Cyscale

Cloud Compliance in 2023
An In-Depth Guide

1.

Predictions for the cloud for 2023

Cloud spending is predicted to grow by 20.7% in 2023 compared to 2022 [1]. Public cloud services have enormous advantages over on-premises and private cloud infrastructures.

Why is the cloud such a popular solution among companies? The most well-known advantages of the cloud are:

An efficient spending mechanism, with a **pay-as-you-go policy**. You only pay for what you use, therefore avoiding keeping servers running when you do not need them. You are only charged for the exact resources you use for the amount of time you need them.

The cloud is **highly scalable**; you can obtain more computing power without having to buy hardware; you can scale vertically, by adding more resources to your existing servers, or horizontally, by adding additional instances to your cloud environment.

Availability is offered by cloud providers using availability zones, which are areas in which cloud data is duplicated, to ensure that if one data center fails, a different one can step in.

Cloud Disaster Recovery or Cloud DR, refers to the plan of performing backup of data, applications, and services on the cloud; this strategy ensures that if a disaster occurs, no data is lost, and the company can resume its activity.

2.

Multi-cloud environments: are they better than using just one cloud provider?

Some companies choose to use multiple cloud providers for their data, applications, and code. The reason for this practice is that, by combining different services, you can extract what you want from each one and achieve an ideal, efficient environment.

However, incorporating services from multiple cloud providers into your systems and applications can quickly increase complexity. Each cloud has different services, security rules, and settings, which can become confusing. Moreover, in order to achieve compliance with international standards, you must correctly secure your multi-cloud environment, which can become a cumbersome task.

Multi-cloud is becoming increasingly popular, and security is sometimes compromised for performance. This can, in turn, increase risks and generate new attack paths.

3.

Why is compliance so important, and why should your company care about it?

Compliance with accredited standards shows that your company cares about customers' data security and makes efforts to ensure it. Think of it like a stamp of approval – everyone knows the stamp and trusts it; therefore, if you own it, you are considered trustworthy.

Since supply chain security has been a sensitive topic in 2022, with breaches affecting even high profile providers, compliance builds trust in the third-party vendors dedicating effort to strong data security programs.

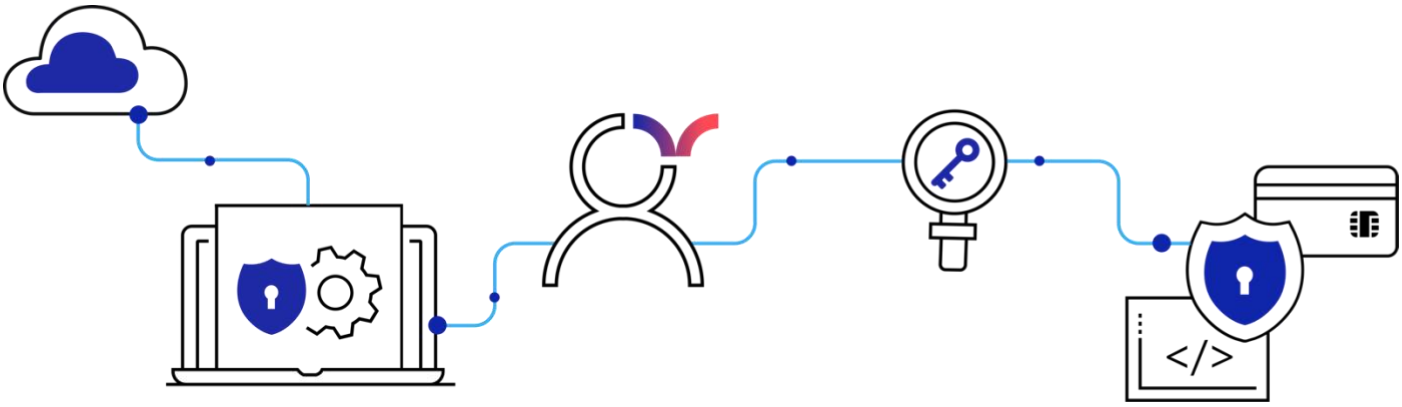
In addition to standards, there are also regulations that organizations are lawfully required to adhere to.

What happens if you fail to comply?

Financial penalties can reach astronomical figures; for example, for GDPR, a company can receive a fine of up to 20 mil. EUR for serious violations, while for HIPAA, criminal penalties can cause the wrong-doers to spend up to 10 years in jail, on top of fines.

In 2022, HIPAA applied a fine of 875,000 USD to Oklahoma State University due to an ePHI breach. [2] In the same year, Clearview AI Inc. was charged 20 mil. EUR for processing personal data illegally under GDPR. [3]

After understanding the importance of compliance, let’s dive deep into the requirements and specifications of three of the most popular compliance standards and two regulatory frameworks. After reading this guide, you will better understand the implications of implementing each framework and be equipped to take the first steps to becoming compliant in 2023.



4.1

ISO 27001:2022

ISO 27001, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), is a standard that defines security best practices for Information Security Management Systems (ISMSs).

It is important to note that this standard was updated in October 2022 and now has a new structure.

The best practices presented in this accreditation come under the form of controls which have to be implemented; the controls refer to the following aspects within a company: **Organizational, People, Physical, Technological.**

The 93 controls required for ISO 27001:2022 are grouped in the categories specified above.

There are 37 “Organizational” controls, located in section A.5., and they are related to various administrative elements:

- → Access control & authentication,
- → Contact with authorities,
- → Data classification,
- → Incident response,
- → Privacy of PHI, and many more.

This section also contains the control “Information security for use of cloud services”, which is a new control specifically related to cloud security.

The "People" category contains 8 controls that are related to remote working, the onboarding and offboarding of employees, non-disclosure agreements, and others. These controls are in section A.6.

In section A.7, under “Physical controls”, we have requirements that regulate the following:

- Physical security which includes perimeters, entry, rooms, monitoring,
- The protection and maintenance of equipment,
- A clear desk and clear screen policy, and others.

What is a clear desk and clear screen policy? This refers to locking computers and other devices when you are away from them.

The last category in ISO 27001:2022 is "Technological". Section A.8. refers to many technical aspects of security, such as:

- → Source code security,
- → Data encryption,
- → Malware protection,
- → Backups,
- → Logging and monitoring, and many more.

Validity

The ISO 27001 certification has a three-year validity, regardless of whether your company has certified against the new or the old version.

Companies who are in the process of certifying for ISO 27001:2013 can still complete the process until April 2024. The validity of the certification will last 3 years regardless of the version.

Duration of audit

It takes between 12 to 18 months to complete the certification.

4.2

SOC 2

Service and Organization Controls 2 (SOC 2) is a standard developed by The American Institute of Certified Public Accountants (AICPA) and specifies requirements regarding data security for B2B organizations.

The standard has 5 Trust Service Criteria (TSC) categories, based on which trust service criteria are established:

1. **Security**
2. **Availability**
3. **Processing Integrity**
4. **Confidentiality**
5. **Privacy**

To better understand what this standard necessitates from companies, let's look at some examples of trust service criteria.

- Implements Boundary Protection Systems - The company uses firewalls, IDSs, DMZs to secure devices. (**Security**)
- Performs Data Backup—Procedures are in place for backing up data, monitoring to detect back-up failures, and initiating corrective action when such failures occur. (**Availability**)
- Archives and Protects System Records—System records are archived, and archives are protected against theft, corruption, destruction, or deterioration that would prevent them from being used. (**Processing Integrity**)
- Destroys Confidential Information—Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction. (**Confidentiality**)
- Ensures Relevance of Personal Information—Personal information is relevant to the purposes for which it is to be used. (**Privacy**)

In total, there are 64 trust service criteria. Based on these criteria, the organization establishes corresponding controls to demonstrate compliance.

Validity

The certification has a one-year validity.

Duration of audit

An audit takes between 3 to 12 months, depending on the type. There are 2 types of audits:

1. **Type 1** requires a single audit and a single report at a specific date and time. This reflects the company's data security plans at that given point in time.
2. **Type 2**, which is carried over a period of time, usually a minimum of six months.

4.3

PCI-DSS

Payment Card Industry Data Security Standard (PCI-DSS) is an international standard that regulates credit or debit card operations performed by a company, which include:

- The processing,
- The storing, and
- The transmission of customer credit card information.

PCI-DSS applies to all companies that manage card information. This framework contains twelve requirements that companies must fulfil to achieve PCI-DSS compliance.

The requirements are:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Protect all systems against malware and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

Based on the number of transactions, there are four compliance levels companies may be at:

→ **Level 1**: over 6 million transactions annually,

→ **Level 2**: between 1 – 6 million transactions annually,

→ **Level 3**: between 20.000 – 1 million transactions annually,

→ **Level 4**: less than 20.000 transactions annually.

The process of becoming compliant with PCI-DSS depends on the level at which a company is; an audit is performed annually under the following conditions:

- The level 1 audit needs to be performed by a Qualified Security Assessor (QSA) or Internal Security Assessor (ISA),
- For levels 1 and 2, a Report of Compliance (RoC) needs to be submitted to the acquiring bank, which is the financial institution that processes the company's transactions,
- Audits for levels 2, 3, and 4 can be completed using a Self-Assessment Questionnaire (QSA), besides the Attestation of Compliance and the frequent network scans necessary.

Validity

The certification is valid for one year.

4.4

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. federal law that regulates processes related to personal health information (PHI).

HIPAA is organized into three rules:

- → The Privacy Rule,
- → The Security Rule,
- → The Breach Notification Rule.

Let's look at what these rules mean to understand HIPAA better.

The Privacy Rule

This rule specifies the individuals' rights to access and obtain digital copies of their medical records, to restrict access to their PHI, and to request any corrections to their medical records.

Moreover, this rule also specifies the duties of medical providers. Medical professionals must, among others:

- Keep PHI secure,
- Inform patients about their rights.

The Security Rule

The Security rule regulates the storage, management, and access control of ePHI (electronic PHI) records. This rule is based on three cybersecurity principles:

- → Confidentiality,
- → Integrity,
- → Availability.

The Breach Notification Rule

Finally, this rule applies after an incident has occurred and PHI has been breached. While companies sometimes fail to announce a breach when it happens and prefer to delay the announcement, this is an incorrect approach that may impact affected individuals.

The parties that must be notified of the breach are:

- The affected individuals,
- The United States Department of Health and Human Services (HHS).

Fines & other consequences

The **financial penalties** for not complying with the law are split into four categories, based on the gravity of the violation:

6. Minimum fine of $128 per violation up to $63,973,
7. Minimum fine of $1,280 per violation up to $63,973,
8. Minimum fine of $12,794 per violation up to $63,973,
9. Minimum fine of $63,973 per violation up to $1,919,173.

Criminal penalties are divided into three categories:

- For reasonable cause or no knowledge of the violation: up to one year in jail,
- For obtaining PHI under false pretenses: up to five years in jail,
- For obtaining PHI for personal gain or malicious attempt: up to ten years in jail.

Validity

For HIPAA, companies do not receive a certification when they become compliant. Instead, a periodic evaluation may be performed by an internal or an outsourced company to establish their compliance.

4.5

GDPR

The General Data Protection Regulation (GDPR) [4] is a privacy and security law drafted and passed by the European Union (EU) that imposes requirements on all entities that store or process EU citizens' data, even if the entities are not from the EU.

The law has seven principles that ensure protection for EU citizens and accountability for organizations that process the data:

- → Lawfulness, fairness, and transparency,
- → Purpose limitation,
- → Data minimization,
- → Accuracy,
- → Storage limitation,
- → Integrity and confidentiality,
- → Accountability.

Fines

Some violations are considered by GDPR more severe than others. Therefore, there are two tiers of penalties that can be applied to non-compliant entities:

1. Up to 10 mil. EUR or 2% of the firm's annual revenue of the preceding financial year, whichever is higher, for less severe violations.
2. Up to 20. mil EUR or 4% of the firm's annual revenue of the preceding financial yar, whichever is higher, for serious infringements.

Similar to HIPAA, it is a company's responsibility to ensure continuous compliance with GDPR and there is no appointed certification body.

5.

How to achieve compliance

After looking at the most well-known compliance standards and laws and understanding which ones your company should implement, the long journey starts. You ask yourself; how do you achieve compliance?

We've comprised a list of steps to follow when launching the process of becoming compliant:

1. Analyze your systems and define the compliance scope,
2. Select or develop controls to fulfill requirements,
3. Start implementing the controls and track your progress in addressing all requirements,
4. Ensure the effectiveness of controls and detect implementation gaps,
5. Perform an internal audit and ensure a high compliance score before the actual audit,
6. Provide evidence on the effectiveness of controls.

Now that we went through **the importance of cloud, its expected growth in 2023, the most popular compliance standards and the steps to becoming compliant**, it's safe to assume that organizations will have to adapt their compliance process to include cloud-specific controls and particularities.

Cyscale offers a fool-proof platform that:

Helps you automatically detect gaps in your company's implementation of controls to meet regulatory requirements.

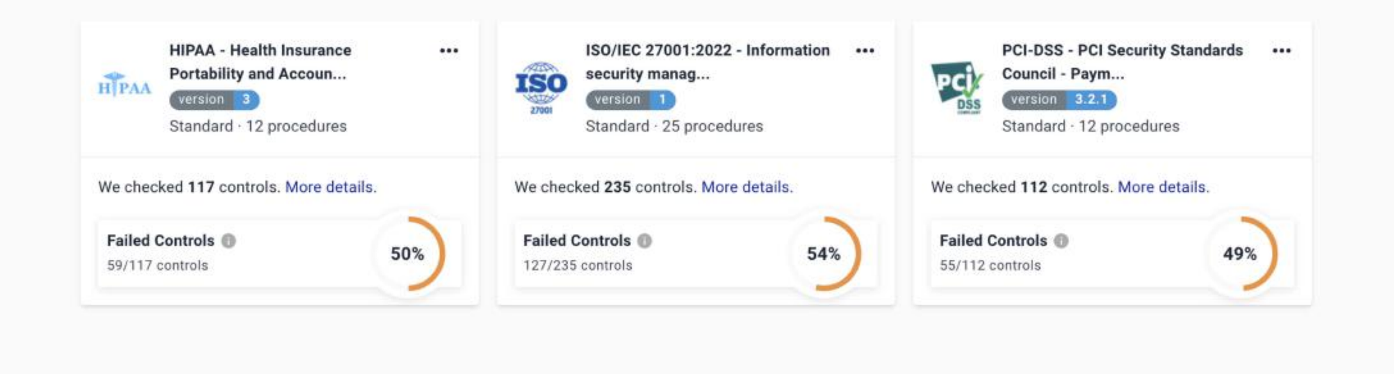
Notifies you when compliance scores drop below a customizable threshold, so that you're never caught off-guard.

Tracks your progress towards becoming audit-ready by providing easy-to-understand compliance scores, trends and charts.

Through reporting, aids you when going through an audit, and others.

A look at compliance-related features in the Cyscale Platform

The **Standards page** contains compliance frameworks that you can enable or disable, based on your preference. From here, you can track your compliance score and the progress in meeting requirements.



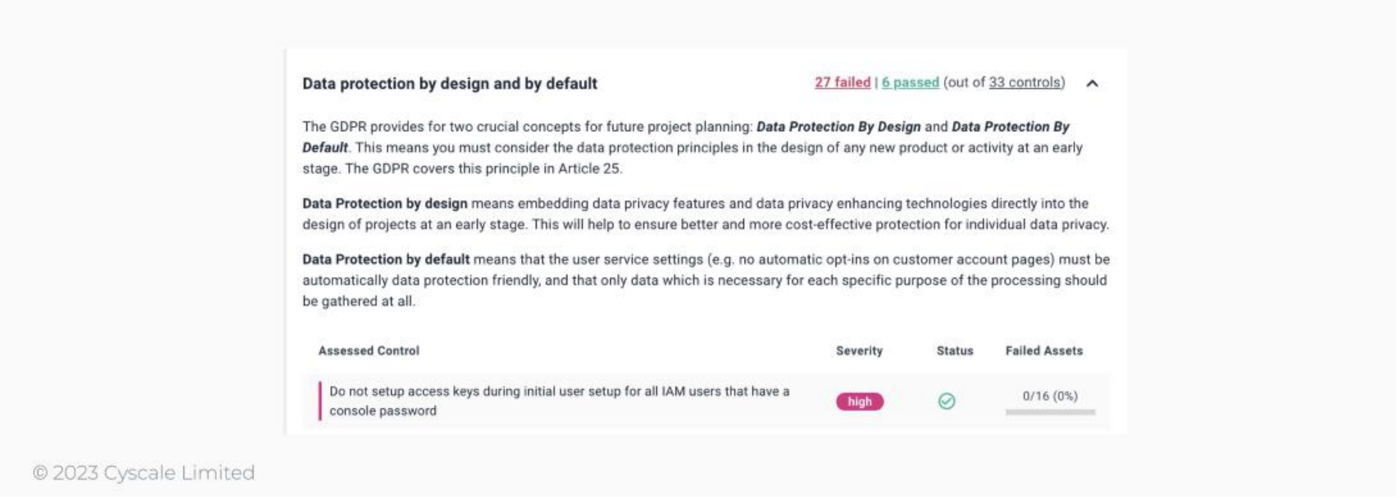
HIPAA - Health Insurance Portability and Accoun...
version 3
Standard · 12 procedures
We checked 117 controls. More details.
Failed Controls
59/117 controls
50%

ISO/IEC 27001:2022 - Information security manag...
version 1
Standard · 25 procedures
We checked 235 controls. More details.
Failed Controls
127/235 controls
54%

PCI-DSS - PCI Security Standards Council - Paym...
version 3.2.1
Standard · 12 procedures
We checked 112 controls. More details.
Failed Controls
55/112 controls
49%

By clicking on one of the standard cards, for instance, on GDPR, we get a description of the law, information about penalties, and, most importantly, the requirements and their associated controls inside the platform, which are cloud specific.

For example, the "Data protection by design and by default" requirement, as seen in the image below, has 34 associated controls, out of which 26 have failed, and 8 have passed.



Data protection by design and by default 27 failed | 6 passed (out of 33 controls)

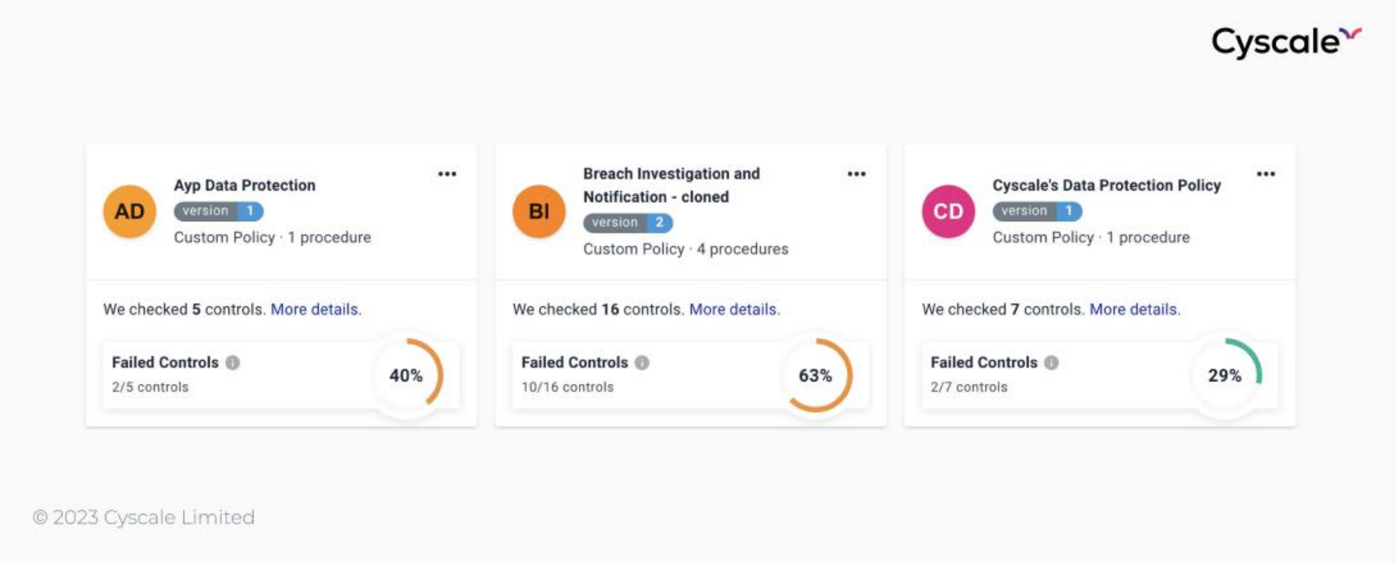
The GDPR provides for two crucial concepts for future project planning: ***Data Protection By Design*** and ***Data Protection By Default***. This means you must consider the data protection principles in the design of any new product or activity at an early stage. The GDPR covers this principle in Article 25.

Data Protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.

Data Protection by default means that the user service settings (e.g. no automatic opt-ins on customer account pages) must be automatically data protection friendly, and that only data which is necessary for each specific purpose of the processing should be gathered at all.

Assessed Control	Severity	Status	Failed Assets
Do not setup access keys during initial user setup for all IAM users that have a console password	high	✓	0/16 (0%)

Every organization that chooses to implement a standard must develop and procedures as part of their controls. To help with this, Cyscale provides out-of-the-box policies such as the ones seen below, available on the **Policies page**. You can use these as templates or create custom policies to cover your needs.



Cyscale

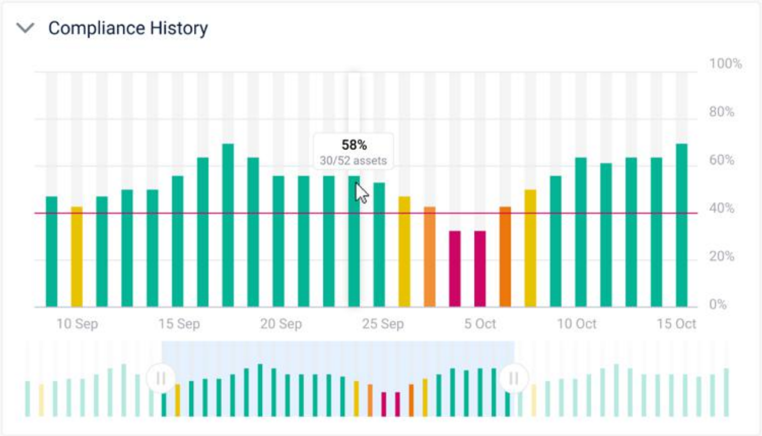
AD **Ayp Data Protection** version 1
Custom Policy · 1 procedure
We checked **5** controls. More details.
Failed Controls 2/5 controls 40%

BI **Breach Investigation and Notification - cloned** version 2
Custom Policy · 4 procedures
We checked **16** controls. More details.
Failed Controls 10/16 controls 63%

CD **Cyscale's Data Protection Policy** version 1
Custom Policy · 1 procedure
We checked **7** controls. More details.
Failed Controls 2/7 controls 29%

Besides these features, you can get a more comprehensive view of your compliance progress through the following capabilities:

- → Compliance score,
- → Compliance-related alerts,
- → Compliance charts.



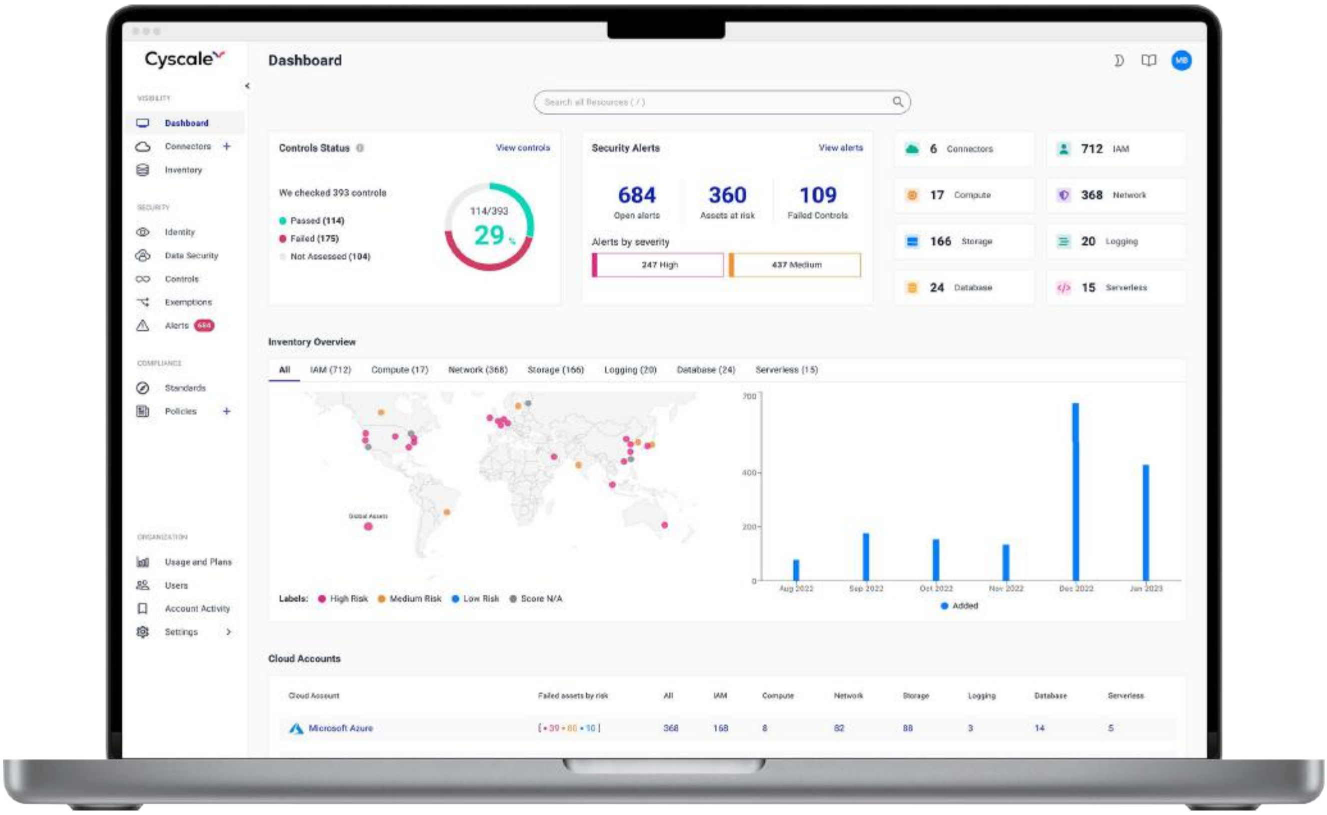
6.

Conclusion

While cloud computing is growing, compliance is becoming more and more important. Data security and privacy are pillars of the cybersecurity industry, and international standards and laws strictly regulate them.

We see growing trends of financial penalties each year – and 2023 will be no better if organizations don't take preventive measures. As companies, we must strive to ensure the best protection of customers' data.

Don't leave compliance for tomorrow; using Cyscale's suite of tools, achieving compliance is no longer a slow and tedious process. We cover the standards and laws included in this whitepaper, and not limited to that. Check out the playground or book a demo with us to start your journey now.



Cloud Account	Failed assets by risk	All	IAM	Compute	Network	Storage	Logging	Database	Serverless
Microsoft Azure	[• 39 • 80 • 10]	368	168	8	82	88	3	14	5

Sources

[1] Gartner, "Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023," 31 October 2022. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023.

[2] Compliancy Group, "Oklahoma State University Agrees to $875k HIPAA Breach Fine," Compliancy Group, 15 July 2022. [Online]. Available: https://compliancy-group.com/oklahoma-state-university-agrees-to-875k-hipaa-breach-fine/.

[3] N. Lomas, "https://techcrunch.com/2022/03/09/clearview-italy-gdpr/," TechCrunch, 9 March 2022. [Online]. Available: https://techcrunch.com/2022/03/09/clearview-italy-gdpr/.

[4] B. Wolford, "What is GDPR, the EU's new data protection law?," [Online]. Available: https://gdpr.eu/what-is-gdpr/.