TOP CLOUD SECURITY AND COMPLIANCE CHECKLIST

SkillWeed

TABLE OF CONTENTS

INTRODUCTION TO CLOUD SECURITY AND COMPLIANCE

In an era where businesses increasingly rely on cloud computing services to power their operations, ensuring compliance with regulatory standards and security best practices is paramount. The landscape of cloud service providers is diverse and dynamic, each offering a unique set of features, capabilities, and compliance frameworks.

In this comprehensive guide, we delve into the intricate world of cloud compliance, providing insights, strategies, and practical approaches for navigating the complexities of regulatory requirements across various cloud service providers. From industry giants like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) to emerging players such as Alibaba Cloud and DigitalOcean, we explore the key compliance areas, sub-areas, and sections within each provider's infrastructure.

Throughout this workbook, you will find detailed tables outlining essential compliance components, including risk assessment, testing steps, mitigation plans, applicable regulations, and sub-controls mapped to leading frameworks such as NIST CSF, ISO 27001, PCI-DSS, COBIT, and CIS. Whether you are a seasoned cloud architect, a compliance officer, or an aspiring cloud practitioner, this book serves as a valuable resource for understanding, implementing, and maintaining robust compliance strategies in the cloud.

In this worbook, we are examining key compliance requirements, best practices, risks, testing steps, and recommendation plans for the following cloud service providers:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Alibaba Cloud
- IBM Cloud (formerly IBM Bluemix)
- Oracle Cloud
- Tencent Cloud
- DigitalOcean
- Linode (owned by Akamai)
- OVHcloud"

Here's an overview of crucial aspects to consider when securing your cloud environment:

- **Compliance Requirements:** Every industry and region has regulations governing data security and privacy. Understanding these regulations (e.g., HIPAA, GDPR) and ensuring your cloud provider meets them is paramount.
- **Best Practices:** Cloud security best practices encompass a range of measures, including encryption, access control, identity management, and activity monitoring. Implementing these practices strengthens your cloud environment's resilience.
- **Risk Assessments:** Regularly evaluating potential threats and vulnerabilities in your cloud setup is crucial. This proactive approach helps identify and address security gaps before they become exploited.

- **Testing and Validation:** Regularly testing your cloud security controls, such as penetration testing and vulnerability scans, verifies their effectiveness and identifies areas for improvement.
- **Remediation Plans:** Having a clear plan to address security incidents and vulnerabilities is essential. This plan should outline procedures for identifying, containing, and recovering from security breaches.

By understanding these key aspects, you can leverage the power of cloud services with confidence, ensuring the security and compliance of your data.

AWS COMPLIANCE CHECKLIST

Compliance Area	Sub-Area	Section in AWS	Risk	Testing Steps	Mitigation Plan	Applicable Regulation	Applicable Sub-Controls Mapped to Leading Frameworks
Identity and Access Management (IAM)	Access Control	IAM Policies	Unauthorized Access	1. Review IAM Policies 2. Conduct Access Reviews 3. Test Permissions	1. Implement Least Privilege Principle 2. Enable Multi-Factor Authentication (MFA) 3. Regularly Review and Update Policies	ISO 27001, PCI-DSS, COBIT	ISO 27001: A.9.2, PCI-DSS: 7.1, COBIT: BAI09
Data Encryption	Encryption at Rest	AWS Key Management Service (KMS)	Data Exposure	1. Verify Encryption Configuration 2. Test Data Access without Appropriate Permissions	1. Implement Strong Encryption Algorithms 2. Regularly Rotate Encryption Keys 3. Monitor Key Usage	ISO 27001, PCI-DSS	ISO 27001: A.8.2, PCI-DSS: 3.4
Network Security	Network Configuration	AWS Security Groups	Unauthorized Access	1. Review Security Group Rules 2. Test Network Access Controls	1. Implement Principle of Least Privilege 2. Enable Logging and Monitoring of Network Traffic	NIST CSF, CIS	NIST CSF: PR.AC-4, CIS Controls: 3.4
Incident Response	Incident Identification	AWS CloudTrail	Delayed Incident Response	1. Monitor CloudTrail Logs 2. Configure Alarms for Suspicious Activities	1. Establish Incident Response Plan 2. Regularly Test Incident Response Procedures	NIST CSF, COBIT	NIST CSF: PR.PT-4, COBIT: BAI06
Compliance Monitoring	Compliance Reporting	AWS Config	Compliance Violations	1. Configure AWS Config Rules 2. Generate Compliance Reports	1. Implement Automated Compliance Checks 2. Regularly Review Compliance Reports	ISO 27001, PCI-DSS	ISO 27001: A.12.4, PCI-DSS: 11.5

AZURE COMPLIANCE CHECKLIST

Compliance Area	Sub-Area	Section in Azure	Risk	Testing Steps	Mitigation Plan	Applicable Regulation	Applicable Sub-Controls Mapped to Leading Frameworks
Identity and Access Management (IAM)	Access Control	Azure Active Directory (AAD)	Unauthorized Access	1. Review AAD Policies 2. Conduct Access Reviews 3. Test Permissions	1. Implement Least Privilege Principle 2. Enable Multi-Factor Authentication (MFA) 3. Regularly Review and Update Policies	ISO 27001, PCI-DSS, COBIT	ISO 27001: A.9.2, PCI-DSS: 7.1, COBIT: BAI09
Data Encryption	Encryption at Rest	Azure Key Vault	Data Exposure	1. Verify Encryption Configuration 2. Test Data Access without Appropriate Permissions	1. Implement Strong Encryption Algorithms 2. Regularly Rotate Encryption Keys 3. Monitor Key Usage	ISO 27001, PCI-DSS	ISO 27001: A.8.2, PCI-DSS: 3.4
Network Security	Network Configuration	Azure Network Security Groups	Unauthorized Access	1. Review Security Group Rules 2. Test Network Access Controls	1. Implement Principle of Least Privilege 2. Enable Logging and Monitoring of Network Traffic	NIST CSF, CIS	NIST CSF: PR.AC-4, CIS Controls: 3.4
Incident Response	Incident Identification	Azure Security Center	Delayed Incident Response	1. Monitor Security Center Alerts 2. Configure Alarms for Suspicious Activities	1. Establish Incident Response Plan 2. Regularly Test Incident Response Procedures	NIST CSF, COBIT	NIST CSF: PR.PT-4, COBIT: BAI06
Compliance Monitoring	Compliance Reporting	Azure Policy	Compliance Violations	1. Configure Azure Policy Rules 2. Generate Compliance Reports	1. Implement Automated Compliance Checks 2. Regularly Review Compliance Reports	ISO 27001, PCI-DSS	ISO 27001: A.12.4, PCI-DSS: 11.5

GOOGLE CLOUD PLATFORM COMPLIANCE CHECKLIST

Compliance Area	Sub-Area	Section in GCP	Risk	Testing Steps	Mitigation Plan	Applicable Regulation	Applicable Sub-Controls Mapped to Leading Frameworks
Identity and Access Management (IAM)	Access Control	Google Cloud Identity and Access Management (IAM)	Unauthorized Access	1. Review IAM Policies 2. Conduct Access Reviews 3. Test Permissions	1. Implement Least Privilege Principle 2. Enable Multi-Factor Authentication (MFA) 3. Regularly Review and Update Policies	ISO 27001, PCI-DSS, COBIT	ISO 27001: A.9.2, PCI-DSS: 7.1, COBIT: BAI09
Data Encryption	Encryption at Rest	Google Cloud Key Management Service (KMS)	Data Exposure	1. Verify Encryption Configuration 2. Test Data Access without Appropriate Permissions	1. Implement Strong Encryption Algorithms 2. Regularly Rotate Encryption Keys 3. Monitor Key Usage	ISO 27001, PCI-DSS	ISO 27001: A.8.2, PCI-DSS: 3.4
Network Security	Network Configuration	Google Cloud Virtual Private Cloud (VPC)	Unauthorized Access	1. Review VPC Configuration 2. Test Network Access Controls	1. Implement Principle of Least Privilege 2. Enable Logging and Monitoring of Network Traffic	NIST CSF, CIS	NIST CSF: PR.AC-4, CIS Controls: 3.4
Incident Response	Incident Identification	Google Cloud Security Command Center	Delayed Incident Response	1. Monitor Security Command Center Alerts 2. Configure Alarms for Suspicious Activities	1. Establish Incident Response Plan 2. Regularly Test Incident Response Procedures	NIST CSF, COBIT	NIST CSF: PR.PT-4, COBIT: BAI06
Compliance Monitoring	Compliance Reporting	Google Cloud Resource Manager	Compliance Violations	1. Configure Resource Manager Policies 2. Generate Compliance Reports	1. Implement Automated Compliance Checks 2. Regularly Review Compliance Reports	ISO 27001, PCI-DSS	ISO 27001: A.12.4, PCI-DSS: 11.5

ALIBABA CLOUD PLATFORM COMPLIANCE CHECKLIST

Compliance Area	Sub-Area	Section in Alibaba Cloud	Risk	Testing Steps	Mitigation Plan	Applicable Regulation	Applicable Sub-Controls Mapped to Leading Frameworks
Identity and Access Management (IAM)	Access Control	Alibaba Cloud Resource Access Management (RAM)	Unauthorized Access	1. Review RAM Policies 2. Conduct Access Reviews 3. Test Permissions	1. Implement Least Privilege Principle 2. Enable Multi-Factor Authentication (MFA) 3. Regularly Review and Update Policies	ISO 27001, PCI-DSS, COBIT	ISO 27001: A.9.2, PCI-DSS: 7.1, COBIT: BAI09
Data Encryption	Encryption at Rest	Alibaba Cloud Key Management Service (KMS)	Data Exposure	1. Verify Encryption Configuration 2. Test Data Access without Appropriate Permissions	1. Implement Strong Encryption Algorithms 2. Regularly Rotate Encryption Keys 3. Monitor Key Usage	ISO 27001, PCI-DSS	ISO 27001: A.8.2, PCI-DSS: 3.4
Network Security	Network Configuration	Alibaba Cloud Security Groups	Unauthorized Access	1. Review Security Group Rules 2. Test Network Access Controls	1. Implement Principle of Least Privilege 2. Enable Logging and Monitoring of Network Traffic	NIST CSF, CIS	NIST CSF: PR.AC-4, CIS Controls: 3.4
Incident Response	Incident Identification	Alibaba Cloud Security Center	Delayed Incident Response	1. Monitor Security Center Alerts 2. Configure Alarms for Suspicious Activities	1. Establish Incident Response Plan 2. Regularly Test Incident Response Procedures	NIST CSF, COBIT	NIST CSF: PR.PT-4, COBIT: BAI06
Compliance Monitoring	Compliance Reporting	Alibaba Cloud Resource Management Service	Compliance Violations	1. Configure Resource Management Policies 2. Generate Compliance Reports	1. Implement Automated Compliance Checks 2. Regularly Review Compliance Reports	ISO 27001, PCI-DSS	ISO 27001: A.12.4, PCI-DSS: 11.5

ORACLE CLOUD PLATFORM COMPLIANCE CHECKLIST

Compliance Area	Sub-Area	Section in Oracle Cloud	Risk	Testing Steps	Mitigation Plan	Applicable Regulation	Applicable Sub-Controls Mapped to Leading Frameworks
Identity and Access Management (IAM)	Access Control	Oracle Identity Cloud Service	Unauthorized Access	1. Review IAM Policies 2. Conduct Access Reviews 3. Test Permissions	1. Implement Least Privilege Principle 2. Enable Multi-Factor Authentication (MFA) 3. Regularly Review and Update Policies	ISO 27001, PCI-DSS, COBIT	ISO 27001: A.9.2, PCI-DSS: 7.1, COBIT: BAI09
Data Encryption	Encryption at Rest	Oracle Cloud Infrastructure Vault	Data Exposure	1. Verify Encryption Configuration 2. Test Data Access without Appropriate Permissions	1. Implement Strong Encryption Algorithms 2. Regularly Rotate Encryption Keys 3. Monitor Key Usage	ISO 27001, PCI-DSS	ISO 27001: A.8.2, PCI-DSS: 3.4
Network Security	Network Configuration	Oracle Cloud Infrastructure Network Security Groups	Unauthorized Access	1. Review Security Group Rules 2. Test Network Access Controls	1. Implement Principle of Least Privilege 2. Enable Logging and Monitoring of Network Traffic	NIST CSF, CIS	NIST CSF: PR.AC-4, CIS Controls: 3.4
Incident Response	Incident Identification	Oracle Cloud Infrastructure Security Advisor	Delayed Incident Response	1. Monitor Security Advisor Alerts 2. Configure Alarms for Suspicious Activities	1. Establish Incident Response Plan 2. Regularly Test Incident Response Procedures	NIST CSF, COBIT	NIST CSF: PR.PT-4, COBIT: BAI06
Compliance Monitoring	Compliance Reporting	Oracle Cloud Infrastructure Compliance Service	Compliance Violations	1. Configure Compliance Policies 2. Generate Compliance Reports	1. Implement Automated Compliance Checks 2. Regularly Review Compliance Reports	ISO 27001, PCI-DSS	ISO 27001: A.12.4, PCI-DSS: 11.5

IBM CLOUD (KYNDRYL) PLATFORM COMPLIANCE CHECKLIST

Compliance Area	Sub-Area	Section in IBM Cloud (Kyndryl)	Risk	Testing Steps	Mitigation Plan	Applicable Regulation	Applicable Sub-Controls Mapped to Leading Frameworks
Identity and Access Management (IAM)	Access Control	IBM Cloud Identity and Access Management (IAM)	Unauthorized Access	1. Review IAM Policies 2. Conduct Access Reviews 3. Test Permissions	1. Implement Least Privilege Principle 2. Enable Multi-Factor Authentication (MFA) 3. Regularly Review and Update Policies	ISO 27001, PCI-DSS, COBIT	ISO 27001: A.9.2, PCI-DSS: 7.1, COBIT: BAI09
Data Encryption	Encryption at Rest	IBM Cloud Key Protect	Data Exposure	1. Verify Encryption Configuration 2. Test Data Access without Appropriate Permissions	1. Implement Strong Encryption Algorithms 2. Regularly Rotate Encryption Keys 3. Monitor Key Usage	ISO 27001, PCI-DSS	ISO 27001: A.8.2, PCI-DSS: 3.4
Network Security	Network Configuration	IBM Cloud Virtual Private Cloud (VPC)	Unauthorized Access	1. Review VPC Configuration 2. Test Network Access Controls	1. Implement Principle of Least Privilege 2. Enable Logging and Monitoring of Network Traffic	NIST CSF, CIS	NIST CSF: PR.AC-4, CIS Controls: 3.4
Incident Response	Incident Identification	IBM Cloud Security Intelligence with Watson	Delayed Incident Response	1. Monitor Security Intelligence Alerts 2. Configure Alarms for Suspicious Activities	1. Establish Incident Response Plan 2. Regularly Test Incident Response Procedures	NIST CSF, COBIT	NIST CSF: PR.PT-4, COBIT: BAI06
Compliance Monitoring	Compliance Reporting	IBM Cloud Continuous Compliance	Compliance Violations	1. Configure Continuous Compliance Policies 2. Generate Compliance Reports	1. Implement Automated Compliance Checks 2. Regularly Review Compliance Reports	ISO 27001, PCI-DSS	ISO 27001: A.12.4, PCI-DSS: 11.5

TENCENT CLOUD KEY COMPLIANCE CHECKLIST

Compliance Area	Sub-Area	Section in Tencent Cloud	Risk	Testing Steps	Mitigation Plan	Applicable Regulation	Applicable Sub-Controls Mapped to Leading Frameworks
Identity and Access Management (IAM)	Access Control	Tencent Cloud Access Management (CAM)	Unauthorized Access	1. Review CAM Policies 2. Conduct Access Reviews 3. Test Permissions	1. Implement Least Privilege Principle 2. Enable Multi-Factor Authentication (MFA) 3. Regularly Review and Update Policies	ISO 27001, PCI-DSS, COBIT	ISO 27001: A.9.2, PCI-DSS: 7.1, COBIT: BAI09
Data Encryption	Encryption at Rest	Tencent Cloud Key Management Service (KMS)	Data Exposure	1. Verify Encryption Configuration 2. Test Data Access without Appropriate Permissions	1. Implement Strong Encryption Algorithms 2. Regularly Rotate Encryption Keys 3. Monitor Key Usage	ISO 27001, PCI-DSS	ISO 27001: A.8.2, PCI-DSS: 3.4
Network Security	Network Configuration	Tencent Cloud Virtual Private Cloud (VPC)	Unauthorized Access	1. Review VPC Configuration 2. Test Network Access Controls	1. Implement Principle of Least Privilege 2. Enable Logging and Monitoring of Network Traffic	NIST CSF, CIS	NIST CSF: PR.AC-4, CIS Controls: 3.4
Incident Response	Incident Identification	Tencent Cloud Security Center	Delayed Incident Response	1. Monitor Security Center Alerts 2. Configure Alarms for Suspicious Activities	1. Establish Incident Response Plan 2. Regularly Test Incident Response Procedures	NIST CSF, COBIT	NIST CSF: PR.PT-4, COBIT: BAI06
Compliance Monitoring	Compliance Reporting	Tencent Cloud Compliance Management	Compliance Violations	1. Configure Compliance Policies 2. Generate Compliance Reports	1. Implement Automated Compliance Checks 2. Regularly Review Compliance Reports	ISO 27001, PCI-DSS	ISO 27001: A.12.4, PCI-DSS: 11.5

OVHCLOUD KEY COMPLIANCE CHECKLIST

Compliance Area	Sub-Area	Section in OVHcloud	Risk	Testing Steps	Mitigation Plan	Applicable Regulation	Applicable Sub-Controls Mapped to Leading Frameworks
Identity and Access Management (IAM)	Access Control	OVHcloud Identity and Access Management (IAM)	Unauthorized Access	1. Review IAM Policies 2. Conduct Access Reviews 3. Test Permissions	1. Implement Least Privilege Principle 2. Enable Multi-Factor Authentication (MFA) 3. Regularly Review and Update Policies	ISO 27001, PCI-DSS, COBIT	ISO 27001: A.9.2, PCI-DSS: 7.1, COBIT: BAI09
Data Encryption	Encryption at Rest	OVHcloud Key Management Service (KMS)	Data Exposure	1. Verify Encryption Configuration 2. Test Data Access without Appropriate Permissions	1. Implement Strong Encryption Algorithms 2. Regularly Rotate Encryption Keys 3. Monitor Key Usage	ISO 27001, PCI-DSS	ISO 27001: A.8.2, PCI-DSS: 3.4
Network Security	Network Configuration	OVHcloud Virtual Private Cloud (VPC)	Unauthorized Access	1. Review VPC Configuration 2. Test Network Access Controls	1. Implement Principle of Least Privilege 2. Enable Logging and Monitoring of Network Traffic	NIST CSF, CIS	NIST CSF: PR.AC-4, CIS Controls: 3.4
Incident Response	Incident Identification	OVHcloud Incident Response Plan	Delayed Incident Response	1. Monitor Security Incidents 2. Configure Alarms for Suspicious Activities	1. Establish Incident Response Plan 2. Regularly Test Incident Response Procedures	NIST CSF, COBIT	NIST CSF: PR.PT-4, COBIT: BAI06
Compliance Monitoring	Compliance Reporting	OVHcloud Compliance Management	Compliance Violations	1. Configure Compliance Policies 2. Generate Compliance Reports	1. Implement Automated Compliance Checks 2. Regularly Review Compliance Reports	ISO 27001, PCI-DSS	ISO 27001: A.12.4, PCI-DSS: 11.5

DIGITALOCEAN KEY COMPLIANCE CHECKLIST

Compliance Area	Sub-Area	Section in DigitalOcean	Risk	Testing Steps	Mitigation Plan	Applicable Regulation	Applicable Sub-Controls Mapped to Leading Frameworks
Identity and Access Management (IAM)	Access Control	DigitalOcean Identity and Access Management	Unauthorized Access	1. Review IAM Policies 2. Conduct Access Reviews 3. Test Permissions	1. Implement Least Privilege Principle 2. Enable Multi-Factor Authentication (MFA) 3. Regularly Review and Update Policies	ISO 27001, PCI-DSS, COBIT	ISO 27001: A.9.2, PCI-DSS: 7.1, COBIT: BAI09
Data Encryption	Encryption at Rest	DigitalOcean Spaces Encryption	Data Exposure	1. Verify Encryption Configuration 2. Test Data Access without Appropriate Permissions	1. Implement Strong Encryption Algorithms 2. Regularly Rotate Encryption Keys 3. Monitor Key Usage	ISO 27001, PCI-DSS	ISO 27001: A.8.2, PCI-DSS: 3.4
Network Security	Network Configuration	DigitalOcean Firewall Configuration	Unauthorized Access	1. Review Firewall Configuration 2. Test Network Access Controls	1. Implement Principle of Least Privilege 2. Enable Logging and Monitoring of Network Traffic	NIST CSF, CIS	NIST CSF: PR.AC-4, CIS Controls: 3.4
Incident Response	Incident Identification	DigitalOcean Incident Response Plan	Delayed Incident Response	1. Monitor Security Incidents 2. Configure Alarms for Suspicious Activities	1. Establish Incident Response Plan 2. Regularly Test Incident Response Procedures	NIST CSF, COBIT	NIST CSF: PR.PT-4, COBIT: BAI06
Compliance Monitoring	Compliance Reporting	DigitalOcean Compliance Management	Compliance Violations	1. Configure Compliance Policies 2. Generate Compliance Reports	1. Implement Automated Compliance Checks 2. Regularly Review Compliance Reports	ISO 27001, PCI-DSS	ISO 27001: A.12.4, PCI-DSS: 11.5

LINODE KEY COMPLIANCE CHECKLIST

Compliance Area	Sub-Area	Section in Linode	Risk	Testing Steps	Mitigation Plan	Applicable Regulation	Applicable Sub-Controls Mapped to Leading Frameworks
Identity and Access Management (IAM)	Access Control	Linode Identity and Access Management	Unauthorized Access	1. Review IAM Policies 2. Conduct Access Reviews 3. Test Permissions	1. Implement Least Privilege Principle 2. Enable Multi-Factor Authentication (MFA) 3. Regularly Review and Update Policies	ISO 27001, PCI-DSS, COBIT	ISO 27001: A.9.2, PCI-DSS: 7.1, COBIT: BAI09
Data Encryption	Encryption at Rest	Linode Disk Encryption	Data Exposure	1. Verify Encryption Configuration 2. Test Data Access without Appropriate Permissions	1. Implement Strong Encryption Algorithms 2. Regularly Rotate Encryption Keys 3. Monitor Key Usage	ISO 27001, PCI-DSS	ISO 27001: A.8.2, PCI-DSS: 3.4
Network Security	Network Configuration	Linode Firewall Configuration	Unauthorized Access	1. Review Firewall Configuration 2. Test Network Access Controls	1. Implement Principle of Least Privilege 2. Enable Logging and Monitoring of Network Traffic	NIST CSF, CIS	NIST CSF: PR.AC-4, CIS Controls: 3.4
Incident Response	Incident Identification	Linode Incident Response Plan	Delayed Incident Response	1. Monitor Security Incidents 2. Configure Alarms for Suspicious Activities	1. Establish Incident Response Plan 2. Regularly Test Incident Response Procedures	NIST CSF, COBIT	NIST CSF: PR.PT-4, COBIT: BAI06
Compliance Monitoring	Compliance Reporting	Linode Compliance Management	Compliance Violations	1. Configure Compliance Policies 2. Generate Compliance Reports	1. Implement Automated Compliance Checks 2. Regularly Review Compliance Reports	ISO 27001, PCI-DSS	ISO 27001: A.12.4, PCI-DSS: 11.5


SkillWeed