Cloud IT Infrastructure Audit Checklist

*This is a general checklist, and specific sections may need to be adapted based on your specific cloud infrastructure and security requirements.

gartsolutions.com

info@gartsolutions.com

Cloud Services and Providers

Service Model

- [ ] Verify the cloud service model used (IaaS, PaaS, SaaS) aligns with organizational needs.

- [ ] Assess the security posture and compliance certifications of the cloud provider.

Deployment Model

- [ ] Identify the cloud deployment model (public, private, hybrid).

- [ ] Review the contract terms regarding security, data ownership, and audit rights.

Service Level Agreements (SLAs)

- [ ] Verify SLAs meet performance, uptime, and availability requirements.

- [ ] Assess disaster recovery and incident response procedures outlined in SLAs.

gartsolutions.com

info@gartsolutions.com

gart.

Identity and Access Management (IAM)

Access Controls

- [ ] Evaluate IAM policies and access controls for cloud resources.
- [ ] Verify the principle of least privilege is enforced for user access.

Multi-Factor Authentication (MFA)

- [ ] Confirm MFA is enabled for all user accounts with access to cloud resources.
- [ ] Assess the strength and complexity requirements for cloud account passwords.

User Provisioning and Deactivation

- [ ] Review processes for user provisioning, access control changes, and deactivation upon termination.
- [ ] Verify automated workflows are in place for user lifecycle management.

gartsolutions.com

info@gartsolutions.com

gart.

Resource Management

Inventory and Visibility

- [ ] Confirm a comprehensive inventory of all cloud resources is maintained.

- [ ] Assess the use of cloud tagging for resource identification and cost allocation.

Resource Utilization

- [ ] Evaluate cloud resource utilization to identify potential optimization opportunities.

- [ ] Review processes for right-sizing cloud resources to avoid unnecessary costs.

Cost Management

- [ ] Verify cloud cost monitoring and budgeting practices are implemented.

- [ ] Assess cost allocation and chargeback models for cloud resources used by different departments.

gartsolutions.com

info@gartsolutions.com

gart.

Data Security and Encryption

Data at Rest Encryption

- [ ] Confirm data at rest is encrypted using industry-standard encryption algorithms.
- [ ] Assess key management practices for encryption keys used in the cloud environment.

Data in Transit Encryption

- [ ] Verify data in transit between cloud resources and on/off-premises locations is encrypted.
- [ ] Review secure transport protocols (HTTPS, SSH) used for data transfer.

gart.

gartsolutions.com

info@gartsolutions.com

Logging and Monitoring

Cloud Logging

- [ ] Verify comprehensive logging for all cloud resources and user activities is enabled.

- [ ] Assess log retention policies and procedures for secure log storage and analysis.

Security Monitoring

- [ ] Confirm continuous monitoring for suspicious activities and potential security threats.

- [ ] Evaluate integration of cloud security monitoring tools with existing security information and event management (SIEM) systems.

Alerting and Notification

- [ ] Verify timely alerts are configured for security incidents, resource anomalies, and performance issues.

- [ ] Assess escalation procedures and responsibilities for responding to security alerts.

gartsolutions.com

info@gartsolutions.com

Vulnerability Management

Vulnerability Scanning

- [ ] Confirm regular vulnerability scanning of cloud resources for known security weaknesses.

- [ ] Assess patch management procedures for timely remediation of identified vulnerabilities.

Security Configuration Management

- [ ] Verify secure configuration baselines are established for cloud resources.

- [ ] Assess configuration management tools and processes for maintaining consistent security settings.

Penetration Testing

- [ ] Confirm periodic penetration testing is conducted to identify exploitable vulnerabilities in the cloud environment.

- [ ] Evaluate remediation plans and timelines for addressing vulnerabilities discovered during penetration tests.

gartsolutions.com

info@gartsolutions.com

gart.

Disaster Recovery and Business Continuity

Backup and Recovery

- [ ] Verify backups of critical data and cloud resources are performed regularly.

- [ ] Assess backup retention policies and procedures for offsite data storage and retrieval.

Disaster Recovery Plan

- [ ] Confirm a documented disaster recovery plan exists for the cloud environment.

- [ ] Assess testing and validation procedures for the disaster recovery plan to ensure effectiveness.

Business Continuity

- [ ] Evaluate the impact of potential cloud outages on critical business processes.

- [ ] Assess business continuity plans for maintaining essential operations during cloud service disruptions.

gartsolutions.com

info@gartsolutions.com

gart.

Compliance

Regulatory Requirements

- [ ] Identify relevant industry regulations and compliance requirements applicable to cloud data.
- [ ] Assess controls and procedures implemented to ensure compliance with data privacy regulations.

Audit Logging

- [ ] Verify audit logging is enabled for all cloud resources and user activities relevant to compliance.
- [ ] Assess procedures for retaining and presenting audit logs for regulatory compliance purposes.

gartsolutions.com

info@gartsolutions.com

Gart Solutions - Your Trusted DevOps & Cloud Services Provider.

We have extensive experience conducting IT infrastructure audits that deliver the insights organizations need.

gart.

gartsolutions.com

info@gartsolutions.com