PLATOPS

Migrate to cloud securely

PlatOps provides security-first DevOps, cloud, and managed IT services for small and mid-sized businesses. We help organizations achieve compliance certifications, secure their infrastructure, and modernize their operations — without the enterprise price tag.

From SOC 2 and HIPAA compliance to cloud migrations and 24/7 monitoring, our team of engineers delivers measurable results with a 100% audit pass rate across 60+ client engagements.

100%	60+	8-12 wk	24/7
AUDIT PASS RATE	ORGANIZATIONS	AVG. TO COMPLIANCE	MONITORING

Cloud Migration Security Checklist

Secure Migration to AWS, Azure & GCP

Prepared by PlatOps Security Version 1.0 | January 2026

MIGRATION PHASES OVERVIEW

The 5 Phases of Secure Cloud Migration

PHASE	FOCUS	DURATION
1. Discovery	Inventory, dependencies, security baseline	2-4 weeks
2. Planning	Architecture, security controls, compliance	2-4 weeks
3. Preparation	Environment setup, security configuration	2-6 weeks
4. Migration	Data and workload transfer	2-8 weeks
5. Optimization	Security hardening, monitoring	Ongoing

STRATEGY	DESCRIPTION	SECURITY CONSIDERATIONS
Rehost	Lift and shift	Same vulnerabilities, new attack surface
Replatform	Minor optimizations	Configuration changes = new risks
Repurchase	Move to SaaS	Vendor security assessment needed
Refactor	Rebuild cloud-native	Secure by design opportunity
Retire	Decommission	Secure data disposal
Retain	Keep on-premises	Hybrid security considerations

PHASE 1 - DISCOVERY

Asset Inventory (6 items)

- □ Complete server and application inventory
- □ Document all data stores and databases
- □ Map network topology and traffic flows
- □ Identify sensitive data locations (PII, PHI, PCI)
- □ List all integrations and dependencies
- □ Document current security controls

Security Baseline Assessment (6 items)

- □ Conduct vulnerability assessment of existing systems
- □ Review current security configurations
- □ Document compliance requirements (SOC 2, HIPAA, PCI)
- □ Identify regulated data and requirements
- □ Assess current access control model
- □ Review existing security monitoring

Dependency Mapping (4 items)

- □ Map application dependencies
- □ Identify shared services
- □ Document external integrations
- □ List third-party connections

Risk Assessment (4 items)

- □ Identify migration risks
- □ Assess data exposure risks during transfer
- □ Evaluate downtime impact
- □ Document rollback requirements

Discovery Total: 20 items

Cloud Security Architecture (8 items)

- □ Design network segmentation (VPCs, subnets)
- □ Plan identity and access management (IAM)
- □ Define encryption strategy (at rest, in transit)
- □ Design security monitoring architecture
- □ Plan disaster recovery and backup
- □ Define incident response for cloud
- □ Design logging and audit trail
- □ Plan for compliance in target environment

Compliance Mapping (4 items)

- □ Map compliance requirements to cloud controls
- □ Identify cloud provider compliance certifications
- □ Document shared responsibility model
- □ Plan for compliance evidence collection

Security Tooling Selection (5 items)

- □ Select CSPM (Cloud Security Posture Management)
- □ Plan SIEM integration or cloud-native logging
- □ Choose identity management solution
- □ Select vulnerability management tools
- □ Plan for secrets management

Migration Security Plan (4 items)

- □ Define secure data transfer methods
- □ Plan for encryption during migration
- □ Document access controls during migration
- □ Create security testing plan

Planning Total: 21 items

PHASE 3 - PREPARATION

Cloud Environment Setup (8 items)

- □ Create landing zone with security baseline
- □ Configure network segmentation (VPCs, subnets, security groups)
- □ Set up IAM structure and policies
- □ Enable cloud provider security services
- □ Configure encryption (KMS keys)
- □ Set up logging and monitoring
- □ Configure backup and DR
- □ Implement security guardrails

Identity & Access (6 items)

- □ Create service accounts with minimal permissions
- □ Configure privileged access management
- □ Set up access review processes

Network Security (6 items)

- □ Configure security groups (deny by default)
- □ Set up network ACLs
- □ Implement WAF for public applications
- □ Configure DDoS protection
- □ Set up VPN or Direct Connect for hybrid
- □ Implement network monitoring

Encryption Configuration (4 items)

- □ Enable encryption at rest (all data stores)
- □ Configure TLS for data in transit
- □ Set up key management (KMS)
- □ Document key rotation procedures

Preparation Total: 24 items

PHASE 4 - MIGRATION EXECUTION

Pre-Migration Security (5 items)

- □ Verify target environment security configuration
- □ Test network connectivity securely
- □ Validate encryption is enabled
- □ Confirm logging is active
- □ Verify rollback procedures

Data Migration Security (6 items)

- □ Encrypt data during transfer
- □ Use secure transfer protocols (TLS, SSH)
- □ Validate data integrity (checksums)
- □ Monitor for data exposure during transfer
- □ Secure staging environments
- □ Delete source data securely when complete

Application Migration Security (5 items)

- □ Update application configurations for cloud
- □ Rotate all secrets and credentials
- □ Update security group rules
- □ Configure cloud-native security services
- □ Test application security post-migration

Cutover Security (4 items)

□ Verify backup and recovery

Migration Execution Total: 20 items

PHASE 5 - POST-MIGRATION OPTIMIZATION

Security Hardening (8 items)

□ Run cloud security posture assessment

□ Remediate misconfigurations

□ Review and tighten IAM policies

□ Implement additional security controls

□ Enable advanced threat detection

□ Configure compliance monitoring

□ Optimize security costs

□ Document security baseline

Continuous Monitoring (6 items)

□ Configure security alerting

□ Set up automated response (SOAR)

□ Implement vulnerability scanning

□ Enable compliance monitoring

□ Configure cost monitoring for security spend

□ Set up regular security reviews

Decommissioning Source (4 items)

□ Secure source system decommissioning

□ Verify data deletion from source

□ Revoke access to old systems

□ Archive audit logs from migration

Post-Migration Total: 18 items

AWS Security Essentials

SERVICE	PURPOSE
AWS IAM	Identity and access management
AWS GuardDuty	Threat detection
AWS Security Hub	Security posture
AWS Config	Compliance monitoring
AWS KMS	Key management
AWS WAF	Web application firewall
AWS CloudTrail	Audit logging
AWS VPC	Network isolation

Azure Security Essentials

SERVICE	PURPOSE
Azure AD	Identity management
Azure Defender	Threat protection
Azure Security Center	Security posture
Azure Policy	Compliance
Azure Key Vault	Secrets management
Azure Firewall	Network security
Azure Monitor	Logging and monitoring

GCP Security Essentials

SERVICE	PURPOSE
Cloud IAM	Identity and access
Security Command Center	Security posture
Cloud Armor	DDoS and WAF
Cloud KMS	Key management
VPC Service Controls	Data exfiltration prevention
Cloud Audit Logs	Audit logging

Top 10 Mistakes to Avoid

1. **Lifting security gaps** - Same vulnerabilities in cloud
2. **Overly permissive IAM** - Everyone is admin
3. **Public storage buckets** - S3/Blob exposed
4. **Unencrypted data transfer** - Data exposed in transit
5. **No network segmentation** - Flat network in cloud
6. **Disabled logging** - No visibility into threats
7. **Default credentials** - Unchanged passwords
8. **Missing MFA** - Single factor for admin
9. **No vulnerability scanning** - Unknown weaknesses
10. **Skipping compliance mapping** - Regulatory gaps

CHECKLIST SUMMARY

Controls by Phase

PHASE	ITEMS	TIMELINE
Discovery	20	Weeks 1-4
Planning	21	Weeks 3-6
Preparation	24	Weeks 5-10
Migration	20	Weeks 8-16
Post-Migration	18	Weeks 14+
TOTAL	**103**	

Critical Success Factors

- □ Executive sponsorship for security
- □ Security team involvement from day 1
- □ Compliance requirements documented early
- □ Rollback plan tested
- □ Security testing before go-live

Let our team of security and infrastructure experts help you achieve your goals faster.

100%	60+	8-12 wk	24/7
AUDIT PASS RATE	ORGANIZATIONS SERVED	AVG. TIME TO COMPLIANCE	MONITORING & SUPPORT

Get Free Assessment | Book Strategy Call | Cloud Migration Services

Email: hello@platops.com Phone: (202) 864-1197 Web: platops.com

This document is provided for informational purposes only. Requirements may vary based on your organization's specific circumstances. PlatOps is a registered trademark. Redistribution without permission is prohibited.