

# Automated AWS Security & Compliance Assessment

Tenfold Security

Dashboard

Dashboard

Overview

Assessments

AWS Settings

Accounts

Profile

User Settings

Custom Reports

org:

Export

Launch New Scan

Overview

Recommendations

Assessment Details

Reports

Filter by Domain...

Filter by service...

showing 95 of 95

15

47

27

6

Priority	Category	Services	Title	Accounts	Actions
critical	Threat Detection	GuardDuty	Enable Amazon GuardDuty	60%	5
				72%	10
				52%	8
				47%	1
				61%	17
critical	Root Account Security	IAM	Enable MFA for Root Account	0%	3
				52%	12
				72%	10
				0%	13
				47%	1
critical	Review IAM Access	IAM	Full Admin Permissions **	61%	17
				72%	10
				61%	17
				72%	10
				61%	17
critical	IAM Security	IAM	Enable MFA for the IAM Users with Administrator Permissions	72%	10
				61%	17
				72%	10
				61%	17
				72%	10



Tenfold Security

Dashboard

Failed Security Findings Summary

critical medium low high info

Security Maturity Level

Top 30 recommendations across all accounts

Priority	Category	Title	Account Ids
critical	Logging & Monitoring	Enable Amazon GuardDuty	61% 17
critical	Identity & Access Management	Enable MFA for the IAM Users with Administrator Permissions	61% 17
high	Infrastructure Security	Disable Direct Internet Access for EC2 Instances	61% 17
high	Infrastructure Security	Configure Instance Metadata Service v2	61% 17
high	Infrastructure Security	Disable Auto-Assign Public IPs	61% 17
medium	Infrastructure Security	Unrestricted Management Port Access (SSH/RDP)	61% 17
medium	Identity & Access Management	Enable MFA for the IAM Users with Console Access	61% 17
medium	Encryption	Enable KMS Key Rotation	61% 17

org: (PCI DSS v3.2.1)

PCI DSS 1.2.1: Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment (CDE), and specifically deny all other traffic

**Control Description**

This requirement is intended to prevent malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within your network out to an unauthorized server). Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.

**Assessment Checks**

- ✗ No Public S3 Buckets
- ✓ S3 Block Public Access is Enabled (Account-Level)
- ✗ No Security Group Rules Allowing 0.0.0.0/0 to SSH (TCP 22)
- ✓ No Public EBS Snapshots
- ✗ Default Security Group No Rules
- ✓ No Public RDS Instances
- No Public RDS Snapshots
- ✗ Amazon Elasticsearch Domain is in a VPC
- No Public Redshift Clusters
- No Direct Internet Access for SageMaker Notebook Instance
- Database Migration Service Instance Not Public

✗ PCI DSS 1.3.1: Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports

**Control Description**

A DMZ is that part of the network that manages connections between the Internet (or other external networks), and services that an organization needs to have available to the public (like a web server). This functionality is intended to prevent malicious individuals from accessing the internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner.

The screenshot shows the AWS Security Hub console. The top navigation bar includes 'Export' and 'Launch New' buttons. The main menu has 'Recommendations', 'Assessment Details', and 'Reports' (which is selected). The 'Reports' section is titled 'Reports' and contains four cards: 'Resiliency & HA', 'Public Resources', 'Encryption In-Transit', and 'Service Access Logs'. Below these is the 'Custom Compliance Standards' section, which is circled in red. It includes a link to 'Click on Custom Reports from the menu to define custom reports for your organization.' and a table of standards:

Standard	Progress	Passed	Failed
NIST 800-53	31%	20	62
NIST CSF	31%	18	55
SOC2	21%	0	34
HIPAA	31%	16	44

Assessment Results > SOC2 > all regions

List of Controls

Assessment Rules

List of Controls (SOC2)

Export PDF

Quick Search

✖ CC1.0 - Common Criteria Related to Control Environment

✖ CC2.0 - Common Criteria Related to Communication and Information

Control Description

The criteria relevant to how the entity (i) uses relevant information, (ii) communicates internally, and (iii) communicates externally

- CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control

Assessment Checks

- ✖ S3 Object-Level Logging with CloudTrail is Enabled
- ✔ Ensure CloudTrail is Enabled for this Region
- ✔ Ensure that a Multi-Region CloudTrail Trail is Configured
- ✖ Ensure that CloudTrail logs are encrypted using KMS
- ✔ Ensure that CloudTrail Log File Validation is Enabled
- ✔ CloudTrail Global Services Enabled
- ✖ Ensure that AWS Config is Enabled

✖ CC3.0 - Common Criteria Related to Risk Assessment

✖ CC4.0 - Monitoring Activities

✖ CC6.0 - Logical and Physical Access

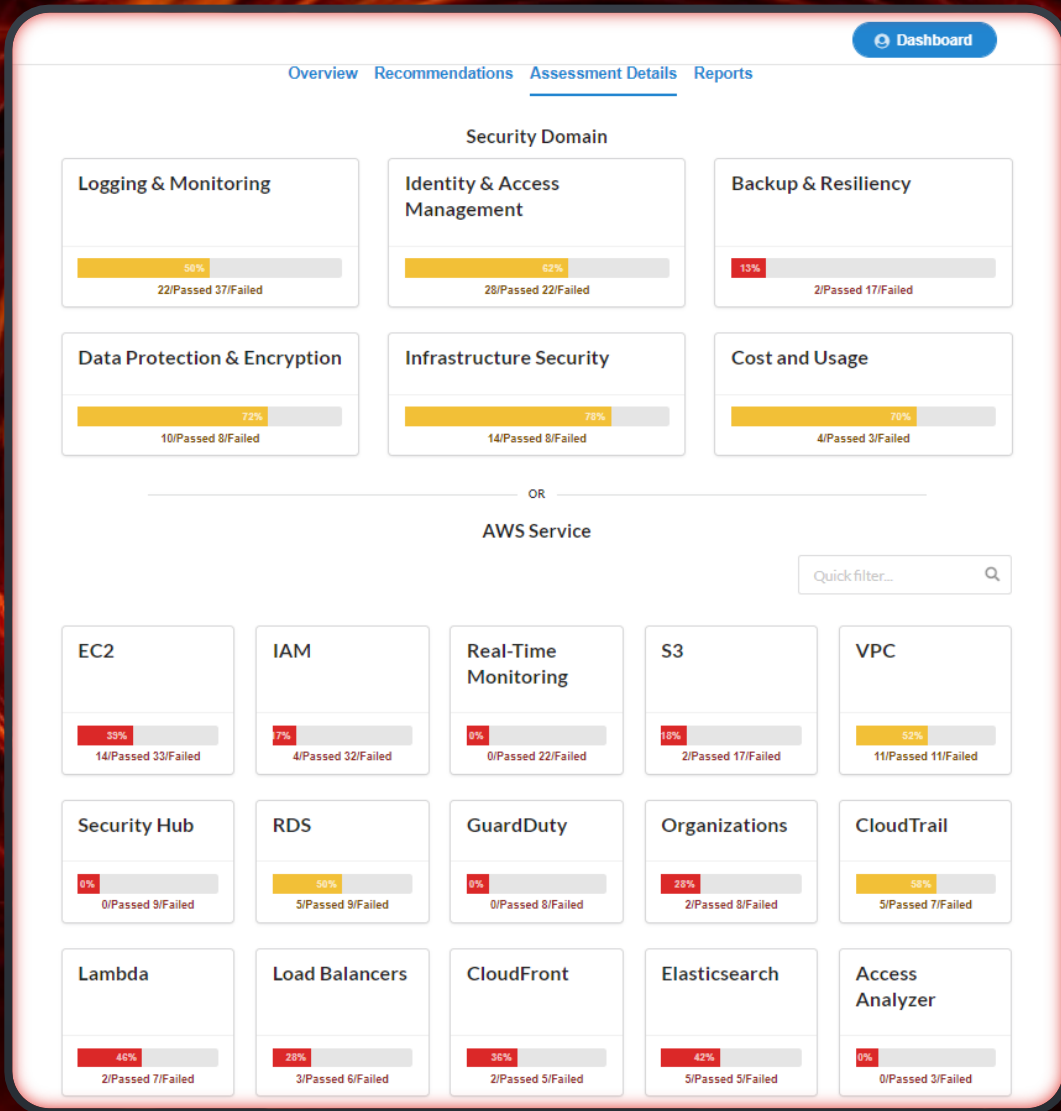
✖ CC7.0 - System Operations

✖ CC8.0 - Change Management

✖ CCA1.0 - Additional Criteria for Availability

✖ CCA2.0 - Additional Criteria for Confidentiality





View Compliance by Domain and Services

Show Public Exposure Across Your Entire Cloud

Dashboard

Reports > Public Resources

Summary

Export PDF

AWS Service	Feature	✓	✗
AWS IAM	No Publicly Assumable IAM Roles	273	0
Amazon S3	No Public Buckets	24	2
Amazon ECR	No Public Repositories	0	0
AWS KMS	No Public KMS Keys	9	0
AWS Lambda	No Public Functions	19	0
Amazon Elasticsearch	No Public Elasticsearch Clusters	0	2
AWS Glue	No Public Glue Dev Endpoints	0	0
Amazon SNS	No Public SNS Topics	22	0
Amazon EC2	No Public EC2 Instances	3	7
	No Public AMIs	6	0
	No Public EBS Snapshots	8	0
Amazon ECS	No Public ECS/Fargate Services	0	0
Amazon RDS	No Public RDS Instances/Clusters	1	0
	No Public RDS Snapshots	0	0
Amazon API Gateway	No Public API Gateway Endpoints	0	0
	API Gateway Endpoints Protected by WAF	0	0
AWS AppSync	AppSync Endpoints Protected by WAF	0	0





**TENFOLD SECURITY**

Contact Us For More Information:

[Info@tenfoldsecurity.com](mailto:Info@tenfoldsecurity.com)

<https://assessment.tenfoldsecurity.com>