

# DataGuardian Pro

## GDPR Compliance Scan Report

Generated on: May 01, 2025 21:31

Scan ID: SOC-20250501-333b4d

## Executive Summary

This report presents the findings of a SOC2 compliance analysis conducted on <https://github.com/vishaal314/terrascan> (branch: **master**) on **2025-05-01 21:30:58**. The scan identified a total of **161** compliance issues with **129** high-risk items. The overall compliance score is **99/100**. **Technologies Detected:** kubernetes, cloudformation, pulumi, docker, terraform, ansible, javascript Each finding in this report is mapped to specific SOC2 Trust Services Criteria (TSC) to help you understand how it impacts your compliance posture. The TSC categories include: • CC: Common Criteria (Security) • A: Availability • PI: Processing Integrity • C: Confidentiality • P: Privacy

Scan Type	soc2
Repository URL	<a href="https://github.com/vishaal314/terrascan">https://github.com/vishaal314/terrascan</a>
Branch	master
Date & Time	2025-05-01 21:30:58
Technologies	kubernetes, cloudformation, pulumi, docker, terraform, ansible, javascript
Compliance Score	99/100
IaC Files Found	1662
Total Files Scanned	2202
High Risk Issues	129
Medium Risk Issues	32
Low Risk Issues	0
Security Issues	146
Availability Issues	10
Confidentiality Issues	5

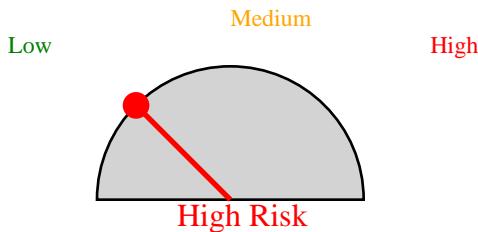
# Risk Assessment



## GDPR Compliance Protection

High risk of potential GDPR fines - immediate action required

Potential fines up to €20 million or 4% of global revenue



This scan has identified a high number of high-risk PII items. Immediate action is recommended to ensure GDPR compliance and protect sensitive data.

# Data Sustainability Compliance

Data sustainability measures how efficiently your organization manages personal data in compliance with GDPR principles of data minimization, storage limitation, and purpose limitation. A higher score indicates better long-term data governance practices.



Measures resource optimization, code efficiency, and energy consumption

## Detailed Findings

File	Line	Description	Risk	Category	SOC2 TSC
deploy/helm/templates/32_main.tf	Container not running as non-root user	Container not running as non-root user	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/1/main.tf	AWS provider without version constraint	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/1/test_provider.go	Container allowed to escalate privileges	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/1/test_provider.go	Container allowed to escalate privileges	Container allowed to escalate privileges	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/cli/testdata/run-test/14/web.tf	Security group with unrestricted ingress	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/cli/testdata/run-test/20/web.tf	Security group with unrestricted ingress	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/downloader/module/57_download.go	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan/107.go	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/file-scan/205.go	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.go/65	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/start.go/96	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/21-scan.go	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/28-scan.go	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/41-scan.go	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/webhook/24-scan.go	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/assets/6/bootstrap.go	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/http-server/testdata/1/testconfig.go	AWS provider without version constraint	AWS provider without version constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/http-server/testdata/50/testconfig.go	Security group with unrestricted ingress	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/http-server/testdata/58/testconfig.go	Security group with unrestricted ingress	Security group with unrestricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/iac-providers/cft/v12/testdata/11_impute/13_deploy.go	Administrator/Deployment access	Administrator/Deployment access	HIGH	Security	CC6.1, CC6.3
pkg/iac-providers/cft/v17/testdata/38_impute/13_deploy.go	Administrator/Deployment access	Administrator/Deployment access	HIGH	Confidentiality	C1.1
pkg/iac-providers/cft/v12/testdata/11_impute/13_deploy/template.go	Administrator/Deployment access	Administrator/Deployment access	HIGH	Security	CC6.1, CC6.3
pkg/iac-providers/cft/v17/testdata/38_impute/13_deploy/template.go	Administrator/Deployment access	Administrator/Deployment access	HIGH	Confidentiality	C1.1
pkg/iac-providers/dock40v1/parts/10_hardcoded.go	Hard-coded credentials or secrets	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/iac-providers/kube167/testset/v1/testusing/k8s/Testplatform.go	Administrator/Deployment access	Administrator/Deployment access	HIGH	Security	CC6.1, CC6.8
pkg/iac-providers/kube167/testset/v1/testusing/k8s/Testplatform.go	Administrator/Deployment access	Administrator/Deployment access	HIGH	Security	CC6.1, CC6.8
pkg/iac-providers/kube155/testset/v1/testdata/15_impute/13_deploy.go	Administrator/Deployment access	Administrator/Deployment access	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/kube155/testset/v1/testdata/15_impute/13_deploy.go	Administrator/Deployment access	Administrator/Deployment access	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/kube155/testset/v1/testdata/15_impute/13_deploy/privilegeddata.yml	Administrator/Deployment access	Administrator/Deployment access	HIGH	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1



pkg/iac-providers/terraform/v1	19	2 Best practice for configuring restricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/iac-providers/terraform/v1	55	2 Best practice for configuring restricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/iac-providers/terraform/v1	59	2 Avoid delay with unselected resources	HIGH	Security	CC6.1, CC6.3
pkg/iac-providers/terraform/v1	44	4 AWS Sptaplatform module constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/terraform/v1	44	4 AWS Sptaplatform module less than constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/terraform/v1	44	4 AWS Sptaplatform module less than or equal constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/terraform/v1	44	4 AWS Sptaplatform module less than or equal to constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/terraform/v1	43	3 Best practice for configuring restricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/iac-providers/terraform/v1	44	4 AWS Sptaplatform module constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/terraform/v1	19	4 Best practice for configuring restricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/iac-providers/terraform/v1	55	4 Best practice for configuring restricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/iac-providers/terraform/v1	59	4 Avoid delay with unselected resources	HIGH	Security	CC6.1, CC6.3
pkg/iac-providers/terraform/v1	54	5 AWS Sptaplatform module constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/terraform/v1	54	5 AWS Sptaplatform module less than constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/terraform/v1	54	5 AWS Sptaplatform module less than or equal constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/terraform/v1	54	5 AWS Sptaplatform module less than or equal to constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/terraform/v1	53	3 Best practice for configuring restricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/iac-providers/terraform/v1	54	4 AWS Sptaplatform module constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
pkg/iac-providers/terraform/v1	19	5 Best practice for configuring restricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/iac-providers/terraform/v1	55	5 Best practice for configuring restricted ingress	HIGH	Security	CC6.6, CC6.7
pkg/iac-providers/terraform/v1	59	5 Avoid delay with unselected resources	HIGH	Security	CC6.1, CC6.3
pkg/initialize/run.go	76	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/k8s/admission-webhook/v1	67	Validating webhook credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/k8s/admission-webhook/v1	73	Validating webhook credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/k8s/admission-webhook/v1	92	Validating webhook credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/k8s/admission-webhook/v1	67	Validating webhook credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/k8s/dblogs/webhook/12-scan-loggerexec function	12	Loggerexec function	HIGH	Security	CC6.1, CC6.8, CC7.2
pkg/k8s/dblogs/webhook/20-scan-loggerexec function	20	Loggerexec function	HIGH	Security	CC6.1, CC6.8, CC7.2
pkg/mapper/iac-provider/arm/config/audit/credentials or secrets	26	Config audit credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider/arm/config/audit/credentials or secrets	26	Config audit credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider/arm/config/audit/credentials or secrets	26	Config audit credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider/arm/config/audit/credentials or secrets	27	Config audit credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7

pkg/mapper/iac-provider	des/arm/ <del>Hard-coded credentials or secrets</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/arm/ <del>Hard-coded credentials or secrets</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/arm/ <del>Hard-coded parameters</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/arm/ <del>Hard-coded resource identity</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/arm/ <del>Hard-coded roles</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/arm/ <del>Hard-coded variables</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/cft/ <del>Untyped/old-style credentials or secrets</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/cft/ <del>Untyped/old-style credentials or secrets</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/cft/st/ <del>Untyped</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/cft/st/ <del>Untyped</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/cft/st/ <del>Untyped</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/mapper/iac-provider	des/cft/st/ <del>Untyped</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/notifications/webhook	22k/webhook/ <del>Hard-coded credentials or secrets</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/policies/opa/rego/aws_lambda	<del>Hard-coded function arn and data encrypted with Kms</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/policies/opa/rego/k8s_kubeconfig	<del>Hard-coded appender profile secrets</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/utils/skip_rules_test	129 S3 bucket with public read access	HIGH	Confidentiality	C1.1
pkg/utils/http/request.go	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/acr.go	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/acr.go	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/gcr.go	Possible hard-coded password	HIGH	Security	CC6.1, CC6.7
pkg/vulnerability/harbo850	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/harbo740	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
pkg/vulnerability/harbo830st.go	Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/scan/scan_test	3.16 Hard-coded credentials or secrets	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/test_data/iac/aws/aws_aws_lambda	<del>AWS provider without version constraint</del>	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
test/e2e/test_data/iac/aws/aws_aws_lambda	<del>AWS provider violation of version constraint</del>	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
test/e2e/test_data/iac/aws/aws_aws_lambda	<del>aws lambda - violates password</del>	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/aws/aws_aws_lambda	<del>aws lambda - violates password</del>	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/aws/aws_aws_lambda	<del>aws lambda - violates password</del>	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/aws/aws_aws_lambda	<del>aws lambda - violates password</del>	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/aws/aws_aws_lambda	<del>aws lambda - violates password</del>	HIGH	Security	CC6.1, CC6.7

test/e2e/test_data/iac/1aws	Possible shared violation password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/18aws	Possible shared violation password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/19aws	Possible shared violation password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/89aws	Possible shared violation password	HIGH	Confidentiality	C1.1
test/e2e/test_data/iac/102aws	Possible shared violation password	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/118aws	Possible shared violation password	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/116aws	Possible shared violation password	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/125aws	Possible shared violation password	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/141aws	Possible shared violation password	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/142resource	Possible shared password terraform/main.tf	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/143resource	Possible shared password terraform/main.tf	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/143resource	Possible shared password severity_set/terraform/main.tf	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/142resource	Possible shared password terraform/main.tf	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/143resource	Possible shared password skip_rule/terraform/main.tf	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/145resource	AWS Spring IDEN without retain constraint	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
test/e2e/test_data/iac/146resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/147resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/148resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/149resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/150resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/151resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/152resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/153resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/154resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/155resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/156resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/157resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/158resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/159resource	Possible shared password	HIGH	Security	CC6.1, CC6.7
test/e2e/test_data/iac/160resource	Skipping/tenant memory option disabled	HIGH	Confidentiality	C1.1
test/e2e/test_data/iac/161resource	Skipping/tenant backup option disabled	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/162resource	Skipping/tenant backup option disabled	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/163resource	Skipping/tenant backup option disabled	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/164resource	Skipping/tenant backup option disabled	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/165resource	Skipping/tenant backup option disabled	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/166resource	Skipping/tenant backup option disabled	MEDIUM	Availability	A1.2, A1.3
test/e2e/test_data/iac/167resource	AWS provider Folder1/subFolder2/constraint.tf	MEDIUM	Security	CC1.1, CC1.2, CC1.3, CC1.4, CC2.1
test/e2e/validatingweb140ok/validatingweb140ok	Validating web secrets	HIGH	Security	CC6.1, CC6.6, CC6.7

test/e2e/validatingwebhook/v16	<del>Hardcoded credentials or secrets</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/validatingwebhook/v17	<del>Hardcoded credentials or secrets</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/vulnerability/v12	<del>Hardcoded credentials or secrets</del>	HIGH	Security	CC6.1, CC6.6, CC6.7
test/e2e/vulnerability/v14	<del>Hardcoded credentials or secrets</del>	HIGH	Security	CC6.1, CC6.6, CC6.7

## SOC2 Trust Services Criteria (TSC) Explanation

SOC2 Trust Services Criteria refer to the specific control points used to assess compliance:

- CC: Common Criteria (security)
- A: Availability
- PI: Processing Integrity
- C: Confidentiality
- P: Privacy

Each finding in this report references specific TSC criteria to help understand how it impacts compliance posture.

## Recommendations & Next Steps

- Implement a formal process for assigning and managing access rights in accordance with the principle of least privilege.
- Develop a comprehensive risk management process that includes automated scanning strategies for Infrastructure-as-Code.
- Conduct periodic reviews of security configurations and apply best practices across all SOC2 Trust Services Criteria.
- Document and verify all control measures relevant to the TSC criteria noted in the findings.
- Implement automated compliance checks in CI/CD pipelines to detect deviations early in the development cycle.

## High-Risk Item Recommendations

- Prioritize immediate remediation of high-risk findings related to CC security-critical components.
- Implement strict access controls for sensitive infrastructure components applying the principle of least privilege.
- Conduct detailed risk assessment for all Common Criteria-related findings.
- Document and test incident response processes for all high-risk vulnerabilities.
- Install an automated validation process that checks IaC changes before they are applied to production environments.

## Data Sustainability Recommendations

- Implement data minimization practices to collect only necessary personal data.
- Establish clear data retention periods and automated deletion processes.
- Regularly audit and clean databases to remove redundant or obsolete data.
- Design systems with privacy by design principles to improve sustainability.
- Consider data storage optimization to reduce environmental impact of data centers.

## Scan Metadata

Scan ID	333b4d5d-436f-43b7-b427-5bb3b5212d9e
Scan Type	soc2
Region	Global
Timestamp	2025-05-01 21:30:58
Repository Provider	GitHub
Repository URL	Not available
Repository Path	Not available
Branch	master
Username	vishaal
Files Scanned	2202
CC Findings	0
A Findings	0
PI Findings	0
C Findings	0
P Findings	0

Disclaimer: This report is provided for informational purposes only and should not be considered legal or compliance advice. The findings in this report are based on automated scanning and may not identify all SOC2-relevant security issues. The Trust Services Criteria (TSC) mapping is intended as guidance. We recommend consulting with a qualified SOC2 auditor or compliance specialist for specific SOC2 compliance guidance.