**Compliance Standards for Cloud**

Cloud-based services are now a crucial component of many businesses, with technology providers adhering to strict privacy and data security guidelines to protect the privacy of user information. Cloud security standards assist and guide organizations in ensuring secure cloud operations.

**What are Cloud Security Standards?**

It was essential to establish guidelines for how work is done in the cloud due to the different security dangers facing the cloud. They offer a thorough framework for how cloud security is upheld with regard to both the user and the service provider.

* Cloud security standards provide a roadmap for businesses transitioning from a traditional approach to a cloud-based approach by providing the right tools, configurations, and policies required for security in cloud usage.
* It helps to devise an effective security strategy for the organization.
* It also supports organizational goals like privacy, portability, security, and interoperability.
* Certification with cloud security standards increases trust and gives businesses a competitive edge.

**Need for Cloud Security Standards**

* **Ensure cloud computing is an appropriate environment:**Organizations need to make sure that cloud computing is the appropriate environment for the applications as security and mitigating risk are the major concerns.
* **To ensure that sensitive data is safe in the cloud:**Organizations need a way to make sure that the sensitive data is safe in the cloud while remaining compliant with standards and regulations.
* **No existing clear standard:**Cloud security standards are essential as earlier there were no existing clear standards that can define what constitutes a secure cloud environment. Thus, making it difficult for cloud providers and cloud users to define what needs to be done to ensure a secure environment.
* **Need for a framework that addresses all aspects of cloud security:**There is a need for businesses to adopt a

**Lack of Cloud Security Standards**

* Enterprises and CSPs have been forced to fumble while relying on an endless variety of auditing needs, regulatory requirements, industry mandates, and data Centre standards to offer direction on protecting their cloud environments due to the lack of adequate cloud security standards.
* Because of this, the Cloud Security Alliance is more difficult to understand than it first appears, and its fragmented strategy does not meet the criteria for “excellent security”.

**Best Practices For Cloud Security**

**1. Secure Access to the Cloud**

Although the majority of cloud service providers have their own ways of safeguarding the infrastructure of their clients, you are still in charge of protecting the cloud user accounts and access to sensitive data for your company. Consider improving password management in your organization to lower the risk of account compromise and credential theft.

Adding password policies to your cybersecurity program is a good place to start. Describe the cybersecurity practices you demand from your staff, such as using unique, complex passwords for each account and routine password rotation.

**2. Control User Access Rights**

Some businesses give employees immediate access to a wide range of systems and data in order to make sure they can carry out their tasks effectively. For cybercriminals, these individuals’ accounts are a veritable gold mine because compromising them can make it simpler to gain access to crucial cloud infrastructure and elevate privileges. Your company can periodically review and revoke user rights to prevent this.

**3. Transparency and Employee Monitoring**

You can use specialized solutions to keep an eye on the behavior of your staff in order to promote transparency in your cloud infrastructure. You can spot the earliest indications of a cloud account compromise or an insider threat by keeping an eye on what your employees are doing while they are at work. Imagine your cybersecurity experts discover a user accessing your cloud infrastructure from a strange IP address or outside of normal business hours. In that situation, they’ll be able to respond to such odd activity promptly because it suggests that a breach may be imminent.

**4. Data Protection**

This involves data protection against unauthorized access, prevention of accidental data disclosure, and ensuring ceaseless access to crucial data in the case of failures and errors.

**5. Access Management**

Three capabilities that are a must in access management are the ability to identify and authenticate users, the ability to assign access rights to users, and the ability to develop and enact access control policies for all the resources.

**Common Cloud Security Standards**

**1. NIST (National Institute of Standards and Technology)**

NIST is a federal organization in the US that creates metrics and standards to boost competition in the scientific and technology industries. The National Institute of Regulations and Technology (NIST) developed the Cybersecurity Framework to comply with US regulations such as the Federal Information Security Management Act and the Health Insurance Portability and Accountability Act (HIPAA) (FISMA). NIST places a strong emphasis on classifying assets according to their commercial value and adequately protecting them.

**2. ISO-27017**

A development of ISO-27001 that includes provisions unique to cloud-based information security. Along with ISO-27001 compliance, ISO-27017 compliance should be taken into account. This standard has not yet been introduced to the marketplace. It attempts to offer further direction in the cloud computing information security field. Its purpose is to supplement the advice provided in ISO/IEC 27002 and various other ISO27k standards, such as ISO/IEC 27018 on the privacy implications of cloud computing, and ISO/IEC 27031 on business continuity.

**3. ISO-27018**

The protection of personally identifiable information (PII) in public clouds that serve as PII processors is covered by this standard. Despite the fact that this standard is especially aimed at public-cloud service providers like AWS or Azure, PII controllers (such as a SaaS provider processing client PII in AWS) nevertheless bear some accountability. If you are a SaaS provider handling PII, you should think about complying with this standard.

**4. CIS controls**

Organizations can secure their systems with the help of Internet Security Center (CIS) Controls, which are open-source policies based on consensus. Each check is rigorously reviewed by a number of professionals before a conclusion is reached.  
To easily access a list of evaluations for cloud security, consult the CIS Benchmarks customized for particular cloud service providers. For instance, you can use the CIS-AWS controls, a set of controls created especially for workloads using Amazon Web Services (AWS).

**5. FISMA**

In accordance with the Federal Information Security Management Act (FISMA), all federal agencies and their contractors are required to safeguard information systems and assets. NIST, using NIST SP 800-53, was given authority under FISMA to define the framework security standards (see definition below).

**6. Cloud Architecture Framework**

These frameworks, which frequently cover operational effectiveness, security, and cost-value factors, can be viewed as best parties standards for cloud architects. This framework, developed by Amazon Web Services, aids architects in designing workloads and applications on the Amazon cloud. Customers have access to a reliable resource for architecture evaluation thanks to this framework, which is based on a collection of questions for the analysis of cloud environments.

**7. General Data Protection Regulation (GDPR)**

For the European Union, there are laws governing data protection and privacy. Even though this law only applies to the European Union, it is something you should keep in mind if you store or otherwise handle any personal information of residents of the EU.

**8. SOC Reporting**

A form of audit of the operational processes used by IT businesses offering any service is known as a “Service and Organization Audits 2” (SOC 2). A worldwide standard for cybersecurity risk management systems is SOC 2 reporting. Your company’s policies, practices, and controls are in place to meet the five trust principles, as shown by the SOC 2 Audit Report. The SOC 2 audit report lists security, availability, processing integrity, confidentiality, and confidentiality as security principles. If you offer software as a service, potential clients might request proof that you adhere to SOC 2 standards.

**9. PCI DSS**

For all merchants who use credit or debit cards, the PCI DSS (Payment Card Industry Data Security Standard) provides a set of security criteria. For businesses that handle cardholder data, there is **PCI DSS**. The PCI DSS specifies fundamental technological and operational criteria for safeguarding cardholder data. Cardholders are intended to be protected from identity theft and credit card fraud by the PCI DSS standard.

**10. HIPAA**

The Health Insurance Portability and Accountability Act (HIPAA), passed by the US Congress to safeguard individual health information, also has parts specifically dealing with information security. **Businesses that handle medical data must abide by HIPAA law**. The HIPAA Security Rule (HSR) is the best choice in terms of information security. The HIPAA HSR specifies rules for protecting people’s electronic personal health information that a covered entity generates, acquires, makes use of or maintains.

Organizations subject to **HIPAA regulations need risk evaluations** and risk management plans to reduce threats to the availability, confidentiality, and integrity of the crucial health data they manage. Assume your company sends and receives health data via cloud-based services (SaaS, IaaS, PaaS). If so, it is your responsibility to make sure the service provider complies with HIPAA regulations and that you have implemented best practices for managing your cloud setups.

**11. CIS AWS Foundations v1.2**

Any business that uses Amazon Web Service cloud resources can help safeguard sensitive IT systems and data by adhering to the CIS AWS Foundations Benchmark. Intelligence analysts developed a set of objective, consensus-driven configuration standards known as the CIS (Center for Internet Security) Benchmarks to help businesses improve their information security. Additionally, CIS procedures are for fortifying AWS accounts to build a solid foundation for running jobs on AWS.

**12. ACSC Essential Eight**

ACSC Essential 8 (also known as the ASD Top 4) is a list of eight cybersecurity mitigation strategies for small and large firms. In order to improve security controls, protect businesses’ computer resources and systems, and protect data from cybersecurity attacks, the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) developed the “Essential Eight Tactics.”

**Why is cloud compliance important?**

As of 2022, [over 60 percent of all corporate data](https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/) is stored in the cloud. This is double the amount stored in the cloud in 2015.

With so much data being stored within the cloud, a business must understand its own role and responsibility for keeping that data safe.

Failure to comply with cloud requirements can result in costly data breaches. In 2022, the average cost of a data breach reached a record high of $4.35 million, according to IBMs’ annual Cost of a Data Breach Report.

IBM statistic that average cost of data breach reached record high of $4.35 million in 2022


Cloud compliance can help you reap the benefits of cloud computing — cost-effectiveness, backup and recovery of data, scalability — while maintaining a [strong security posture](https://secureframe.com/blog/security-posture).

**Cloud compliance challenges**

While cloud solutions offer a variety of benefits, they also come with a unique set of challenges.

Cloud compliance opens the door to [shadow IT](https://www.forcepoint.com/cyber-edu/shadow-it) by using cloud technology without explicit approval.

This term may sound scary. But in practice, shadow IT could be as simple as purchasing additional cloud storage without proper approval. Left unchecked, shadow IT can lead to lost data, an increased attack surface, and non-compliance.

Using a well-known CSP can also give companies a false sense of data security.

Take the [2021 Azure Cosmos DB vulnerability](https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-azure-customers-of-critical-cosmos-db-vulnerability/), for example. Used by brands like Mercedes-Benz and Mars, Incorporated, the database experienced a large vulnerability that made it possible for a user to steal the access key of another. This vulnerability went undetected for two years.

This shows that Microsoft Azure, like other well-known CSPs, can experience vulnerabilities — even if they have a hefty list of compliance certifications. That’s why it’s so important for businesses using CSPs to put a high priority on their own security management and compliance monitoring.

## 8 tips for better cloud compliance

Wondering how you can level up your cloud compliance practices? We offer eight tips below.



### 1. Identify regulations and guidelines.

The first step in achieving cloud compliance is identifying which regulations and industry standards your organization needs to comply with.

Common cloud [compliance frameworks](https://secureframe.com/blog/security-frameworks) include:

* [ISO 27001](https://secureframe.com/products/iso-27001)
* [SOC 2](https://secureframe.com/products/soc-2)
* [NIST](https://www.nist.gov/)
* [HIPAA](https://secureframe.com/products/hipaa)
* [PCI DSS](https://secureframe.com/products/pci)
* [Sarbanes-Oxley Act (SOX)](https://www.soxlaw.com/)
* [FedRAMP](https://www.fedramp.gov/)
* [Cloud Controls Matrix](https://cloudsecurityalliance.org/research/cloud-controls-matrix/)

**2. Understand responsibility.**

Many cloud providers like Amazon Web Services (AWS) outline specific cloud usage responsibilities. AWS uses the [shared responsibility model](https://aws.amazon.com/compliance/shared-responsibility-model/), which splits responsibility between AWS and the customer.

AWS is responsible for security of the infrastructure that runs all of the services in the AWS Cloud. The customer is responsible for the secure configurations of the cloud services in use as well as any customer data.

The AWS shared responsibility model leads many businesses to mistakenly think that all compliance responsibility falls on AWS. This is not the case.

The burden of compliance ultimately falls on the business’s shoulders because you are responsible for the data you choose to put on the cloud and the secure configuration of the services in use.

### 3. Understand the unique requirements of your cloud environment.

In addition to the shared security responsibility, a cloud environment’s service and deployment model affects who handles security requirements. The most common services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The most common deployment models are public, private, and hybrid.

For example, in a PaaS environment, the administrator is responsible for the applications while the CSP is responsible for the physical servers, physical network, hypervisor, and operating systems. Who handles the inventory and control of hardware assets would differ for hybrid and public cloud environments.

To ensure you’re following security and compliance best practices, you must understand the unique risks and requirements of your cloud environment.

### 4. Ensure proper access control.

Just like companies have a process for sharing access control with new hires or vendors, you need something similar when it comes to cloud security.

Companies should establish a policy for limiting and granting access to their cloud environment and data stored within it. You can also introduce need-based access rules and expiration dates to help you keep track of who has access and for how long.

### 5. Classify your data.

When it comes to storing data on the cloud, it’s important to know where server locations are because many regulations require servers to reside within the U.S.

Once you’ve chosen a cloud provider, you need to determine what types of data you want to live on the cloud. You can do this by classifying your data.

[Data classification](https://secureframe.com/blog/data-classification) is the process of sorting data into different categories. This helps businesses more easily manage, secure, and store their data.

As a general best practice, highly confidential or sensitive data should remain on an internal network rather than migrating to the cloud.

**6. Encrypt all sensitive data that exists in the cloud.**

According to the [2021 Thales Global Cloud Security Study](https://cts.businesswire.com/ct/CT?id=smartlink&url=https%3A%2F%2Fcpl.thalesgroup.com%2Fcloud-security-research&esheet=52514586&newsitemid=20211027005044&lan=en-US&anchor=2021+Thales+Global+Cloud+Security+Study&index=1&md5=135297761f6f907bbe530ae4c019c1df), the vast majority (83%) of businesses are still failing to encrypt half of the sensitive data they store in the cloud, despite 40% revealing they dealt with a cloud breach in the last year.

Encryption is key to protecting sensitive data that must exist on the cloud. Encrypting data also helps you meet most compliance requirements such as PCI DSS and GDPR.

Your cloud provider may offer encryption services, but remember that it’s still the business’s responsibility to protect data while it’s being moved and stored.

### 7. Conduct regular internal audits.

One of the best ways to uncover security gaps and vulnerabilities is by conducting regular [internal security audits](https://secureframe.com/blog/security-audit-checklist).

Re-examine your cloud compliance to ensure it aligns with regulatory requirements. It’s also a good practice to stay on top of updates to regulatory requirements so you can make adjustments proactively.

### 8. Understand your service level agreement and legal contract inside and out.

Simply put, service level agreements (SLAs) spell out ground rules and expectations that a company has for the cloud service provider they choose to entrust their data with.

An SLA should be very clear on roles and responsibilities, incident response execution, and data breach remediation. Everything in the SLA must be in accordance with the regulations governing your business.

Your SLA should also be a guide for how to handle problems — both expected and unexpected.

A legal contract is another important piece of your cloud security. It should highlight liability, as well as breach disclosure and incident response timeframes.