

# AWS SECURITY AUDIT

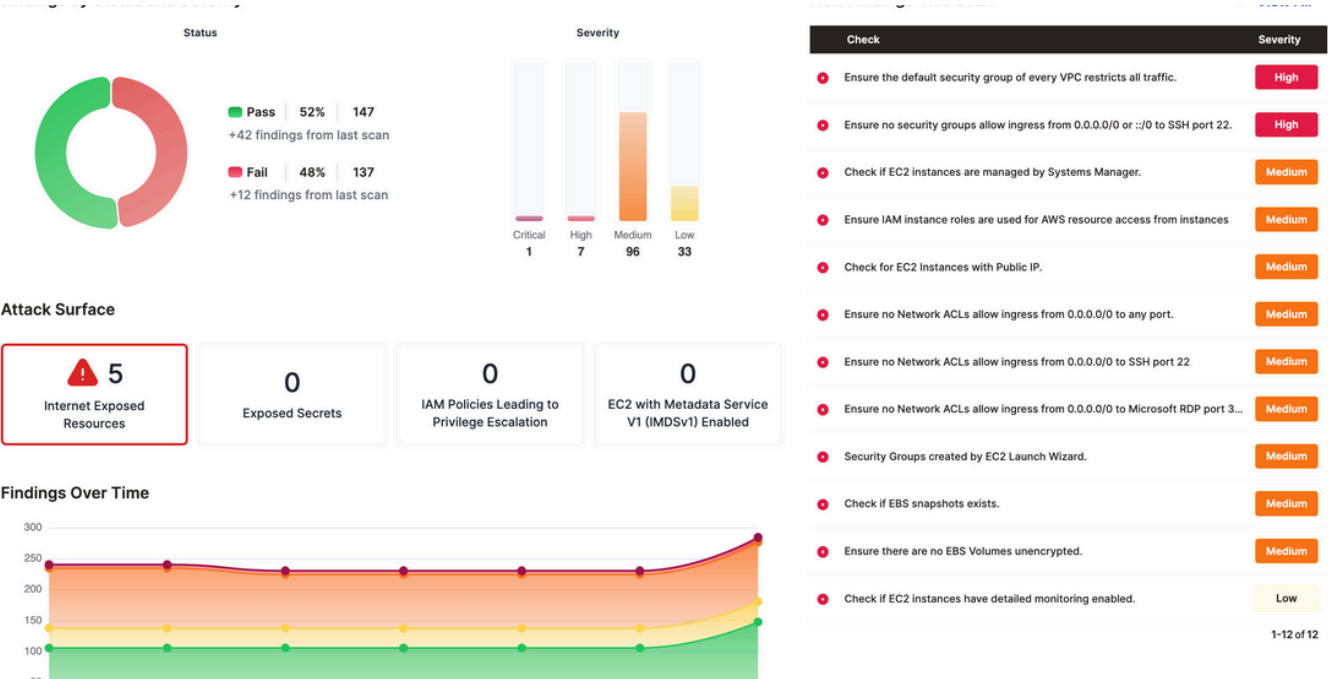
**JULY 2025**

Prepared by  
**A Cloud Wizard**



# SECURITY AUDIT – FINDINGS

## Findings by Status and Severity



## Urgent Findings – Immediate Action Needed

Check	Severity
Ensure the default security group of every VPC restricts all traffic.	High
Ensure no security groups allow ingress from 0.0.0.0/0 or ::0 to SSH port 22.	High

# Findings by Region



1.  eu-west-1	45 Fails	1 Critical	5 High	32 Medium	7 Low
2.  us-east-1	41 Fails	0 Critical	2 High	34 Medium	5 Low
3.  us-east-2	13 Fails	0 Critical	0 High	10 Medium	3 Low
4.  us-west-2	12 Fails	0 Critical	0 High	9 Medium	3 Low
5.  eu-south-2	10 Fails	0 Critical	0 High	8 Medium	2 Low
6.  ap-southeast-2	2 Fails	0 Critical	0 High	1 Medium	1 Low

Failed Findings by Account (Top 10)

1.  logs-demo 890837126756	147 Fails	1 Critical	7 High	106 Medium	33 Low
-------------------------------	--------------	---------------	-----------	---------------	-----------

Failed Findings by Service (Top 10)

1.  accessanalyzer	18 Fails	0 Critical	0 High	0 Medium	18 Low
2.  ec2	17 Fails	0 Critical	2 High	14 Medium	1 Low
3.  cloudwatch	15 Fails	0 Critical	0 High	15 Medium	0 Low
4.  cloudtrail	15 Fails	0 Critical	0 High	10 Medium	5 Low
5.  config	13 Fails	0 Critical	0 High	13 Medium	0 Low
6.  iam	12 Fails	1 Critical	4 High	7 Medium	0 Low

## Top Region Security Failures

Region with most Issues

1.  eu-west-1	45 Fails	1 Critical	5 High	32 Medium	7 Low
---------------	-------------	---------------	-----------	--------------	----------

No 1. Service Issue

1.  accessanalyzer	18 Fails	0 Critical	0 High	0 Medium	18 Low
--------------------	-------------	---------------	-----------	-------------	-----------





Account with most Issues

1.  logs-demo 890837126756	147 Fails	1 Critical	7 High	106 Medium	33 Low
-------------------------------	--------------	---------------	-----------	---------------	-----------

# Findings by Services

 <b>IAM Access Analyzer</b> ▲ 18 Failed Findings	 <b>AWS Account</b> ▲ 1 Failed Findings	 <b>Amazon Athena</b> ● No Failed Findings	 <b>AWS Lambda</b> ● No Failed Findings	 <b>AWS Backup</b> ▲ 1 Failed Findings	 <b>AWS CloudFormation</b> ▲ 4 Failed Findings
 <b>AWS CloudTrail</b> ▲ 15 Failed Findings	 <b>Amazon CloudWatch</b> ▲ 15 Failed Findings	 <b>AWS Config</b> ▲ 13 Failed Findings	 <b>AWS Data Replication Service</b> ▲ 5 Failed Findings	 <b>Amazon EC2</b> ▲ 17 Failed Findings	 <b>Amazon EMR</b> ● No Failed Findings
 <b>AWS Glue</b> ▲ 10 Failed Findings	 <b>Amazon GuardDuty</b> ▲ 5 Failed Findings	 <b>AWS IAM</b> ▲ 12 Failed Findings	 <b>Amazon Inspector</b> ▲ 4 Failed Findings	 <b>Amazon Macie</b> ▲ 4 Failed Findings	 <b>AWS Network Firewall</b> ▲ 1 Failed Findings
 <b>AWS Organizations</b> ● No Failed Findings	 <b>AWS Resource Groups</b> ▲ 1 Failed Findings	 <b>Amazon S3</b> ▲ 7 Failed Findings	 <b>AWS Security Hub</b> ▲ 3 Failed Findings	 <b>Amazon SNS</b> ● No Failed Findings	 <b>AWS Systems Manager Incident Manager</b> ▲ 1 Failed Findings
 <b>AWS Trusted Advisor</b> ▲ 1 Failed Findings	 <b>Amazon VPC</b> ▲ 9 Failed Findings				

## Top Service Security Failures

 <b>IAM Access Analyzer</b> ▲ 18 Failed Findings	 <b>Amazon EC2</b> ▲ 17 Failed Findings
 <b>AWS CloudTrail</b> ▲ 15 Failed Findings	 <b>Amazon CloudWatch</b> ▲ 15 Failed Findings

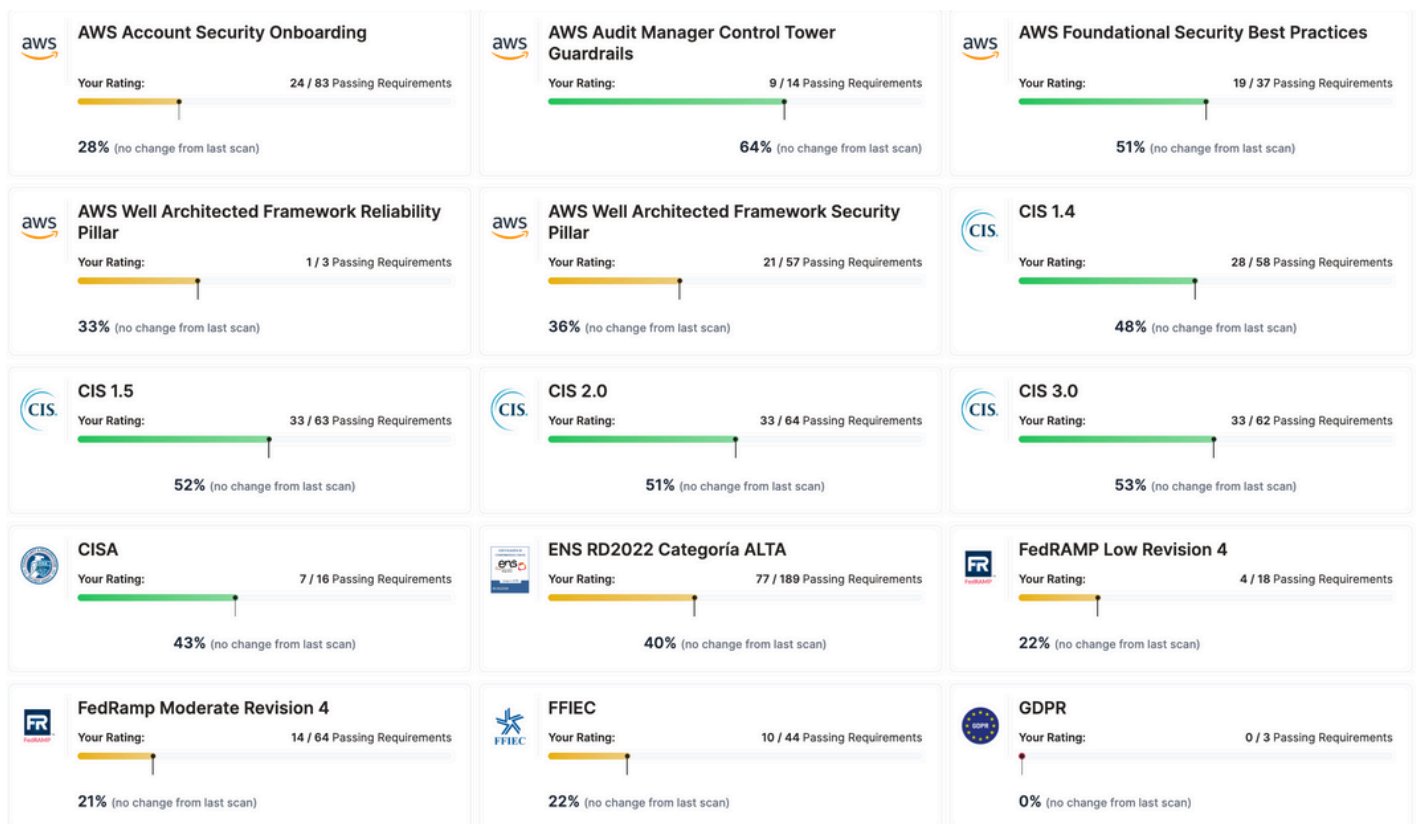
# Findings by Severity

Check	Severity ↑	Status	Region	Service	Account
› Ensure MFA is enabled for the root account	<div>Critical</div>	FAIL	eu-west-1	iam	logs-demo (890837126756)
› Ensure IAM AWS-Managed policies that allow full "*" administrative privileges are not attached	<div>High</div>	FAIL	eu-west-1	iam	logs-demo (890837126756)
› Ensure the default security group of every VPC restricts all traffic.	<div>High</div>	FAIL	us-east-1	ec2	logs-demo (890837126756)
› Ensure no security groups allow ingress from 0.0.0.0/0 or ::0 to SSH port 22.	<div>High</div>	FAIL	us-east-1	ec2	logs-demo (890837126756)
› Check S3 Account Level Public Access Block.	<div>High</div>	FAIL	eu-west-1	s3	logs-demo (890837126756)
› Ensure IAM Roles do not have AdministratorAccess policy attached	<div>High</div>	FAIL	eu-west-1	iam	logs-demo (890837126756)
› Ensure IAM Service Roles prevents against a cross-service confused deputy attack	<div>High</div>	FAIL	eu-west-1	iam	logs-demo (890837126756)
› Ensure IAM Roles do not have AdministratorAccess policy attached	<div>High</div>	FAIL	eu-west-1	iam	logs-demo (890837126756)
› Ensure DRS is enabled with jobs.	<div>Medium</div>	FAIL	us-east-2	drs	logs-demo (890837126756)
› Ensure AWS Config is enabled in all regions.	<div>Medium</div>	FAIL	sa-east-1	config	logs-demo (890837126756)
› Ensure DRS is enabled with jobs.	<div>Medium</div>	FAIL	eu-south-2	drs	logs-demo (890837126756)

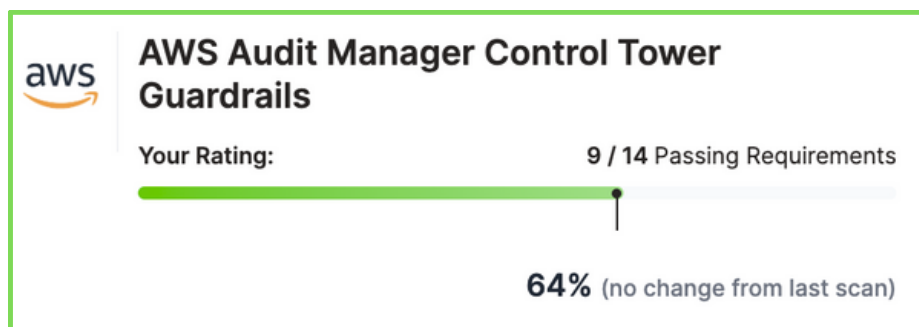
## Critical Failures

Check	Severity ↑	Status	Region	Service
Ensure MFA is enabled for the root account	<div>Critical</div>	FAIL	eu-west-1	iam

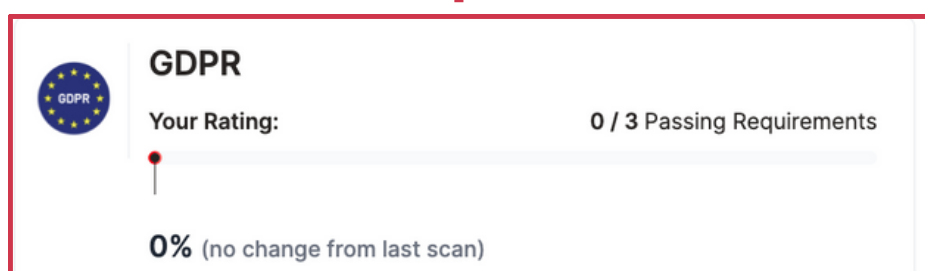
# Compliance



## Highest Compliance Score



## Lowest Compliance Score



# Recommendations

## Strengthen IAM Access Controls

- Implement the principle of least privilege by regularly reviewing IAM policies to ensure users and roles have only the permissions necessary for their tasks.
- Enable multi-factor authentication (MFA) for all IAM users, especially those with administrative privileges.
- Use AWS IAM Access Analyzer to identify unused permissions, overly permissive policies, or external access to resources.

## Enhance AWS CloudTrail Configuration

- Ensure CloudTrail is enabled for all AWS regions and configured to log all API activities, including read and write events.
- Enable log file integrity validation to detect unauthorized changes to CloudTrail logs.
- Store CloudTrail logs in a secure, centralized S3 bucket with restricted access and lifecycle policies to manage retention.

## Optimize AWS CloudWatch

- Configure CloudWatch Logs to capture and analyze logs from CloudTrail, VPC Flow Logs, and other critical services for real-time monitoring.
- Set up CloudWatch Alarms to alert on suspicious activities, such as unauthorized API calls or changes to critical resources.
- Integrate CloudWatch with AWS Security Hub for centralized visibility into security alerts and compliance status.

## General Security Best Practices

- Conduct regular security assessments using tools like AWS Trusted Advisor and AWS Config to identify misconfigurations and compliance issues.
- Encrypt sensitive data at rest and in transit using AWS Key Management Service (KMS) and enforce SSL/TLS for all communications.
- Implement automated remediation for common issues using AWS Systems Manager or Lambda functions triggered by CloudWatch Events.