bitHost

CLOUD SECURITY READINESS CHECKLIST

Essential Checkpoints for Secure Cloud Operations

Moving to the cloud or already there? This checklist helps you figure out if your cloud infrastructure is actually secure. Go through each item honestly. Finding gaps is good. It means you know what needs fixing before something breaks.

1. Cloud Infrastructure Visibility

You can't secure what you can't see. First step is knowing what's actually running in your cloud environment.

- ☐ We have a complete inventory of all cloud resources across all regions
- ☐ We know which cloud services we're using (compute, storage, database, etc.)
- ☐ We track resources across multiple cloud providers if we use more than one
- ☐ We have visibility into shadow IT (resources created outside official channels)
- ☐ We regularly audit for unused or forgotten resources
- ☐ We use tagging to organize and track cloud resources
- ☐ We have a cloud asset management system or tool
- ☐ We maintain network diagrams showing how cloud resources connect

2. Identity and Access Management

Who can access what in your cloud? Bad access control is one of the most common ways cloud environments get compromised.

- ☐ We use multi factor authentication for all cloud accounts
- ☐ We enforce strong password policies
- ☐ We follow principle of least privilege (people only get access they actually need)
- ☐ We regularly review and remove unnecessary access permissions
- ☐ We disable or delete accounts when employees leave
- ☐ We limit use of root or admin accounts
- ☐ We use role based access control (RBAC) instead of direct permissions
- ☐ We have separate accounts for production and development environments
- ☐ We monitor for suspicious login activity
- ☐ We use single sign on (SSO) where possible
- ☐ We audit all access changes and permission grants

3. Data Protection and Encryption

Your data is probably your most valuable asset. It needs to be encrypted and protected both when stored and when moving around.

- ☐ We encrypt data at rest (stored data)
- ☐ We encrypt data in transit (data moving between services)
- ☐ We use strong encryption standards (AES 256 or equivalent)
- ☐ We manage encryption keys securely (not hardcoded in applications)
- ☐ We use key management services provided by cloud vendors or third parties
- ☐ We regularly rotate encryption keys
- ☐ We classify data by sensitivity level
- ☐ We have data retention policies
- ☐ We securely delete data when no longer needed
- ☐ We control data residency (know where data is stored geographically)

4. Network Security

Cloud networks need proper boundaries and controls. Just because something is in the cloud doesn't mean it's automatically isolated and safe.

- ☐ We use firewalls to control traffic in and out of our cloud environment
- ☐ We segment networks (separate production from development, public from private)
- ☐ We use security groups or network ACLs to control traffic between resources
- ☐ We limit public internet access to only what's necessary
- ☐ We use VPNs or private connections for accessing cloud resources
- ☐ We implement DDoS protection
- ☐ We use web application firewalls (WAF) for web facing applications
- ☐ We monitor network traffic for suspicious patterns
- ☐ We disable unused ports and services
- ☐ We have proper DNS security configured

5. Compliance and Governance

Different industries have different rules. Make sure you're following whatever regulations apply to your business and location.

- ☐ We know which compliance requirements apply to us (GDPR, HIPAA, SOC 2, etc.)
- ☐ We have policies documented for cloud security
- ☐ We conduct regular security audits
- ☐ We maintain audit logs for compliance purposes
- ☐ We have data processing agreements with cloud providers
- ☐ We conduct regular compliance assessments
- ☐ We have someone responsible for cloud governance
- ☐ We review and update security policies regularly
- ☐ We have change management processes for cloud infrastructure

6. Incident Response and Monitoring

Security incidents will happen. The question is whether you'll catch them quickly and know what to do about them.

- ☐ We have 24/7 monitoring of cloud infrastructure
- ☐ We use security information and event management (SIEM) tools
- ☐ We have alerts set up for suspicious activities
- ☐ We log all critical activities and keep logs for adequate time
- ☐ We have an incident response plan documented
- ☐ We have assigned roles for incident response
- ☐ We practice incident response through drills or tabletop exercises
- ☐ We can isolate compromised systems quickly
- ☐ We document and learn from security incidents
- ☐ We have contact information for cloud provider support ready

7. Backup and Disaster Recovery

Cloud services can fail. Accounts can get compromised. You need backups and a plan to recover when things go wrong.

- ☐ We regularly backup critical data and systems
- ☐ We store backups in separate locations or regions
- ☐ We test backup restoration regularly
- ☐ We have a documented disaster recovery plan
- ☐ We know our recovery time objectives (how fast we need to recover)
- ☐ We know our recovery point objectives (how much data loss is acceptable)
- ☐ We encrypt backups
- ☐ We have immutable backups (that can't be deleted or modified)
- ☐ We test disaster recovery procedures at least annually
- ☐ We have failover capabilities to another region if needed

8. Application Security

Applications running in the cloud need to be secure too. Cloud security isn't just about infrastructure.

- ☐ We scan application code for vulnerabilities
- ☐ We perform security testing before deploying to production
- ☐ We use secure coding practices
- ☐ We keep application dependencies and libraries updated
- ☐ We validate and sanitize all user inputs
- ☐ We protect against common vulnerabilities (SQL injection, XSS, etc.)
- ☐ We use API security best practices

- ☐ We implement rate limiting to prevent abuse
- ☐ We conduct penetration testing

9. Configuration Management

Misconfiguration is one of the top causes of cloud security breaches. Default settings are usually not secure enough.

- ☐ We use infrastructure as code to manage cloud resources
- ☐ We scan for security misconfigurations automatically
- ☐ We follow cloud provider security best practices
- ☐ We use security benchmarks (CIS benchmarks, etc.)
- ☐ We regularly review and harden configurations
- ☐ We disable default accounts and credentials
- ☐ We have change control processes
- ☐ We document our security configurations
- ☐ We use configuration management tools
- ☐ We ensure storage buckets are not publicly accessible unless intended

10. Vendor and Third Party Risk

Your cloud security depends partly on your cloud provider and other third parties. You need to understand their security too.

- ☐ We review cloud provider security certifications
- ☐ We understand the shared responsibility model with our cloud provider
- ☐ We vet third party integrations for security
- ☐ We limit third party access to only what's necessary
- ☐ We have contracts that define security requirements
- ☐ We review vendor security practices regularly
- ☐ We monitor third party services for security issues
- ☐ We have exit strategies if a vendor becomes insecure

11. Container and Serverless Security

If you use containers or serverless functions, they need their own security considerations beyond traditional VMs.

- ☐ We scan container images for vulnerabilities
- ☐ We use trusted base images
- ☐ We implement container runtime security
- ☐ We secure container registries

- ☐ We apply least privilege to serverless functions
- ☐ We validate inputs to serverless functions
- ☐ We monitor container and serverless logs
- ☐ We keep container orchestration platforms updated

12. Security Operations and Team Readiness

Technology alone isn't enough. Your team needs to know what they're doing and stay updated on threats.

- ☐ We have security training for all team members
- ☐ We have specialized cloud security expertise on the team
- ☐ We stay updated on cloud security threats and best practices
- ☐ We conduct security awareness training regularly
- ☐ We have processes for security reviews of new cloud services
- ☐ We participate in threat intelligence sharing
- ☐ We have security champions in different teams
- ☐ We conduct regular security assessments and gap analysis
- ☐ We have budget allocated for security tools and training
- ☐ We measure and track security metrics

What Your Score Means

Count how many boxes you checked honestly. Here's where you stand:

Score	What It Means
0-30	Critical Risk: Major security gaps. You need immediate attention to basics like access control, encryption, and monitoring. Don't wait.
31-60	High Risk: You have some security in place but significant holes remain. Focus on the sections with the most unchecked boxes first.
61-80	Medium Risk: You're better than average. Keep working on weak areas and maintain what's working. You're on the right track.
81-100	Low Risk: Strong cloud security posture. Keep monitoring, testing, and improving. Security is never finished.

Priority Actions to Take Now

Don't try to fix everything at once. Start with these high impact items based on your weakest areas:

If you scored under 40:

- ☐ Enable multi factor authentication everywhere
- ☐ Turn on encryption for data at rest and in transit
- ☐ Review who has admin access and remove unnecessary permissions
- ☐ Set up basic monitoring and alerts
- ☐ Start regular backups if you haven't already

If you scored 40 to 70:

- ☐ Implement network segmentation
- ☐ Set up automated security scanning
- ☐ Create and test your incident response plan
- ☐ Review and update cloud configurations against benchmarks
- ☐ Conduct security training for your team

If you scored over 70:

- ☐ Conduct penetration testing
- ☐ Implement advanced threat detection
- ☐ Automate compliance monitoring
- ☐ Review and improve disaster recovery procedures
- ☐ Share your security practices with the team and industry

Remember: Cloud security is ongoing work, not a one time project. Review this checklist every quarter and adjust as your environment changes. What's secure today might not be secure tomorrow as new threats emerge.
