FAIR

GRC RISK & COMPLIANCE REPORT

SOC2 Type II / ISO27001 / PCI-DSS Evidence Package

Reporting Period: Q4 2025

Generated: 2026-01-12

AUDITOR USE ONLY – CONFIDENTIAL

1. Executive Summary

This audit quantifies financial risk exposure for multi-cloud infrastructure (AWS/Azure) using the FAIR (Factor Analysis of Information Risk) methodology. Analysis of 87 security findings identified **21 Critical** and **66 High** risk items with a total Annual Loss Expectancy (ALE) of **$1,156,200.00**.

Risk Distribution by Data Classification

Total Risk Exposure (ALE)	**$1,156,200.00**
Critical Findings	**21**
High Findings	**66**
Medium Findings	**0**
Low Findings	**0**

Asset Classification Breakdown

Highly Sensitive	**2**
Sensitive	**55**
Internal	**30**
Public	**0**

2. Risk Quantification Methodology

This assessment employs the FAIR model to calculate Annual Loss Expectancy (ALE) using the formula:

ALE = (Asset Value × Threat Frequency) × (1 - Control Effectiveness)

The following parameters were derived from industry standards and control assessments:

FAIR Model Parameters

Parameter	Source	Values
Asset Value	Classification-based	Highly Sensitive: $1M | Sensitive: $100K | Inte
Threat Frequency	MITRE ATT&CK + Prowler Severity	Critical: 30% | High: 15% | Medium: 5% | Low:
Control Effectiveness	NIST 800-53 assessment	MFA: 90% | Encryption: 95% | Security Groups

Validation & Benchmarking

- Loss magnitudes benchmarked against IBM Cost of Data Breach Report 2024
- Threat frequencies validated against Verizon DBIR incident statistics
- Control effectiveness derived from NIST 800-53 and CIS Controls assessments
- Cross-validated with MITRE ATT&CK threat models for cloud environments

3. Control & Compliance Mapping

Each finding is mapped to applicable compliance frameworks including NIST 800-53r5, SOC2 Trust Services Criteria, ISO27001 Annex A, PCI-DSS, and industry-specific regulations (HIPAA, GDPR, C5, NIS2).

Resource	Service	Severity	ALE ($)	Classification	Control
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	ac_3
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	SC-7
i-013c78e009ad3c889	Compute	Critical	$3,000	Internal	ac_3
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	ac_3
i-0127d80de5014204b	Compute	Critical	$3,000	Internal	ac_3
sg-05169f1f38f1135a8	IAM	Critical	$30,000	Sensitive	ac_3
sg-05d5c9870e78283ab	IAM	High	$15,000	Sensitive	SC-7
sg-05d5c9870e78283ab	IAM	High	$3,000	Sensitive	ac_3
sg-0c067238158a89668	IAM	High	$15,000	Sensitive	ac_5
AdminGroup	IAM	High	$15,000	Sensitive	rr_1
869935106430	IAM	High	$15,000	Sensitive	SC-7
AdministratorAccess	IAM	High	$15,000	Sensitive	rr_1
AdminGroup	IAM	High	$15,000	Sensitive	rr_1
Cloud-DevSecops-user/clo	IAM	High	$15,000	Sensitive	rr_1
869935106430	IAM	Critical	$30,000	Sensitive	ac_1
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	rr_1
Backend-Threat-Modelling	IAM	High	$15,000	Sensitive	rr_1
disaster_mgmt_policy	IAM	High	$15,000	Sensitive	rr_1
IAMmodified	IAM	High	$15,000	Sensitive	rr_1
fullaccess/ec2all	IAM	High	$15,000	Sensitive	rr_1
AmazonSageMaker-Executio	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMaker-Executio	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7

AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7
AmazonSageMakerServiceCa	IAM	High	$15,000	Sensitive	SC-7
awsVPCfullaccess	IAM	High	$15,000	Sensitive	SC-7
codebuild_lambda/codebui	IAM	High	$15,000	Sensitive	SC-7
CodeBuild_role/custom_IA	IAM	High	$15,000	Sensitive	SC-7
DataSyncMigrationRole/Ae	IAM	High	$15,000	Sensitive	SC-7
EC2ToS3Access	IAM	High	$15,000	Sensitive	SC-7
ecs-task-execution-role	IAM	High	$15,000	Sensitive	SC-7
labagent	IAM	High	$15,000	Sensitive	SC-7
lambdaexecutionrole/cust	IAM	High	$15,000	Sensitive	SC-7
whizlab-role-obkow5d5/Ap	IAM	High	$15,000	Sensitive	SC-7
<root_account>	IAM	Critical	$3,000	Sensitive	ac_2_1
myuser/ec2	IAM	High	$13,500	Sensitive	rr_1
SecurityTeamAdmin/Admini	IAM	High	$13,500	Sensitive	rr_1
Aws_backup_user/disaster	IAM	High	$15,000	Sensitive	ac_7
Backend-App-Threat-Hunti	IAM	High	$15,000	Sensitive	ac_7
Cloud-DevSecops-user/Clo	IAM	High	$15,000	Sensitive	ac_7
mc-iam-user-Admin/IAMMod	IAM	High	$15,000	Sensitive	ac_7
myuser/ec2	IAM	High	$15,000	Sensitive	ac_7
SecurityTeamAdmin/Admini	IAM	High	$15,000	Sensitive	ac_7
terraform-20260106140714	Database	High	$135,000	Highly Sensitive	ds_2
869935106430	Storage	High	$135,000	Highly Sensitive	ac_3
IoT Hub Defender	unknown	High	$1,350	Internal	SC-7
grc-keyvault123	IAM	High	$13,500	Sensitive	SC-7
grc-keyvault123	IAM	High	$13,500	Sensitive	SC-7
grc-keyvault123	IAM	High	$13,500	Sensitive	SC-7
grc-keyvault123	IAM	High	$13,500	Sensitive	SC-7
Monitor	Monitoring	High	$1,350	Internal	SC-7
Monitor	Monitoring	High	$1,350	Internal	SC-7
Monitor	Monitoring	High	$1,350	Internal	SC-7
Monitor	Monitoring	High	$1,350	Internal	SC-7
Monitor	Monitoring	High	$1,350	Internal	SC-7
Monitor	Monitoring	High	$1,350	Internal	SC-7
Monitor	Monitoring	High	$1,350	Internal	SC-7
Monitor	Monitoring	High	$1,350	Internal	SC-7

Monitor	Monitoring	High	$1,350	Internal	SC-7
Monitor	Monitoring	High	$1,350	Internal	SC-7
Monitor	Monitoring	High	$1,350	Internal	SC-7
grcmigrationdst	IAM	High	$13,500	Sensitive	SC-7
grcmigrationdst	IAM	High	$13,500	Sensitive	SC-7
grcmigrationdst	IAM	High	$13,500	Sensitive	SC-7
grcmigrationdst	IAM	High	$15,000	Sensitive	SC-7
grcmigrationdst	IAM	High	$13,500	Sensitive	SC-7

Compliance Framework Coverage

- C5-2025: 75 findings
- NIS2: 71 findings
- CCC: 70 findings
- SOC2: 37 findings
- ENS-RD2022: 27 findings
- MITRE-ATTACK: 27 findings
- KISA-ISMS-P-2023: 18 findings
- CIS-2.0: 17 findings
- ISO27001-2022: 16 findings
- CISA: 13 findings

4. Risk Heat Map Analysis

Risk Heat Map Matrix

Critical	$0	$63,000	$54,000	$0
High	$270,000	$753,000	$16,200	$0
Medium	$0	$0	$0	$0
Low	$0	$0	$0	$0

5. Top 10 Prioritized Risks

Prioritized based on ALE magnitude and data sensitivity classification.

5.1 terraform-20260106141714016300000001

Asset Type: AwsRdsDbInstance | Service: Database

ALE: $135,000.00 | Classification: Highly Sensitive | Severity: High

NIST Control: ds_2 | Public: False | Retention: 30 days

Risk Details:
If not enabled, sensitive information in transit is not protected.

Remediation:
Ensure that instances provisioned with Amazon RDS enforce SSL/TLS for client connections to meet security and compliance requirements.

5.2 869935106430

Asset Type: AwsS3AccountPublicAccessBlock | Service: Storage

ALE: $135,000.00 | Classification: Highly Sensitive | Severity: High

NIST Control: ac_3 | Public: False | Retention: 30 days

Risk Details:
Public access policies may be applied to sensitive data buckets.

Remediation:
You can enable Public Access Block at the account level to prevent the exposure of your data stored in S3.

5.3 sg-05169f1f38f1135a8

Asset Type: AwsEc2SecurityGroup | Service: IAM

ALE: $30,000.00 | Classification: Sensitive | Severity: Critical

NIST Control: ac_3 | Public: True | Retention: 30 days

Risk Details:
If Security groups are not properly configured the attack surface is increased. An attacker could exploit this misconfiguration to gain unauthorized access to resources.

Remediation:
Use a Zero Trust approach. Narrow ingress traffic as much as possible. Consider north-south as well as east-west traffic.

5.4 869935106430

Asset Type: AwsIamAccessKey | Service: IAM

ALE: $30,000.00 | Classification: Sensitive | Severity: Critical

NIST Control: ac_1 | Public: False | Retention: 30 days

Risk Details:
The root account is the most privileged user in an AWS account. AWS Access Keys provide programmatic access to a given AWS account. It is recommended that all access keys associated with the root acco

Remediation:
Use the credential report to check the user and ensure the access_key_1_active and access_key_2_active fields are set to FALSE. If using AWS Organizations, consider enabling Centralized Root Managemen

5.5 sg-0c067238158a89668

Asset Type: AwsEc2SecurityGroup | Service: IAM

ALE: $15,000.00 | Classification: Sensitive | Severity: High

NIST Control: ac_5 | Public: False | Retention: 30 days

Risk Details:
Even having a perimeter firewall, having security groups open allows any user or malware with vpc access to scan for well known and sensitive ports and gain access to instance.

Remediation:
Apply Zero Trust approach. Implement a process to scan and remediate unrestricted or overly permissive security groups. Recommended best practices is to narrow the definition for the minimum ports req

5.6 sg-05d5c9870e78283ab

Asset Type: AwsEc2SecurityGroup | Service: IAM

ALE: $15,000.00 | Classification: Sensitive | Severity: High

NIST Control: SC-7 | Public: True | Retention: 30 days

Risk Details:
The security group allows all traffic from the internet to any port. This could allow an attacker to access the instance.

Remediation:
Use a Zero Trust approach. Narrow ingress traffic as much as possible. Consider north-south as well as east-west traffic.

5.7 AdminGroup

Asset Type: AwsIamUser | Service: IAM

ALE: $15,000.00 | Classification: Sensitive | Severity: High

NIST Control: rr_1 | Public: False | Retention: 30 days

Risk Details:
Policy may allow Anonymous users to perform actions.

Remediation:
Ensure this repository and its contents should be publicly accessible.

5.8 disaster_mgmt_policy

Asset Type: AwsIamPolicy | Service: IAM

ALE: $15,000.00 | Classification: Sensitive | Severity: High

NIST Control: rr_1 | Public: False | Retention: 30 days

Risk Details:
Users with some IAM permissions are allowed to elevate their privileges up to administrator rights.

Remediation:
Grant usage permission on a per-resource basis and applying least privilege principle.

5.9 Backend-Threat-Modelling-Policy

Asset Type: AwsIamPolicy | Service: IAM

ALE: $15,000.00 | Classification: Sensitive | Severity: High

NIST Control: rr_1 | Public: False | Retention: 30 days

Risk Details:

Users with some IAM permissions are allowed to elevate their privileges up to administrator rights.

Remediation:
Grant usage permission on a per-resource basis and applying least privilege principle.

5.10 AmazonSageMakerServiceCatalogProductsCloudformationRole

Asset Type: AwsIamRole | Service: IAM

ALE: $15,000.00 | Classification: Sensitive | Severity: High

NIST Control: SC-7 | Public: False | Retention: 30 days

Risk Details:
Allow attackers to gain unauthorized access to resources

Remediation:
To mitigate cross-service confused deputy attacks, it's recommended to use the aws:SourceArn and aws:SourceAccount global condition context keys in your IAM role trust policies. If the role doesn't su

6. Remediation Roadmap

This roadmap prioritizes remediation efforts based on risk magnitude, asset criticality, and compliance requirements. All timeframes align with NIST 800-53r5 recommended practices.

Phase 1 (0-30 days): Critical Risk Reduction

Scope: Critical findings + ALE > $100,000

- Implement Multi-Factor Authentication on all IAM roles and users (IA-2, AC-2)
- Remove root account access keys and enable hardware MFA (IA-2, AC-6)
- Remove internet exposure from all database instances (SC-7, AC-3)
- Revoke AdministratorAccess policy from non-essential principals (AC-6, SC-2)
- Deploy AWS Config rules for continuous compliance monitoring
- Create JIRA/ServiceNow tickets with P0 priority for tracking

Phase 2 (30-90 days): High Risk Mitigation

Scope: High findings + ALE $10,000-$100,000

- Enable encryption at rest for all storage accounts (SC-13, SC-28)
- Implement least-privilege IAM policies across all services (AC-6)
- Enable soft-delete and versioning on all storage buckets (SI-12)
- Add confused deputy protection to all service roles (SC-7)
- Configure CloudTrail logging for all regions (AU-2, AU-3)
- Establish weekly Steampipe compliance scanning cron jobs

Phase 3 (90+ days): Continuous Improvement

Scope: Medium/Low findings + Process establishment

- Implement automated remediation using AWS Lambda/Config (SI-7)
- Integrate findings with SIEM/SOAR platform (AU-6, IR-4)
- Conduct quarterly access reviews for all IAM principals (AC-2)
- Establish KPI dashboard for ongoing risk monitoring
- Perform annual third-party penetration testing
- Update disaster recovery plans based on risk assessments

7. Asset Inventory Summary

Comprehensive inventory of assessed cloud resources organized by service.

Assets by Service Category

- IAM: 55 assets | $816,000 total ALE
- Compute: 18 assets | $54,000 total ALE
- Monitoring: 11 assets | $14,850 total ALE
- Database: 1 assets | $135,000 total ALE
- Storage: 1 assets | $135,000 total ALE
- unknown: 1 assets | $1,350 total ALE

Appendix A – Detailed Risk Register

Complete listing of all identified risks with full compliance mappings.

Asset	Service	Severity	ALE	Class	Public	Retention	Control	Frameworks
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	ac_3	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	SC-7	NIS2, SOC2, C5-
i-013c78e009ad3c889	Compute	Critical	$3,000	Internal	True	30d	ac_3	CCC, NIS2, SOC2
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	ac_3	CCC, NIS2, SOC2
i-0127d80de5014204	Compute	Critical	$3,000	Internal	True	30d	ac_3	NIS2, SOC2, C5-
sg-05169f1f38f1135a8	IAM	Critical	$30,000	Sensitive	True	30d	ac_3	CCC, CISA, SOC2
sg-05d5c9870e78283ab	IAM	High	$15,000	Sensitive	True	30d	SC-7	CCC, SOC2, C5-2
sg-05d5c9870e78283ab	IAM	High	$3,000	Sensitive	True	30d	ac_3	CCC, CISA, SOC2
sg-0c067238158a89668	IAM	High	$15,000	Sensitive	False	30d	ac_5	CCC, CISA, FFIE
AdminGroup	IAM	High	$15,000	Sensitive	False	30d	rr_1	CCC, NIS2, C5-2
869935106430	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AdministratorAccess	IAM	High	$15,000	Sensitive	False	30d	rr_1	CCC, CISA, GDPR
AdminGroup	IAM	High	$15,000	Sensitive	False	30d	rr_1	CCC, C5-2025, N
Cloud-DevSecopsUser	IAM	High	$15,000	Sensitive	False	30d	rr_1	CCC, SOC2, C5-2
869935106430	IAM	Critical	$30,000	Sensitive	False	30d	ac_1	CCC, CISA, GDPR
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	rr_1	CCC, NIS2, C5-2
Backend-Threat-Model	IAM	High	$15,000	Sensitive	False	30d	rr_1	CCC, NIS2, C5-2
disaster_mgmt_policy	IAM	High	$15,000	Sensitive	False	30d	rr_1	CCC, NIS2, C5-2
IAMmodified	IAM	High	$15,000	Sensitive	False	30d	rr_1	CCC, NIS2, C5-2
fullaccess/ec2all	IAM	High	$15,000	Sensitive	False	30d	rr_1	CCC, NIS2, C5-2
AmazonSageMakerExec	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerExec	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
AmazonSageMakerServi	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2

awsVPCfullaccess	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
codebuild_lambda/cod	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
CodeBuild_role/custo	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
DataSyncMigrationRol	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
EC2ToS3Access	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
ecs-task-execution	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
labagent	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
lambdaexecutionrole/	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
whizlab-role-obkoW9d	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
<root_account>	IAM	Critical	$3,000	Sensitive	False	30d	ac_2_1	CCC, CISA, GDPR
myuser/ec2	IAM	High	$13,500	Sensitive	False	30d	rr_1	CCC, C5-2025, F
SecurityTeamAdmin/Ad	IAM	High	$13,500	Sensitive	False	30d	rr_1	CCC, C5-2025, F
Aws_backup_user/Admsa	IAM	High	$15,000	Sensitive	False	30d	ac_7	CCC, CISA, GDPR
Backend-App-Threat-H	IAM	High	$15,000	Sensitive	False	30d	ac_7	CCC, CISA, GDPR
Cloud-DevSecops-User	IAM	High	$15,000	Sensitive	False	30d	ac_7	CCC, CISA, GDPR
mc-iam-user-Admin/IA	IAM	High	$15,000	Sensitive	False	30d	ac_7	CCC, CISA, GDPR
myuser/ec2	IAM	High	$15,000	Sensitive	False	30d	ac_7	CCC, CISA, GDPR
SecurityTeamAdmin/Ad	IAM	High	$15,000	Sensitive	False	30d	ac_7	CCC, CISA, GDPR
terraform-2026010614	Database	High	$135,000	Highly Sensitive	False	30d	ds_2	CCC, C5-2025, C
869935106430	Storage	High	$135,000	Highly Sensitive	False	30d	ac_3	CCC, CISA, FFIE
IoT Hub Defender	unknown	High	$1,350	Internal	False	30d	SC-7	NIS2, SOC2, C5-
grc-keyvault123	IAM	High	$13,500	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
grc-keyvault123	IAM	High	$13,500	Sensitive	False	30d	SC-7	CCC, NIS2, SOC2
grc-keyvault123	IAM	High	$13,500	Sensitive	False	30d	SC-7	CCC, NIS2, C5-2
grc-keyvault123	IAM	High	$13,500	Sensitive	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, NIS2, SOC2
Monitor	Monitoring	High	$1,350	Internal	False	30d	SC-7	CCC, C5-2025, C
grcmigrationdst	IAM	High	$13,500	Sensitive	False	30d	SC-7	CCC, C5-2025, C
grcmigrationdst	IAM	High	$13,500	Sensitive	False	30d	SC-7	CCC, CIS-4.0
grcmigrationdst	IAM	High	$13,500	Sensitive	False	30d	SC-7	CCC, C5-2025, C
grcmigrationdst	IAM	High	$15,000	Sensitive	False	30d	SC-7	CCC, NIS2, SOC2
grcmigrationdst	IAM	High	$13,500	Sensitive	False	30d	SC-7	CCC, C5-2025, C

Appendix B – Control Effectiveness Calculations

Detailed assumptions for control effectiveness coefficients used in FAIR calculations.

Control Type	Effectiveness	Rationale	Mapped Findings
Multi-Factor Authentication (MFA)	90%	Based on Microsoft research showing	iam_root_hardware_mfa_ena
Encryption at Rest (AES-256)	95%	Considered cryptographically unbrea	S3 bucket encryption, RDS
Security Group Restrictions	80%	Reduces lateral movement but not fo	ec2_securitygroup_allow_i
Least Privilege IAM	85%	Limits blast radius but requires co	iam_policy_allows_privile
CloudTrail Logging	60%	Aids detection but not prevention;	Logging configuration che
Backup & Versioning	70%	Protects against ransomware but has	S3 versioning, RDS snapsh
Cross-Service Confused Deputy Protection	75%	AWS IAM conditions significantly re	iam_role_cross_service_co
No Control / Full Exposure	0%	Baseline for unmitigated risk scena	Default security group ru

Appendix C – Assumptions & Limitations

Scope Assumptions:
• Assessment limited to AWS and Azure resources discoverable by Prowler and Steampipe
• Asset values based on estimated business impact, not actual revenue attribution
• Threat frequencies derived from public incident statistics, not organization-specific data
• Control effectiveness assumes proper implementation and monitoring

Limitations:
• Does not account for zero-day vulnerabilities or advanced persistent threats
• Loss magnitude estimates do not include reputational damage or legal costs
• Network effects and cloud blast radius scenarios are simplified
• Assumes independent risk events; does not model compounding incidents

Validation:
• Findings cross-referenced with AWS Security Hub and Azure Security Center
• Control mappings validated against NIST 800-53r5 official controls catalog
• ALE calculations peer-reviewed against FAIR Institute guidelines