How Compliance Assessment Works

Compliance regulations help companies improve their information security strategies by providing recommendations, guidelines, and best practices relevant to their product profiles, domains, and business practices. For example, the PCI-DSS standard is designed to protect customer credit card information and reduce fraud in companies that handle credit card information. Poor compliance can result in official fines and security incidents.

Most companies seek to adhere to the recommendations of at least one relevant compliance regulation. For example, medical companies follow the HIPAA framework, while companies that utilize AWS and GCP cloud infrastructures follow CIS AWS and CIS GCP benchmarks.

Official compliance regulations can be described as a broad range of assessment concepts and control restriction resolution levels that vary widely in specificity:

- Some guidelines lack detailed compliance control lists entirely, e.g. GDPR
- Others provide sets of control groups while offering the freedom to choose relevant scopes, e.g. NIST SP 800-53
- The most specific provide detailed and restrictive sets of configuration tests that must be adhered to, e.g. the CIS benchmarks

Disclaimer

> ⚠ The built-in compliance frameworks in Wiz are not designed to fully ensure compliance with a specific governance or compliance standard. Organizations are responsible for making sure their assessment meets applicable legal and regulatory requirements.
>
> Since each organization has a unique compliance assessment based on its product profile, domain, and business practices, and since official auditing is based on a custom compliance process and requirements, it is recommended to create a custom framework in Wiz (which can be based on the built-in one).
>
> The requirements under compliance frameworks may differ between organizations, so achieving full compliance may require you to perform

> independent reviews, take certain actions, and/or implement certain controls.

> 🎞 You can watch our webinar on secure configuration & compliance.

How it works

Our wizards map recommendations from each supported compliance framework to built-in Controls, Cloud Configuration Rules, and Host Configuration Rules in Wiz. This process varies somewhat between benchmark guidelines and non-restrictive guidelines. For frameworks with multiple versions, existing Rules are mapped to each new version as long as the Rule logic and metadata haven't changed.

Wiz supports two types of compliance frameworks:

1. Built-in frameworks:
   i. Cloud assessment frameworks—Related to the cloud vendors and official regulations. For example, ISO 27001, SOC2, CIS AWS, CIS Azure, and FedRamp.
   ii. Host configuration assessment frameworks—Related to OS and application hardening and compliance. For example, CIS Ubuntu Linux 22.04 LTS Benchmark, Windows Server 2022 Benchmark, and CIS Red Hat Enterprise Linux 8 Benchmark.
2. Custom frameworks: can mix and match Controls, Cloud Configuration Rules, and Host Configuration Rules. Learn how to create a custom framework.

Benchmark guidelines

For benchmark guidelines, Wiz implements dedicated Controls and Cloud Configuration Rules that follow the technical recommendations of the benchmark.

CIS benchmarks

The CIS benchmarks are a great starting point to measure your organization's compliance posture. You can use them out of the box to compare the compliance scores of your Wiz Projects or integrate them with your overall compliance policy.

Being an auditing rather than a risk assessment tool, the recommendations are not assigned severities for prioritization but focus on whether settings align with desired configurations. As such, they offer a baseline for strong configurations, alleviating the need for extensive risk assessment for every configuration option. If you want to prioritize failed results, you should determine your risk tolerance and perform a risk assessment considering factors such as the necessity of configurations and the potential impacts of misuse. CIS does, however, facilitate some prioritization by dividing its benchmarks into levels; level 1 covers the most essential recommendations while level 2 (and sometimes 3) covers more stringent security configurations.

CIS labels each recommendation as either manual or automated. Wiz tries to cover as many automated recommendations as possible. Manual recommendations require human analysis according to CIS, though there are cases where Wiz can assess them.

CIS Benchmark Assessment Certifications

Wiz holds CIS Benchmark Assessment Certification for CIS benchmarks assessment. These certifications were awarded after CIS inspected Wiz and ensured we cover and adequately assess its required recommendations by our built-in automated Policies. See below the complete certification list and examine the detailed documentation.

By working according to the latest version of a CIS benchmark, for which Wiz is certified, you can rest assured that your organization is following the latest security guidelines. Moreover, by relying on a certified baseline for CIS benchmarks and security best practices, your team can focus on remediation and close gaps without spending time on assessment and customization. Learn more about CIS Benchmark Assessment Certification.

Non-restrictive guidelines

Guidelines that lack detailed lists of controls, such as NIST SP 800, CIS Controls, GDPR, and PCI, are more challenging to map in Wiz; this is because parts of the compliance regulations are not written as restrictive, specific requirements that can be easily understood and translated into actionable steps.

We assign all relevant built-in Cloud Configuration Rules and Controls to appropriate categories and sub-categories in order to provide improved visibility as you work to achieve compliance. The framework, category, and subcategory scores represent a baseline to perform an ongoing assessment, remediate the Cloud Configuration Findings, and improve your organization’s alignment with the relevant framework. This ongoing process gives you transparency to achieve overall technical cloud domain compliance.

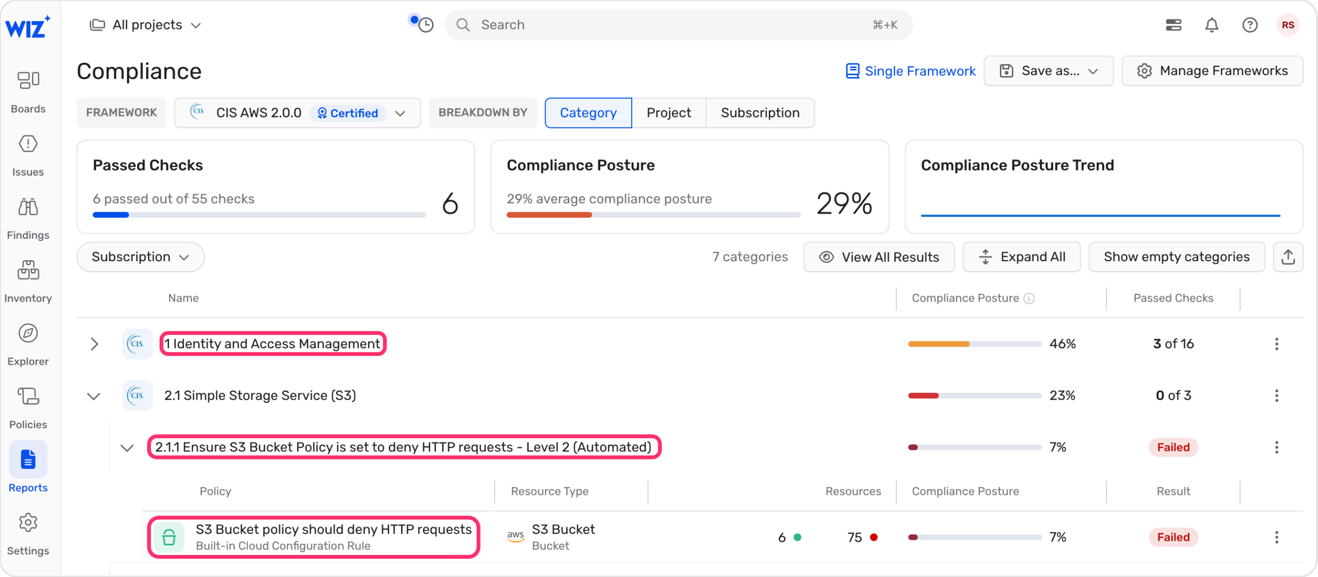
Technical vs. procedural controls

Categories and recommendations in Wiz relate to technical aspects, not procedural recommendations. For instance, in SOC2.8 Change Management, section "SOC2.CC8.1 Tracks System Changes" recommends that there be "a process... in place to track system changes prior to implementation". The "Tracks System Changes" control is procedural; it is something that security personnel must *do*. The Cloud Configuration Rules assigned to this category support this process by ensuring resources are being monitored, but they do not verify that the recommended procedure was performed.

Consider another example: Wiz cannot *enforce* a procedural recommendation like in CIS Azure v1.4.0 to "ensure guest users are reviewed on a monthly basis". Wiz can only provide visibility into guest users so that your security personnel can perform the review.

Framework structure

To the greatest extent possible, the requirements of every built-in framework are mapped to categories and sub-categories in Wiz.



Compliance

Single Framework | Save as... | Manage Frameworks

FRAMEWORK: CIS AWS 2.0.0 Certified

BREAKDOWN BY: Category | Project | Subscription

Passed Checks: 6 passed out of 55 checks — 6

Compliance Posture: 29% average compliance posture — 29%

Compliance Posture Trend

Subscription | 7 categories | View All Results | Expand All | Show empty categories

Name	Compliance Posture	Passed Checks
1 Identity and Access Management	46%	3 of 16
2.1 Simple Storage Service (S3)	23%	0 of 3
2.1.1 Ensure S3 Bucket Policy is set to deny HTTP requests - Level 2 (Automated)	7%	Failed

Policy	Resource Type	Resources	Compliance Posture	Result
S3 Bucket policy should deny HTTP requests Built-in Cloud Configuration Rule	S3 Bucket Bucket	6 ● 75 ●	7%	Failed

- Framework—The drop-down lists all frameworks, both built-in and custom. See the list of all supported frameworks below.
- Category—A chapter, section, or article (terminology varies) from the source compliance framework, e.g. "1 Identity and Access Management", along with the posture for that category and the number of checks that passed.
- Sub-Category—A sub-chapter, sub-section, or article (terminology varies) from the source compliance framework, e.g. "2.1.1 Ensure S3 Bucket Policy is set to deny HTTP requests - Level 2 (Automated)", along with the posture for that sub-category and whether the sub-category passed or failed.
- Policy—Controls, Cloud Configurations Rules, and Host Configuration Rules in a sub-category, e.g. "S3 Bucket policy should deny HTTP requests", along with the type of resource that is assessed, the number of resources that passed and failed the Control or Rule, the posture score, and the overall result.
- Passed checks—For a category, the number of sub-categories with status Passed out of the total number of assessed sub-categories (sub-categories with status No Resources or No Policies are excluded). For a sub-category or policy, the assessment status.

Assessment statuses

Each mapped Wiz Policy (Control, Cloud Configuration Rule, and Host Configuration Rule) and sub-category, and some categories, are assigned a status:

	Policy	Sub-category	Category
Failed	At least one resource generated an Issue (for a Control) or failed a	The sub-category includes at least	Read below about the compliance

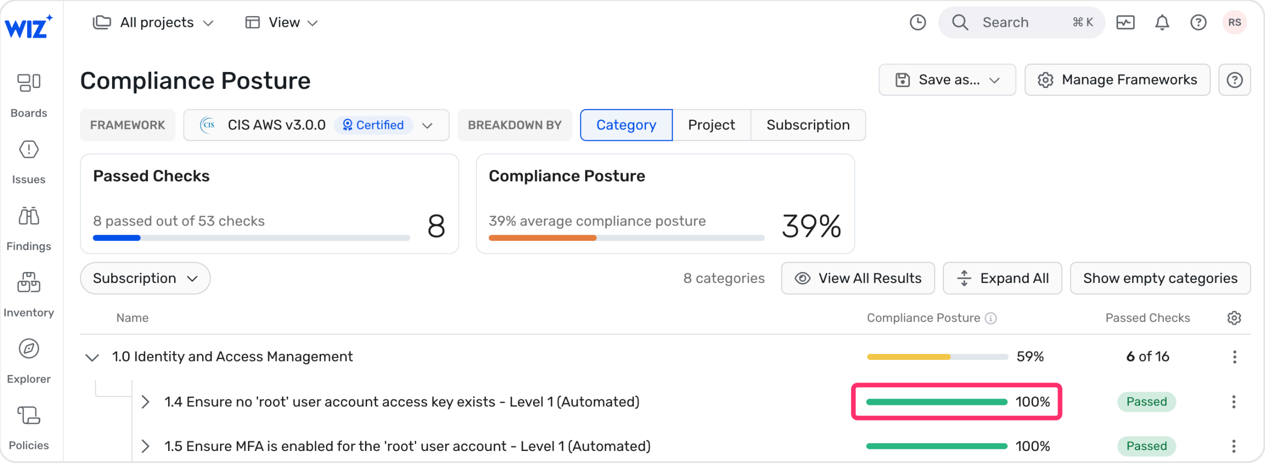
	Policy	Sub-category	Category
	configuration check (for a Cloud Configuration Rule or Host Configuration Rule)	one Policy with status Failed	posture score of categories
Passed	All assessed resources meet the requirements of the Policy	All Policies in the sub-category have status Passed	Read below about the compliance posture score of categories
No Resources [1]	There are no assessable resources in your environment (and therefore, no score is assigned to the Policy)	—	—
Rejected	At least one resource generated an Issue that was manually marked `rejected` by the user (such Issues do not impact compliance scores)	—	—
No Policies	—	No Policies are mapped to the sub-category (and therefore, no score is assigned to it)	—
Not Assessed	—	—	All sub-categories have the status `No Policies` or `No Resource` (and therefore, no score is assigned to the category)

> [1] Most of the time, the `No Resources` status reduces noise and improves the accuracy of the overall compliance posture score. However, sometimes the lack of assessable resources is itself a problem. For instance, a Cloud Configuration Rule like Activity log alert for 'Update or Create Network Security Group Rule' does not exist should always find assessable resources. Be sure to thoroughly inspect all Policies with this status.

Compliance posture scores

Overall compliance posture score is the best indicator of your organization's overall adherence to a given framework.

Sub-category scores



Compliance Posture

FRAMEWORK: CIS AWS v3.0.0 Certified — BREAKDOWN BY: Category | Project | Subscription

Passed Checks: 8 passed out of 53 checks — 8

Compliance Posture: 39% average compliance posture — 39%

Subscription — 8 categories

Name	Compliance Posture	Passed Checks
1.0 Identity and Access Management	59%	6 of 16
1.4 Ensure no 'root' user account access key exists - Level 1 (Automated)	100%	Passed
1.5 Ensure MFA is enabled for the 'root' user account - Level 1 (Automated)	100%	Passed

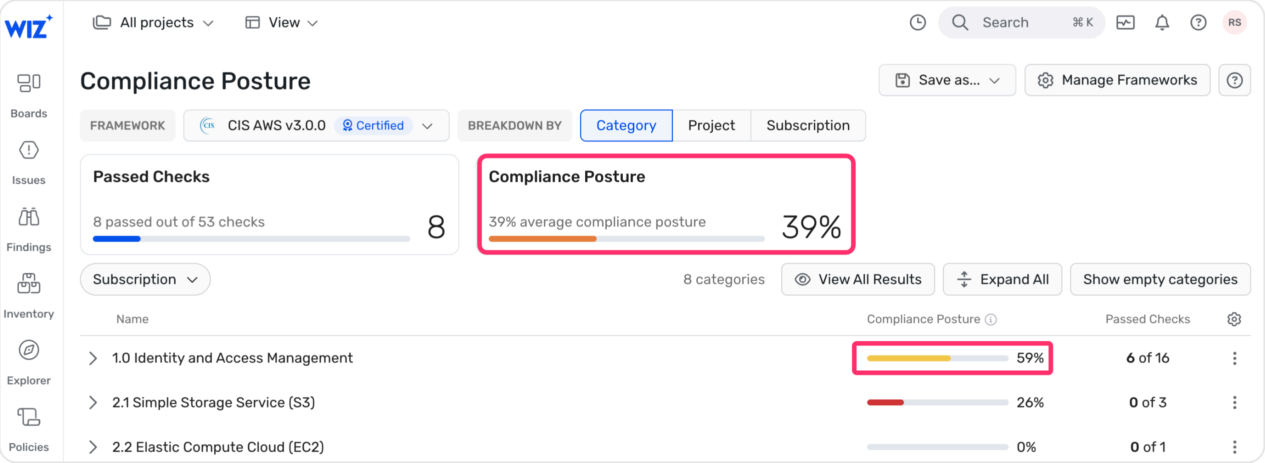
Compliance postures for each sub-category are percentages calculated as the total number of passed resources divided by the total number of assessed resources, i.e.

Sub-category score = $(P_1 + P_2 + \dots + P_n) \div (P_1 + P_2 + \dots + P_n + F_1 + F_2 + \dots + F_n)$

where:

- P_m is the number of resources that passed the m^{th} Control or Rule
- F_m is the number of resources that failed the m^{th} Control or Rule
- $1 < m < n$
- n is the number of Controls and Rules in the sub-category with assessable resources

Category and framework scores



Compliance Posture

FRAMEWORK: CIS AWS v3.0.0 Certified — BREAKDOWN BY: Category | Project | Subscription

Passed Checks: 8 passed out of 53 checks — 8

Compliance Posture: 39% average compliance posture — 39%

Subscription — 8 categories

Name	Compliance Posture	Passed Checks
1.0 Identity and Access Management	59%	6 of 16
2.1 Simple Storage Service (S3)	26%	0 of 3
2.2 Elastic Compute Cloud (EC2)	0%	0 of 1

Compliance posture scores for each framework and category are percentages calculated recursively, i.e.

Category score = ($SC_1 + SC_2 + \ldots + SC_r$) ÷ r

and

Framework score = ($C_1 + C_2 + \ldots + C_s$) ÷ s

where:

- SC_t is the score of the t^{th} sub-category
- C_u is the score of the u^{th} category
- r is the number of sub-categories in a given category
- s is the number of categories in a given framework

Score exclusions

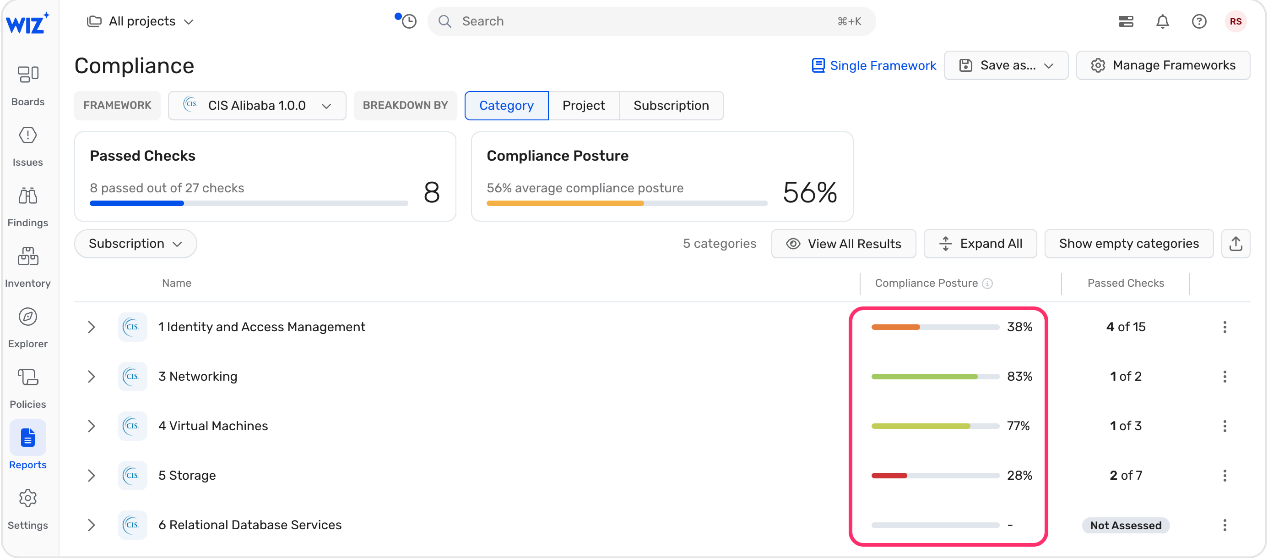
The following categories, sub-categories, and Policies are excluded from score calculations:

- `Not Assessed`—There are no valid sub-category scores.
- `No Resources`—There are no matching resource types in your environment.
- `Disabled`—Policies that were disabled by users or are built-in Rules related to uncommon use cases that require customer action to enable.
- `Rejected`—Issues that were manually marked as rejected by users.

Score examples

Framework score

There are five categories in the CIS Alibaba 1.0.0 framework, but one of them is marked `Not Assessed` because it has no assessable resources. Its overall compliance score is (38% + 83% + 77% + 28%) ÷ 4 = 56%.



Compliance

FRAMEWORK: CIS Alibaba 1.0.0 — BREAKDOWN BY: Category | Project | Subscription

Passed Checks
8 passed out of 27 checks — 8

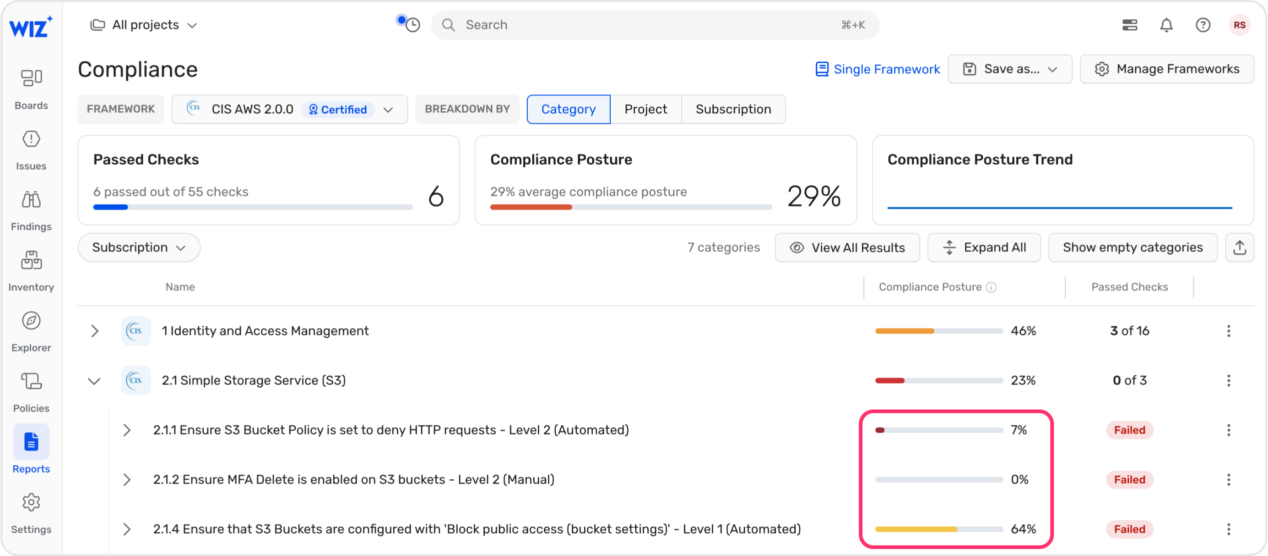
Compliance Posture
56% average compliance posture — 56%

Subscription — 5 categories

Name	Compliance Posture	Passed Checks
1 Identity and Access Management	38%	4 of 15
3 Networking	83%	1 of 2
4 Virtual Machines	77%	1 of 3
5 Storage	28%	2 of 7
6 Relational Database Services	-	Not Assessed

Category score

There are 3 sub-categories in the "2.1 Simple Storage Service (S3)" category. Its compliance score is (7% + 0% + 64%) ÷ 3 = 23%.



Compliance

FRAMEWORK: CIS AWS 2.0.0 Certified — BREAKDOWN BY: Category | Project | Subscription

Passed Checks
6 passed out of 55 checks — 6

Compliance Posture
29% average compliance posture — 29%

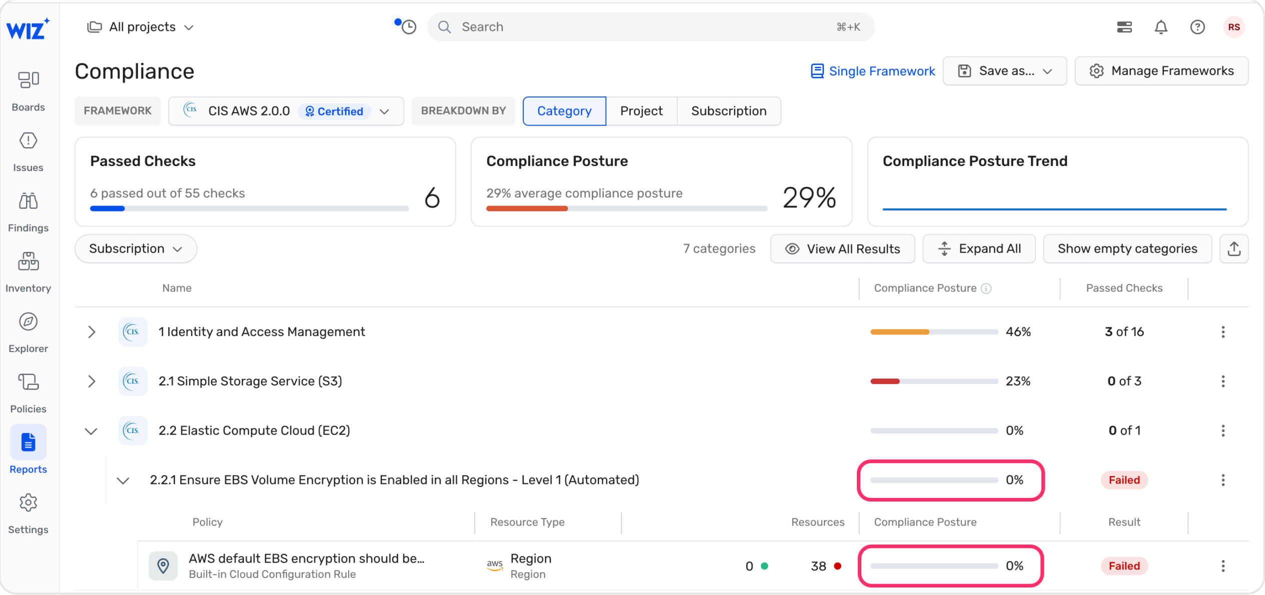
Compliance Posture Trend

Subscription — 7 categories

Name	Compliance Posture	Passed Checks
1 Identity and Access Management	46%	3 of 16
2.1 Simple Storage Service (S3)	23%	0 of 3
2.1.1 Ensure S3 Bucket Policy is set to deny HTTP requests - Level 2 (Automated)	7%	Failed
2.1.2 Ensure MFA Delete is enabled on S3 buckets - Level 2 (Manual)	0%	Failed
2.1.4 Ensure that S3 Buckets are configured with 'Block public access (bucket settings)' - Level 1 (Automated)	64%	Failed

Sub-category score

There is only one Policy in the "2.2.1 Ensure EBS Volume Encryption is Enabled in all Regions - Level 1 (Automated)" sub-category. Both the sub-category and Policy compliance scores are 0 ÷ (38) = 0%.



Compliance

FRAMEWORK: CIS AWS 2.0.0 Certified — BREAKDOWN BY: Category | Project | Subscription

Passed Checks — 6 passed out of 55 checks — 6

Compliance Posture — 29% average compliance posture — 29%

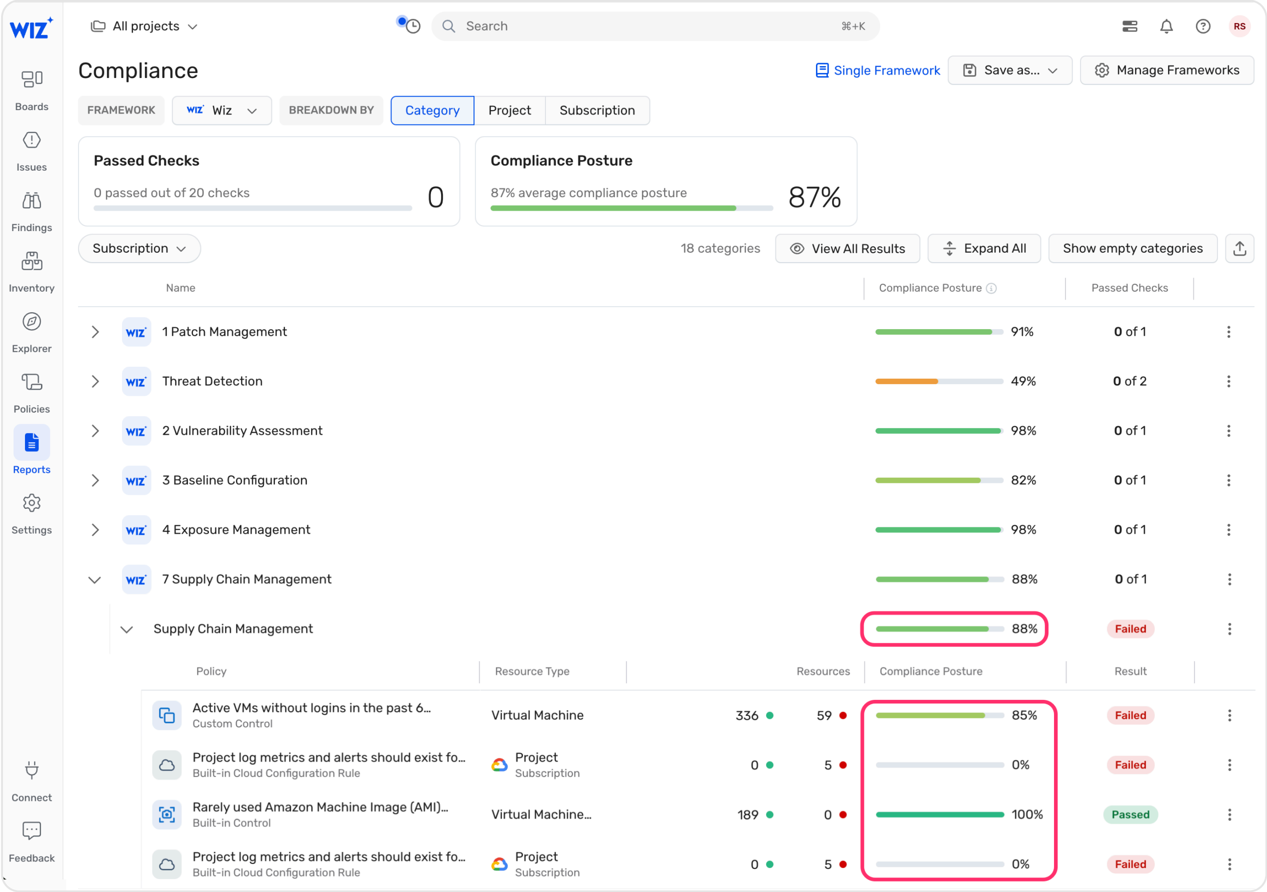
Compliance Posture Trend

Subscription — 7 categories

Name	Compliance Posture	Passed Checks
1 Identity and Access Management	46%	3 of 16
2.1 Simple Storage Service (S3)	23%	0 of 3
2.2 Elastic Compute Cloud (EC2)	0%	0 of 1
2.2.1 Ensure EBS Volume Encryption is Enabled in all Regions - Level 1 (Automated)	0%	Failed

Policy	Resource Type	Resources		Compliance Posture	Result
AWS default EBS encryption should be... Built-in Cloud Configuration Rule	Region Region	0 ●	38 ●	0%	Failed

There are 4 Policies in the 7 Supply Chain Management sub-category. Its compliance score is (336 + 189) ÷ (336 + 59 + 5 + 189 + 5) = 88%.



Compliance

FRAMEWORK: Wiz — BREAKDOWN BY: Category | Project | Subscription

Passed Checks — 0 passed out of 20 checks — 0

Compliance Posture — 87% average compliance posture — 87%

Subscription — 18 categories

Name	Compliance Posture	Passed Checks
1 Patch Management	91%	0 of 1
Threat Detection	49%	0 of 2
2 Vulnerability Assessment	98%	0 of 1
3 Baseline Configuration	82%	0 of 1
4 Exposure Management	98%	0 of 1
7 Supply Chain Management	88%	0 of 1
Supply Chain Management	88%	Failed

Policy	Resource Type	Resources		Compliance Posture	Result
Active VMs without logins in the past 6... Custom Control	Virtual Machine	336 ●	59 ●	85%	Failed
Project log metrics and alerts should exist fo... Built-in Cloud Configuration Rule	Project Subscription	0 ●	5 ●	0%	Failed
Rarely used Amazon Machine Image (AMI)... Built-in Control	Virtual Machine...	189 ●	0 ●	100%	Passed
Project log metrics and alerts should exist fo... Built-in Cloud Configuration Rule	Project Subscription	0 ●	5 ●	0%	Failed

Supported compliance frameworks

Host configuration assessment frameworks

Built-in host configuration assessment frameworks and assigned Rules are disabled by default. You can enable the necessary frameworks and Rules

> from the Reports > Compliance Frameworks page.

Logo	Platform	Benchmarks (Level 1 + Level 2)[1]
	Alibaba Cloud Linux	CIS Alibaba Cloud Linux (Aliyun Linux) 2 Benchmark v1.0.0 CIS Alibaba Cloud Linux (Aliyun Linux) 3 Benchmark v1.0.0 `(Latest)`
	AlmaLinux	CIS AlmaLinux OS 8 Benchmark v2.0.0 CIS AlmaLinux OS 8 Benchmark v3.0.0 `(Latest)` CIS AlmaLinux OS 9 Benchmark v1.0.0 `(Latest)`
	Amazon	CIS Amazon Linux Benchmark v2.0.0 CIS Amazon Linux 2 Benchmark v1.0.0.1 CIS Amazon Linux 2 Benchmark v2.0.0 CIS Amazon Linux 2 Benchmark v3.0.0 `(Latest)` CIS Amazon Linux 2 STIG Benchmark v2.0.0 `(Latest)` CIS Amazon Linux 2023 Benchmark v1.0.0 `(Latest)`
	CBL Mariner	CIS AKS Optimized Azure Linux Benchmark v1.0.0 `(Latest)`
	CentOS	CIS CentOS Linux 6 Benchmark v2.0.2 CIS CentOS Linux 6 Benchmark v3.0.0 `(Latest)` CIS CentOS Linux 7 Benchmark v3.0.0 CIS CentOS Linux 7 Benchmark v3.1.2 CIS CentOS Linux 7 Benchmark v4.0.0 `(Latest)` CIS CentOS Linux 8 Benchmark v1.0.0.1 CIS CentOS Linux 8 Benchmark v2.0.0 `(Latest)`
	Debian	CIS Debian Family Linux Benchmark v1.0.0 CIS Debian Linux 8 Benchmark v2.0.1 CIS Debian Linux 8 Benchmark v2.0.2 `(Latest)` CIS Debian Linux 9 Benchmark v1.0.1 CIS Debian Linux 10 Benchmark v1.0.0 CIS Debian Linux 10 Benchmark v2.0.0 `(Latest)` CIS Debian Linux 11 Benchmark v1.0.0 `(Latest)` CIS Debian Linux 12 Benchmark v1.0.1 `(Latest)`

Logo	Platform	Benchmarks (Level 1 + Level 2)[1]
		CIS Debian Linux 11 STIG Benchmark v1.0.0 `(Latest)`
	Fedora	CIS Fedora 19 Family Linux Benchmark v1.0.0 `(Latest)` CIS Fedora 28 Family Linux Benchmark v1.0.0 CIS Fedora 28 Family Linux Benchmark v2.0.1 `(Latest)`
	Microsoft Windows	CIS Microsoft Windows 8 Benchmark v1.0.0 `(Latest)` CIS Microsoft Windows 8.1 Workstation Benchmark v2.4.0 CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 `(Latest)` CIS Microsoft Windows 10 Enterprise Release 1903 Benchmark v1.7.1 `(Latest)` CIS Microsoft Windows 10 Enterprise Release 1909 Benchmark v1.8.1 `(Latest)` CIS Microsoft Windows 10 Enterprise Release 2004 Benchmark v1.9.0 CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0 `(Latest)`
	Microsoft Windows Server	CIS Azure Compute Microsoft Windows Server 2019 Benchmark v1.0.0 `(Latest)` CIS Azure Compute Microsoft Windows Server 2022 Benchmark v1.0.0 `(Latest)` CIS Microsoft Windows Server 2003 Benchmark v3.1.0 `(Latest)` CIS Microsoft Windows Server 2008 Benchmark v3.1.0 CIS Microsoft Windows Server 2008 (non-R2) Benchmark v3.3.1 `(Latest)` CIS Microsoft Windows Server 2008 R2 Benchmark v3.2.0 CIS Microsoft Windows Server 2008 R2 Benchmark v3.3.1 `(Latest)` CIS Microsoft Windows Server 2012 (non-R2) Benchmark v2.2.0 CIS Microsoft Windows Server 2012 (non-R2) Benchmark v2.4.0 CIS Microsoft Windows Server 2012 (non-R2) Benchmark v3.0.0 `(Latest)` CIS Microsoft Windows Server 2012 R2

Logo	Platform	Benchmarks (Level 1 + Level 2)[1]
		Benchmark v2.4.0 CIS Microsoft Windows Server 2012 R2 Benchmark v2.6.0 CIS Microsoft Windows Server 2012 R2 Benchmark v3.0.0 `(Latest)` CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark v1.2.0 CIS Microsoft Windows Server 2016 Benchmark v2.0.0 CIS Microsoft Windows Server 2016 Benchmark v3.0.0 `(Latest)` CIS Microsoft Windows Server 2016 STIG Benchmark v1.2.0 CIS Microsoft Windows Server 2016 STIG Benchmark v2.0.0 `(Latest)` CIS Microsoft Windows Server 2019 Benchmark v1.1.0 CIS Microsoft Windows Server 2019 Benchmark v1.3.0 CIS Microsoft Windows Server 2019 Benchmark v2.0.0 CIS Microsoft Windows Server 2019 Benchmark v3.0.0 CIS Microsoft Windows Server 2019 Benchmark v3.0.1 `(Latest)` CIS Microsoft Windows Server 2019 STIG Benchmark v1.1.0 CIS Microsoft Windows Server 2019 STIG Benchmark v2.0.0 `(Latest)` CIS Microsoft Windows Server 2022 Benchmark v1.0.0 CIS Microsoft Windows Server 2022 Benchmark v2.0.0 CIS Microsoft Windows Server 2022 Benchmark v3.0.0 `(Latest)` CIS Microsoft Windows Server 2022 STIG Benchmark v1.0.0 `(Latest)`
	NGINX	CIS NGINX Benchmark v1.1.0
	Oracle Linux	CIS Oracle Linux 6 Benchmark v1.0.0 CIS Oracle Linux 6 Benchmark v2.0.0 `(Latest)` CIS Oracle Linux 7 Benchmark v3.0.0 CIS Oracle Linux 7 Benchmark v3.1.1 CIS Oracle Linux 7 Benchmark v4.0.0 `(Latest)`

Logo	Platform	Benchmarks (Level 1 + Level 2)[1]
		CIS Oracle Linux 8 Benchmark v1.0.0.1 CIS Oracle Linux 8 Benchmark v2.0.0 CIS Oracle Linux 8 Benchmark v3.0.0 `(Latest)` CIS Oracle Linux 9 Benchmark v1.0.0 `(Latest)`
	PostgreSQL[2] (hosted technology)	CIS PostgreSQL 10 Benchmark CIS PostgreSQL 11 Benchmark v1.0.0 `(Latest)` CIS PostgreSQL 12 Benchmark v1.0.0 CIS PostgreSQL 13 Benchmark v1.0.0 CIS PostgreSQL 14 Benchmark v1.0.0 CIS PostgreSQL 15 Benchmark v1.1.0 `(Latest)`
	Red Hat Enterprise Linux	CIS Red Hat Enterprise Linux 5 Benchmark v2.2.0 CIS Red Hat Enterprise Linux 6 Benchmark v2.0.2 CIS Red Hat Enterprise Linux 6 Benchmark v3.0.0 `(Latest)` CIS Red Hat Enterprise Linux 7 Benchmark v3.0.0 CIS Red Hat Enterprise Linux 7 Benchmark v3.1.1 CIS Red Hat Enterprise Linux 7 Benchmark v4.0.0 `(Latest)` CIS Red Hat Enterprise Linux 7 STIG Benchmark v2.0.0 `(Latest)` CIS Red Hat Enterprise Linux 8 Benchmark v1.0.0.1 CIS Red Hat Enterprise Linux 8 Benchmark v2.0.0 CIS Red Hat Enterprise Linux 8 Benchmark v3.0.0 `(Latest)` CIS Red Hat Enterprise Linux 8 STIG Benchmark v1.0.0 `(Latest)` CIS Red Hat Enterprise Linux 9 Benchmark v1.0.0 `(Latest)`
	Rocky	CIS Rocky Linux 8 Benchmark v1.0.0 CIS Rocky Linux 8 Benchmark v2.0.0 `(Latest)` CIS Rocky Linux 9 Benchmark v1.0.0 `(Latest)`
SUSE	SUSE Linux Enterprise	CIS SUSE Linux Enterprise 11 Benchmark v2.0.0 CIS SUSE Linux Enterprise 11 Benchmark v2.1.1 `(Latest)` CIS SUSE Linux Enterprise 12 Benchmark v2.0.0 CIS SUSE Linux Enterprise 12 Benchmark v3.1.0

Logo	Platform	Benchmarks (Level 1 + Level 2)[1]
		`(Latest)` CIS SUSE Linux Enterprise 15 Benchmark v1.0.0 CIS SUSE Linux Enterprise 15 Benchmark v1.1.1 `(Latest)`
	Ubuntu Linux	CIS Ubuntu Linux 14.04 LTS Benchmark v2.0.0 CIS Ubuntu Linux 16.04 LTS Benchmark v1.0.0 CIS Ubuntu Linux 16.04 LTS Benchmark v2.0.0 `(Latest)` CIS Ubuntu Linux 18.04 LTS Benchmark v2.0.1 CIS Ubuntu Linux 18.04 LTS Benchmark v2.1.0 CIS Ubuntu Linux 18.04 LTS Benchmark v2.2.0 `(Latest)` CIS Ubuntu Linux 20.04 LTS Benchmark v1.0.0 CIS Ubuntu Linux 20.04 LTS Benchmark v1.1.0 CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.1 `(Latest)` CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0 CIS Ubuntu Linux 20.04 LTS STIG Benchmark v1.0.0 CIS Ubuntu Linux 20.04 LTS STIG Benchmark v2.0.0 `(Latest)`

> [1] CIS STIG benchmarks include more Rules to align with the STIG DISS requirements and comply with federal regulations. Learn more.
>
> [2] To assess your compliance with frameworks related to PostgreSQL, you must enable data scanning of hosted databases (IaaS) on the Settings > Scanners > Data Security page in Wiz.

Cloud assessment frameworks

Logo	Framework	Enabled by default[1] [2]	Region [3]
	APRA CPS 234	▯	Australia
	AWS Foundational Security Best Practices	▯	General
	AWS Well-Architected Framework (Section 2 - Security)	▯	General

Logo	Framework	Enabled by default[1] [2]	Region [3]
	CCF (The Adobe Common Controls Framework)	▯	General
	Azure Security Benchmark v3	▯	General
	C5 - Cloud Computing Compliance Criteria Catalogue	▯	Germany
	Canadian PBMM (ITSG-33)	▯	Canada
	CCPA/CPRA	▯	USA
CIS	CIS AKS v1.0.0 CIS AKS v1.2.0 Certified CIS AKS v1.3.0 Certified CIS AKS v1.4.0 Certified CIS AKS v1.5.0 `(Latest)`	▯	General
CIS	CIS Alibaba Cloud v1.0.0	▯	General
CIS	CIS AWS v1.2.0 CIS AWS v1.3.0 CIS AWS v1.4.0 Certified CIS AWS v1.5.0 Certified CIS AWS v2.0.0 Certified CIS AWS v3.0.0 Certified `(Latest)`	▯	General
CIS	CIS AWS Database Services Benchmark v1.0.0	▯	General
CIS	CIS Azure v1.1.0 CIS Azure v1.3.0 CIS Azure v1.4.0 Certified CIS Azure v1.5.0 Certified CIS Azure v2.0.0 Certified CIS Azure v2.1.0 Certified `(Latest)`	▯	General
CIS	CIS Controls v7.1 CIS Controls v8 `(Latest)`	▯	General
CIS	CIS Docker v1.5.0 CIS Docker v1.6.0 Certified `(Latest)`	▯	General

Logo	Framework	Enabled by default[1] [2]	Region [3]
	CIS EKS v1.0.1 CIS EKS v1.1.0 CIS EKS v1.2.0 Certified CIS EKS v1.3.0 Certified CIS EKS v1.4.0 Certified CIS EKS v1.5.0 `(Latest)`	□	General
	CIS GCP v1.1.0 CIS GCP v1.2.0 CIS GCP v1.3.0 Certified CIS GCP v2.0.0 Certified CIS GCP v3.0.0 Certified `(Latest)`	□	General
	CIS GitHub v1.0.0 `(Latest)`	□	General
	CIS GKE v1.1.0 CIS GKE v1.3.0 Certified CIS GKE v1.4.0 Certified CIS GKE v1.5.0 Certified CIS GKE v1.6.0 `(Latest)`	□	General
	CIS Kubernetes v1.6.1 CIS Kubernetes v1.7.0 Certified CIS Kubernetes v1.7.1 Certified CIS Kubernetes v1.8.0 Certified CIS Kubernetes v1.9.0 Certified `(Latest)`	□	General
	CIS OCI v1.1.0 CIS OCI v1.2.0 Certified CIS OCI v2.0.0 `(Latest)`	□	General
	CIS VMware ESXi 7.0 v1.1.0	□	General
	CMMC v2.0	□	USA
	CSA CCM v4.0.5	□	General
	Digital Operational Resilience Act (DORA)	□	EU
	Essential Eight	□	Australia
	FedRAMP (Moderate and Low levels)	□	USA

Logo	Framework	Enabled by default[1] [2]	Region [3]
	GDPR	□	EU
	HIPAA Security Rules	□	General
HT	HITRUST CSF v9.5.0 HITRUST CSF v11.2	□	General
ISO	ISO/IEC 27001	□	General
	Kubernetes Pod Security Standards (Baseline)	□	General
	Kubernetes Pod Security Standards (Restricted)	□	General
	Microsoft Cloud Security Benchmark v1	□	General
&	MITRE ATT&CK Matrix	□	General
	NIS2 Directive (Article 21)	□	EU
NIST	NIST SP 800-53 Revision 4 NIST SP 800-53 Revision 5	□	USA
NIST	NIST CSF v1.1	□	USA
NIST	NIST SP 800-171 Revision 2	□	USA
	NYDFS (23 NYCRR 500)	□	USA
	OpenSSF Source Code Management Platform Best Practices	□	General
	OWASP CI/CD Top 10	□	General
	OWASP Kubernetes Top 10	□	General
	OWASP ML Security Top 10	□	General
PCI	PCI DSS v3.1.0 PCI DSS v3.2.1 PCI DSS v4.0	□	General
SOC2	SOC 2 Type II	□	General

Logo	Framework	Enabled by default[1] [2]	Region [3]
	Secure Controls Framework (SCF)	▯	General
	UK Cyber Essentials	▯	UK
	VMware vSphere Security Configuration Guide	▯	General

> [1] Applies to new tenants only. To enable/disable a framework, go to [Reports > Compliance Frameworks](), search for the relevant framework, and click More options > Disable/Enable.
>
> [2] For frameworks enabled by default with multiple versions:
>
> - Only the latest version is enabled by default
> - For CIS frameworks - if Wiz is not yet certified for the latest, then the previous version is also enabled
>
> [3] The "Region" column provides geographical context to help you understand the regulatory landscape each framework operates within.

> Our wizards are hard at work on adding detailed documentation for each of the supported frameworks. Let us know if you have any suggestions or feedback.

Custom compliance frameworks

If the built-in compliance frameworks do not meet your organizational needs, you can create custom frameworks or assign custom Controls, custom Cloud Configuration Rules, and custom Host Configuration Rules to the built-in compliance frameworks. However, you *cannot* assign built-in Controls and Rules to built-in compliance frameworks. See the possible combinations in the table below:

	Built-in Framework	Custom Framework
Built-in Control	▯	▯
Built-in Cloud Configuration Rule	▯	▯

	Built-in Framework	Custom Framework
Built-in Host Configuration Rule	▯	▯
Custom Control	▯	▯
Custom Cloud Configuration Rule	▯	▯
Custom Host Configuration Rule	▯	▯

FAQ

Questions? Take a look at the FAQ.

Updated 4 days ago

← Compliance Solutions

CIS AKS 1.5.0 →