

# Practical 1: AWS Security Hub: Compliance check

## Screenshot 1- Security Standard Score

The screenshot displays the AWS Security Hub console for the eu-north-1 region. The left sidebar shows the navigation menu with 'Security Hub CSPM' selected. The main content area is titled 'Security standards' and shows a 'Security score' of 84% (277 of 329 controls passed). Below this, a table lists the standards and their compliance status:

| Standard  | Passed | Failed | Score |
|---|--------|--------|-------|
| CIS AWS Foundations Benchmark v1.2.0            | 14     | 28     | 33%   |
| CIS AWS Foundations Benchmark v1.4.0            | 15     | 24     | 38%   |
| AWS Foundational Security Best Practices v1.0.0 | 271    | 28     | 91%   |

On the right, the 'Assets with the most findings' section shows a list of resources with their respective finding counts and severity levels. The resources listed are:

- AWS::Account:527001004240
- arn:aws:ec2:eu-north-1:527001004240:vpc/vpc-08294235aa02e1568
- arn:aws:s3::veer-cloudtrail-logs
- arn:aws:s3::config-bucket-527001004240

## Screenshot 2- VPC Non-compliant

-> Solving one finding, identified VPC flow logs as non-compliant in CIS Benchmark

The screenshot displays the AWS Security Hub console for the eu-north-1 region, specifically the 'Security standards' section for the CIS AWS Foundations Benchmark v1.2.0. The left sidebar shows the navigation menu with 'Security standards' selected. The main content area is titled 'Checks (1)' and shows a list of findings. The finding is identified as 'VPC flow logs as non-compliant' and is marked as 'FAILED'.

| Compliance Status | Workflow | Account      | Region     | Resource                      |
|-------------------|----------|--------------|------------|-------------------------------|
| FAILED            | NEW      | 527001004240 | eu-north-1 | EC2 VPC vpc-08294235aa02e1568 |

# Screenshot 3- VPC fix details

-> Configured VPC flow logs by setting traffic type to all

The screenshot shows the AWS VPC console for the VPC **fl-0b65265eb0d34b230** in the **eu-north-1** region. The left sidebar shows the navigation menu with options like VPC dashboard, Virtual private cloud, and Security. The main content area displays the details of the flow log, including its ID, Name, State (Active), Creation Time, Destination Type (cloud-watch-logs), Destination Name (vpc-log-flow-trial), Traffic Type (ALL), Max Aggregation Interval (10 minutes), Log Format (Default), File Format, Hive Compatible Partitions, and Partition Logs. The Tags section is also visible at the bottom.

| Details   |  |   |  |
|---|--|---|--|
| <b>Flow Log ID</b><br>fl-0b65265eb0d34b230                            | <b>Destination Type</b><br>cloud-watch-logs  | <b>Traffic Type</b><br>ALL                    | <b>File Format</b><br>-                |
| <b>Name</b><br>-  | <b>Destination Name</b><br><a href="#">vpc-log-flow-trial</a>                              | <b>Max Aggregation Interval</b><br>10 minutes | <b>Hive Compatible Partitions</b><br>- |
| <b>State</b><br>Active  | <b>IAM Role</b><br><a href="#">arn:aws:iam::527001004240:role/service-role/AWSflowlogs</a> | <b>Log Format</b><br>Default                  | <b>Partition Logs</b><br>-             |
| <b>Creation Time</b><br>Saturday, August 2, 2025 at 00:11:58 GMT+5:30 | <b>Cross Account IAM Role</b><br>-   |   |  |

# Screenshot 4- VPC-Compliant

-> Re-scanned VPC showing CIS compliance achieved

The screenshot shows the AWS Security Hub console for the **CIS AWS Foundations Benchmark v1.2.0** in the **EC2.6** category. The left sidebar shows the navigation menu with options like Security Hub CSPM, Summary, Controls, Security standards, Insights, Findings, Integrations, Management, and Settings. The main content area displays the results of the benchmark scan, showing a **PASSED** status. The table below lists the checks and their details.

| Compliance Status | Workflow | Account      | Region     | Resource                      | Investigate                 |
|-------------------|----------|--------------|------------|-------------------------------|-----------------------------|
| <b>PASSED</b>     | RESOLVED | 527001004240 | eu-north-1 | EC2 VPC vpc-08294235aa02e1568 | <a href="#">Config rule</a> |