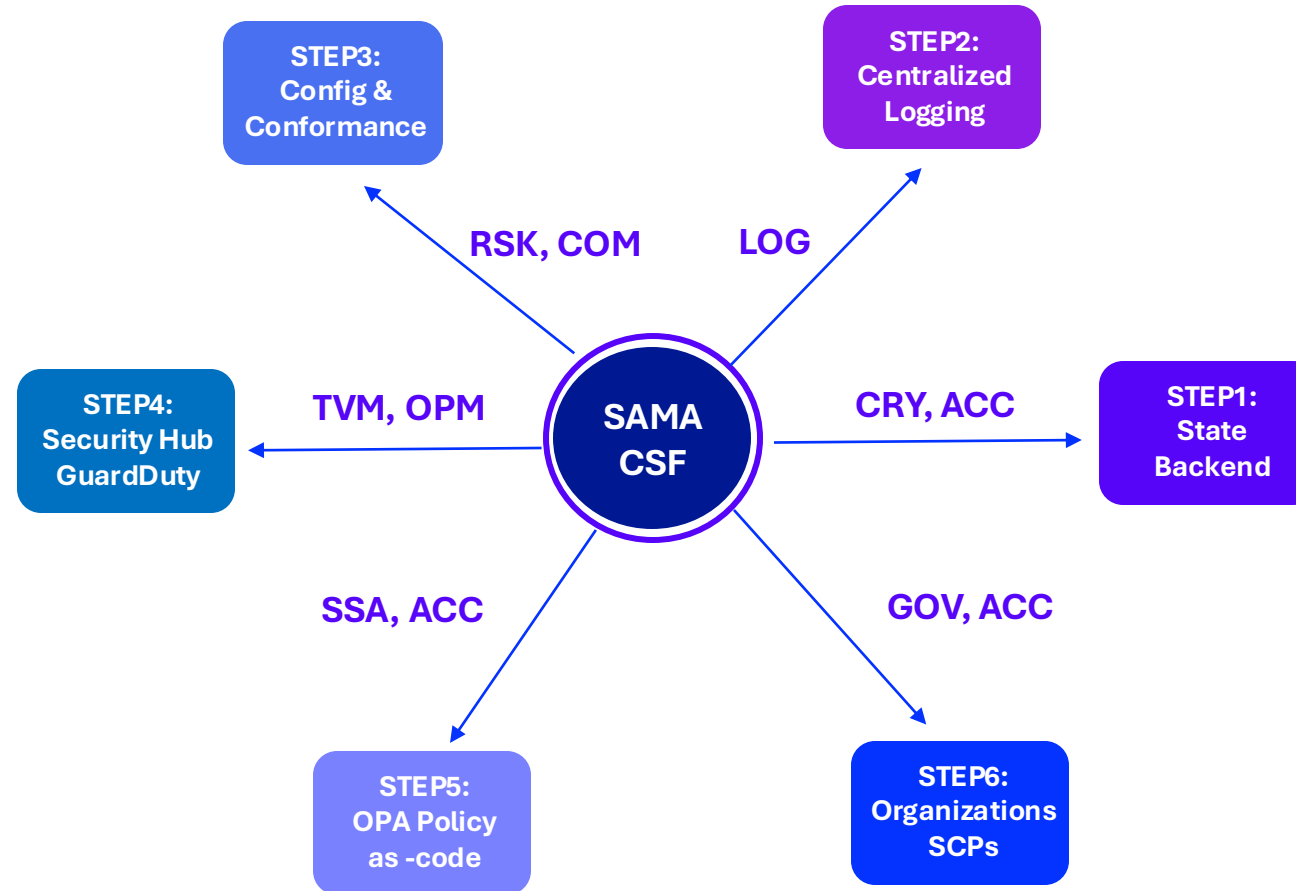
Step	Implementation Example	ISO/IEC 27001 (2013→2022)	NIST CSF	PCI DSS	CIS AWS Foundations	Saudi NCA ECC	Saudi SAMA CSF	UAE NESA IAS	Qatar NCSA CSF
1 — State Backend	S3 backend SSE-KMS, DynamoDB lock	A.8.20 → 8.24 (crypto), A.8.16 → 5.15 (access control)	PR.DS-1 (Data-at-rest protected)	Req. 3.5 (Encryption of cardholder data)	2.2 (Log encryption), 2.1.1 (Block public access)	—	Cryptography (CRY), Access Control (ACC)	—	Data Protection
2 — Centralized Logging	CloudTrail, CloudWatch, KMS	A.12.4 → 8.15 (logging), A.8.20 → 8.24	DE.AE-1 (Anomalous activity detected)	Req. 10 (Logging & monitoring)	2.1 (All regions), 2.2 (Validation), 2.3 (CMKs)	D1/D2 (Logging & monitoring)	Operations & Technology (LOG)	Logging & monitoring	Logging & Monitoring
3 — Config & Conformance	Config rules, Conformance packs	A.12.1 → 5.14, A.18.2.2 → 5.36	ID.RA-1 (Risks identified)	Req. 11.5 (File integrity monitoring)	2.5 (Config enabled), 2.6 (All resources)	CC-06 (Compliance checks)	Risk Mgmt & Compliance (RSK), Compliance (COM)	Compliance & audit governance	Risk Mgmt & Compliance
4 — Security Hub & GuardDuty	Threat detection, incident dashboard	A.12.4 → 8.15, A.12.6 → 8.8, A.16.1 → 5.25	DE.CM-1 (Continuous monitoring)	Req. 12.10 (Incident response)	3.1 (GuardDuty), 3.2 (Security Hub)	D5.5 (Threat detection), CC-06	Operations & Technology (TVM, OPM)	Threat & vulnerability mgmt, monitoring	Threat Detection & Response
5 — OPA Policy-as-Code	Terraform plan eval, CI/CD enforcement	A.12.6 → 8.8, A.18.2.2 → 5.36, A.9.2.3 → 5.18	PR.IP-3 (Secure dev lifecycle)	Req. 6.3 (Secure development practices)	1.1 (MFA), 2.x (Log checks), 3.x (GuardDuty/SecHub)	D3.2 (Secure by design), D5.3 (IAM)	Operations & Technology (SSA), Identity & Access (ACC)	Secure development lifecycle	Secure Development Lifecycle
6 — Organizations & SCPs	DenyLeaveOrg, Protect Security Services, RestrictRegions	A.5.1.1 → 5.1, A.12.4 → 8.15, A.9.1.2 → 5.12, A.9.2.3 → 5.18	RS.MI-1 (Mitigation executed)	Req. 7.2 (Restrict access to cardholder data)	1.1 (MFA), 1.5 (IAM), 1.6 (Root disabled), 2.1 (CloudTrail)	D5.2 (IAM), D5.5 (GuardDuty), D1/D2 (Logging), CC-06	Governance & Leadership (GOV), Access Control (ACC)	Governance, access control, monitoring	Governance & Access Control

Legend

- **ISO/IEC 27001:** Mapping includes 2013 Annex A → 2022 control renumbering.
- **NIST CSF:** ID = Identify | PR = Protect | DE = Detect | RS = Respond | RC = Recover.
- **PCI DSS:** Req. = Requirement (PCI DSS v4.0).
- **CIS AWS Foundations:** v1.4.0 baseline.
- **SAMA:** GOV = Leadership & Governance | RSK = Risk Mgmt | COM = Compliance | CRY = Cryptography | LOG = Logging | TVM = Threat & Vulnerability Mgmt | SSA = Secure Systems & Applications | ACC = Identity & Access Mgmt.
- **NCA, NESA, NCSA:** Domains aligned to national cybersecurity frameworks.

SAMA CSF Mapping Highlights

Mapping Portfolio Steps to SAMA Cyber Security Framework Domains



*SAMA CSF Acronyms (Legend):

GOV = Leadership & Governance | **RSK** = Risk Management | **COM** = Compliance
CRY = Cryptography | **LOG** = Logging & Monitoring | **TVM** = Threat & Vulnerability Management
SSA = Secure Systems & Applications | **ACC** = Identity & Access Management

CI/CD Enforcement with Policy-as-Code

What this proves

- GitHub Actions pipeline runs **security checks automatically**.
- Every pull request triggers **tfsec, Checkov, OPA** before merge.
- Pipeline ensures “**no code is applied without passing security gates.**”

Controls

- **ISO 27001:** A.14.2 Secure coding, A.12.1.2 Change management, A.18.2.3 Technical compliance review → 2022: **8.28, 5.14, 5.35**
- **NCA: DEV-01 Secure Dev, CC-06 Compliance checks**
- **SAMA CSF:** SSA (Secure Systems & Applications), ACC (Identity & Access Management), COM (Compliance)

Proofs / Screenshots

GitHub Actions YAML workflow

```
name: terraform-security-checks

on:
  pull_request:
    paths:
      - "**/*.tf"
      - "policies-as-code/**"
      - ".github/workflows/plan.yml"
  workflow_dispatch:

jobs:
  security_checks:
    runs-on: ubuntu-latest
    env:
      # Default guess; we'll auto-correct this below if the folder doesn't exist
      WORK_DIR: envs/dev
      OPA_DIR: policies-as-code/opa
```

CI Badge Green



Enterprise AWS Secure Baseline (Terraform + PaC)

This project demonstrates **how to design and enforce a secure AWS environment at enterprise scale**. It includes:

- Multi-account setup with AWS Organizations & Service Control Policies
- Centralized logging (CloudTrail, CloudWatch, S3 + KMS)
- AWS Config Conformance Packs for compliance monitoring
- Security Hub & GuardDuty as Cloud Security Posture Management (CSPM) tools
- Policy-as-Code (OPA/Rego) to enforce encryption, IAM boundaries, and security service activation

📄 Compliance Mapping: **ISO/IEC 27001 Annex A (2013 & 2022), Saudi NCA ECC, UAE NESAS IAS**

ISO/IEC 27001 Annex A — Control Mapping (2013 → 2022)

Key takeaway: IaC merges are blocked unless security & compliance tests pass → demonstrates real DevSecOps maturity and ability to operationalize cloud security pipelines.

Conclusion

“Every slide is a proof I built, validated, and enforced in AWS.”

- ✓ **Compliance → ISO 27001, NCA ECC, NESAS IAS**
- ✓ **Security → SCPs, Logging, GuardDuty, Security Hub**
- ✓ **DevSecOps → Policy-as-Code in CI/CD pipelines**

Amina Jiyu An

Cloud Security & Compliance Engineer/Architect