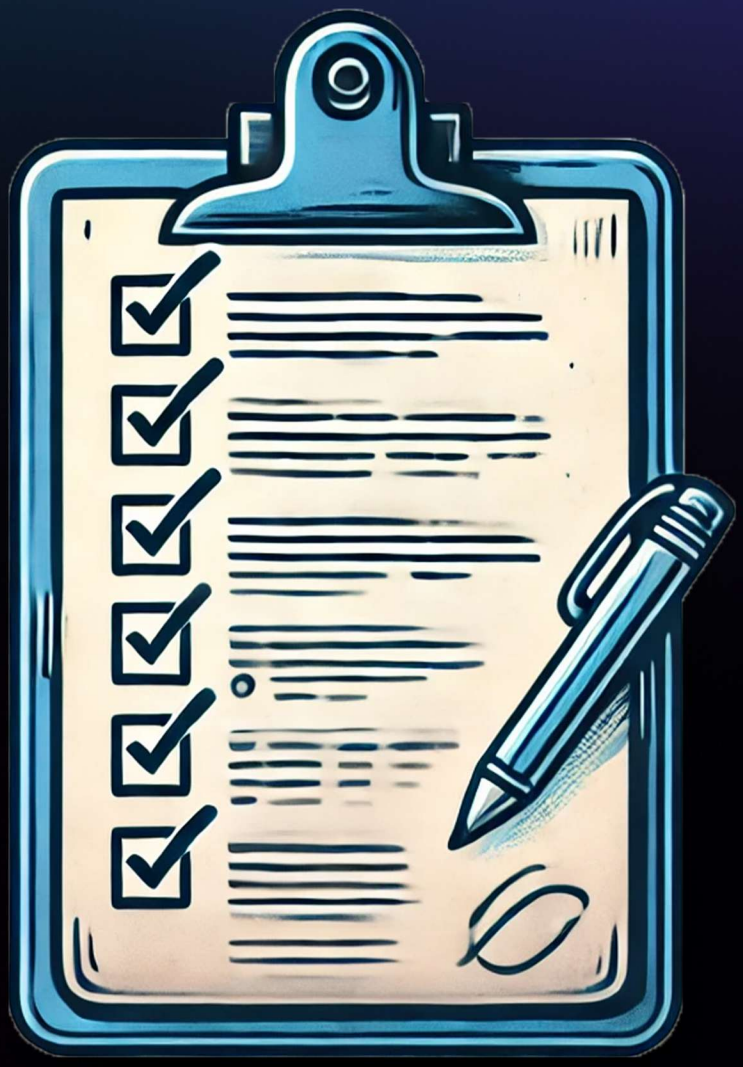
TITAN
CLOUD STORAGE

WHITE PAPERS



CHECKLIST FOR COMPLIANCE IN THE CLOUD

This document provides a concise guide for ensuring cloud service providers meet stringent compliance standards. It outlines key regulations, evaluates the suitability of cloud solutions, and offers a checklist for assessing providers. Key areas include physical security, data encryption, backup and recovery, and audit controls. It also highlights Titan Cloud Storage's commitment to compliance, security, and support. This guide is crucial for organizations aiming to maintain compliance in cloud environments.

CHECKLIST FOR COMPLIANCE IN THE CLOUD

CONTENTS

Regulations and Standards

With the industrialization of hacking and the enormous impact of security breaches, governments, industries, and individual organizations are increasingly adopting regulations and standards to handle sensitive information. Complying with these rules and best practices challenges any IT team. Audit processes and the need to prove compliance further complicate matters. As organizations pursue cloud-based services, upholding compliance together with their cloud service provider can raise additional hurdles.

Is the Cloud Right for Stringent Compliance Applications?

The cloud offers significant benefits: instant scalability, flexibility, access when and where needed, lowered costs, and fewer operational demands on the IT department. It allows organizations to respond to their present and future needs without up-front lead time and capital investment. They can get and use what they need, when they need it. The organization can focus on their core mission and invest in areas strategic to their business. Despite these advantages, many still question whether flexibility and cost savings are worth the risks when faced with a potentially daunting regulatory environment.

Key Compliance Requirements for Cloud Service Providers:

- **Physical Security:** Secure physical access to facilities stoing data.
- **Data Encryption:** Encrypt sensitive data at rest and in transit.
- **Backup and Recovery:** Documented plans for backup, operation in an emergency, and disaster recovery.
- **Session Management:** Securely disconnect inactive sessions.
- **Audit Controls:** Implement audit controls and documentation to demonstrate compliance and identify vulnerabilities.

Evaluating your Cloud Service Provider for Compliance

When selecting a cloud service provider, consider the following steps:

1. Identify Regulations and Requirements: Understand the regulations that bind your organization, such as HIPAA, PCI, and geographical constraints.

2. Evaluate Service Providers: Look at analyst reports, customer stories, and referrals. Approach it as a search for a long-term partnership, not just transactions.

3. Use a Checklist: Engage in a conversation with prospective providers and ensure all questions are answered.

Key Qualities of a Cloud Service Provider

- **Commitment to Compliance:** Adheres to applicable regulations and standards like SOC2, HIPAA, ITIL and ISO.
- **Risk Assessment:** Constantly assesses cloud infrastructure to meet requirements.
- **Business Associates Agreement (BAA):** Willing to sign and incorporate compliance language in contracts.
- **Incident Response:** Documents and fulfills security incident response, emergency operations, and disaster recovery plans.

Reporting Capabilites Available

• On-Demand Reporting:

Provide audit documentation and support for the audit process without undue bureaucracy.

• Incident Reporting:

Report vulnerabilities rapidly to address them.

• Compliance Technology:

Utilize software and services to identify and alert compliance gaps, and employ physical safeguards and authentication methods.

A checklist for evaluating Cloud Service Providers

When evaluating potential cloud providers, consider the following:

1. **Compliance Certifications:**
   Ensure the provider upholds necessary certifications and standards.

2. **Audit Readiness:**
   Verify the provider’s audit controls and documentation practices.

3. **Physical and Data Security:**
   Assess the provider's physical security measures and data encryption practices.

4. **Support and Communication:**
   Ensure the provider offers compliance-oriented customer support and can discuss compliance procedures directly with auditors if needed.

Fulfilling Your Compliant Cloud

Realizing the Benefits of a Compliant Cloud

Work with your cloud partner to configure workloads to ensure compliance. Start with less sensitive workloads to build confidence. Ensure your cloud service provider prioritizes your compliance and audit needs from the beginning. Choose a provider that will protect your organization's sensitive data and maintain compliance.

Schedule a consultation with one of our compliance experts today. Not ready to talk? Explore our other compliance-related materials.

- Ensuring a Compliant Cloud That's Audit Ready
- Learn More About Titan Cloud Storage Compliance

DISCOVER THE TITAN CLOUD STORAGE DIFFERENCE

DRaaS: With Titan Cloud Storage, you aren't alone preparing for a disaster. With hundreds of partners that will assist in your journey, your business is in good hands.

IaaS: Titan Cloud Storage provides peace of mind with security and compliance as top priorities, upholding various global certifications and standards.

BaaS: With Titan's S3 Compatible API, you can easily plug into a rich system of backup solutions. Our team also has a catalog of easily implementable processes to backup or archive your data that takes minutes to implement. Achieve 3-2-1 resiliency with cloud-based backup, offering encrypted communication and secure off-site storage.