AWS Account Governance - Assessment Worksheet

Core Security Controls

Security Control	Implemented	Notes/Evidence
IAM Password Policy	☑	Enforced strong password policy via IAM; verified policy restrictions.
Multi-Factor Authentication (MFA)	☑	MFA enforced for root and IAM users; verified via Security Hub finding, login tested.
CloudTrail with Multi-Region Logging	☑	Trail configured with multi-region enabled.
CloudTrail S3 Bucket (encrypted, access-controlled)	☑	S3 bucket created with KMS encryption using cloudtrail-key.
AWS Config Recorder	☑	Config enabled in us-east-1 and logging all supported resources.
AWS Config Rules	☑	Deployed 5 config rules via CloudFormation and Security Hub extended rules.
Security Hub	☑	Enabled with AWS Foundational & CIS Benchmarks; findings reviewed.
IAM Access Analyzer	☑	Analyzer created and configured.
CloudWatch Alarms for Security Events	☑	Alarms created for root login, IAM changes, login failures.
SNS Topic for Alerts	☑	SNS topic created and subscribed via email.
AWS Budget with Notifications	☑	Cost budget configured with alert thresholds and email notification.

AWS Config Rule Compliance

Rule Name	Compliance Status	Non-Compliant Resources
iam-password-policy	✓ Compliant	1
mfa-enabled-for-iam-console-access	✓ Compliant	0
root-account-mfa-enabled	✓ Compliant	0
cloudtrail-enabled	✓ Compliant	0
s3-bucket-public-write-prohibited	✓ Compliant	0
securityhub-subnet-auto-assign-public-ip-disabled	✗ Non-compliant	6 subnets

Rule Name	Compliance Status	Non-Compliant Resources
securityhub-s3-bucket-mfa-delete-enabled	❌ Non-compliant	5 s3 buckets
securityhub-s3-bucket-logging-enabled	❌ Non-compliant	5
securityhub-s3-bucket-ssl-requests-only	❌ Non-compliant	5 s3 buckets
securityhub-s3-lifecycle-policy-check	❌ Non-compliant	5
securityhub-cmk-backing-key-rotation-enabled	❌ Non-compliant	1
securityhub-ec2-ebs-encryption-by-default	❌ Non-compliant	1
securityhub-ec2-vpc-bpa-internet-gateway-blocked	❌ Non-compliant	1

Security Hub Standards Section

Security Standard	Current Score	Critical/High Findings
AWS Foundational Security Best Practices v1.0.0	**70%**	Multiple HIGH; e.g. Macie not enabled.
CIS AWS Foundations Benchmark v1.4.0	**60%**	Medium/High IAM and S3 controls failed
PCI DSS	**Not enabled**	-

Open-Ended Reflection Questions

1. **Security Posture Evaluation**

How would you characterize the overall security posture achieved by implementing these controls? What are the strongest elements and what gaps remain?

The strongest elements are Identity and access controls (IAM password policy, MFA, IAM Identity Center with permission sets) every user, including the root account, must use multi-factor authentication, and permission sets ensure only the right privileges are granted. At the same time, CloudTrail captures every API call, and CloudWatch Logs with custom metric filters turn those events into actionable metrics, and alarms notify us in real time. AWS Config rules deployed via CloudFormation and Security Hub give us automated checks against best-practice standards.

The gaps I see are:

Some AWS managed rules (like public-access checks on S3) showed up as failures in AWS Config and Security Hub controls failed by default and need remediation. Also, lack of data

classification (Macie), and automated response (Lambda functions or Security Hub automations) to close the loop.

2. Alignment with Security Frameworks

How do the controls implemented in this lab align with industry security frameworks (such as NIST CSF, ISO 27001, or CIS Controls)? Identify specific domains or control families.

The controls implemented map closely to industry-standard frameworks:

NIST Cybersecurity Framework (CSF):

- Identify -Asset inventory via AWS Config.
- Protect – through strict IAM policies, MFA, and encryption.
- Detect - by leveraging CloudTrail, CloudWatch alarms, and Security Hub findings.
- Respond – through SNS notifications that can trigger incident workflows.

CIS AWS Foundations Controls:

- CSC 1: Inventory and Control of Enterprise Assets (AWS Config).
- CSC 4: Continuous Vulnerability Assessment (Security Hub insights).
- CSC 16: Account Monitoring and Control (CloudTrail logging + alarms).

ISO 27001:

A.9: Access Control (IAM, MFA)

A.12.4: Logging and Monitoring (CloudTrail, CloudWatch)

A.12.7: Audit Logging (AWS Config and Security Hub reports).

3. Business Risk Reduction

Identify 3-5 specific business risks that are mitigated by the security controls you've implemented. How would you explain the value of these controls to non-technical executives?

These controls implemented to mitigate these business risks.

- Stolen credentials: by enforcing Multi-factor authentication and strong password policies, we are able to mitigate risk of stolen credentials leading to unauthorized access.
- Unauthorized changes: CloudWatch alarms on root logins and policy changes give us rapid warnings of any potentially malicious or accidental privilege escalations.
- Data exposure: AWS Config rules for S3 buckets protect against inadvertent data exposure, avoiding regulatory penalties and reputational damage.

- Regulatory non-compliance: Automated compliance checks document our adherence to standards.
- Cost surprises: AWS Budgets alert us before we exceed spend thresholds.

To a non-technical executive, I'd say:

"These controls are like installing secure locks, motion sensors, CCTV security cameras (logging), locked doors with badges (MFA), and an alarm system (CloudWatch alerts). With this, we know who is coming in, get alerts if someone tampers with the locks, and prevent unauthorized access, or cost incident before, all working together to keep the business safe and costs predictable".

4. Advanced Security Architecture

If you were designing a more advanced security architecture for an enterprise, what additional services or features would you incorporate? Why?

If I were designing a more advanced security architecture for an enterprise, I would add:

- Amazon Macie to automatically scan S3 buckets for sensitive data and ensure it remains protected.
- AWS WAF & Shield to guard web applications from DDoS and common exploits.
- Configure Security Hub custom actions backed by AWS Lambda to automatically remediate the critical findings as soon as they appear.
- Use Service Control Policies in AWS Organizations to enforce mandatory guardrails across all accounts, ensuring consistency and reducing administrative overhead.

These additions move us from passive monitoring to proactive defense and centralized policy enforcement at scale.

5. Automation Opportunities

Which aspects of the security implementation could benefit most from automation? How would you approach automating these controls for a large-scale deployment?

I will say the deployment of Config rules, creating CloudWatch metric filters and alarms, and managing SNS topics are ideal for automation.

My approach to automating these controls for a large-scale deployment would be:

- Define every control in infrastructure-as-code templates using CloudFormation or Terraform, and integrate them into a CI/CD pipeline so that any new or updated account instantly inherits the same governance policies.
- Use AWS Lambda functions triggered by Security Hub findings to automatically correct common misconfigurations, such as reapplying public-block settings to S3 buckets.

By treating security as code, we ensure consistency, scalability, and easy auditing, which are critical for large environments.