



Cloud Infrastructure Service Desk Support Checklist 2026

Incident Intake & Initial Assessment

Procedures for verifying service desk tickets, identifying-affected cloud resources, and determining the severity of the infrastructure outage or performance degradation.

Incident Ticket ID

Write something...

Incident Severity Level

- ☐ Critical (P1) - Total Service Outage
- ☐ High (P2) - Major Functionality Degradation
- ☐ Medium (P3) - Partial Service Disruption
- ☐ Low (P4) - Minor Bug or Feature Request

Incident Detection Timestamp

Enter date...

Initial Issue Description

Write something...

Affected Cloud Services

- ☐ Compute (EC2/VMs)
- ☐ Storage (S3/Blob)
- ☐ Networking (VPC/DNS)
- ☐ Database (RDS/SQL)
- ☐ Identity & Access (IAM)

Error Logs or Screenshots

 Upload File

Cloud Environment & Resource Identification

Steps to identify specific cloud providers (AWS, Azure, GCP), regions, availability zones, and impacted microservices or virtual machine instances.

Cloud Service Provider

- ☐ Amazon Web Services (AWS)
- ☐ Microsoft Azure
- ☐ Google Cloud Platform (GCP)
- ☐ Oracle Cloud (OCI)
- ☐ IBM Cloud
- ☐ Other

Affected Resource ID

Write something...

Impacted Service Layers

- ☐ Compute (EC2/VMs)
- ☐ Storage (S3/Blob/Disk)
- ☐ Database (RDS/SQL/NoSQL)
- ☐ Networking (VPC/DNS/CDN)
- ☐ Identity & Access (IAM/AD)
- ☐ Containerization (Kubernetes/ECS)

Cloud Region/Availability Zone

- ☐ US-East (N. Virginia)
- ☐ US-West (Oregon)
- ☐ EU-Central (Frankfurt)
- ☐ AP-Southeast (Singapore)
- ☐ Other/Global

Environment Context Details

Write something...

Service Level Agreement (SLA) Verification

Checklist for verifying current SLA commitments, calculating remaining time before breach, and notifying stakeholders of potential downtime impact.

SLA Tier Level

- ☐ Critical (P1) - 1 Hour Response
- ☐ High (P2) - 4 Hour Response
- ☐ Medium (P3) - 1 Business Day Response
- ☐ Low (P4) - 3 Business Days Response

Incident Start Timestamp

Enter date...

Current Time Remaining (Minutes)

Enter a number...

Impacted Service Categories

- ☐ Compute/EC2
- ☐ Storage/S3
- ☐ Database/RDS
- ☐ Networking/VPC
- ☐ Identity/IAM

SLA Breach Risk Assessment

Write something...

Incident Manager Verification

Diagnostic & Troubleshooting Protocols

Standardized procedures for checking VPC connectivity, monitoring cloudwatch/log metrics, inspecting load balancer health, and reviewing IAM permission errors.

Impacted Cloud Service Provider

- ☐ AWS
- ☐
- ☐ Google Cloud Platform (GCP)
- ☐ Other/Hybrid

Components Under Investigation

- ☐ Compute Instances (EC2/VM)
- ☐ Storage Buckets (S3/Blob)
- ☐ Networking (VPC/DNS/VPN)
- ☐ Database Services (RDS/SQL)
- ☐ Load Balancers
- ☐ IAM & Permissions

Error Code or Exception Log Snippet

Detailed Diagnostic Findings

Write something...

System Logs or Screenshot of Error

 Upload File

Time of First Detected Anomaly

Enter date...

Escalation & Incident Response Management

Guidelines for notifying DevOps engineers, Cloud Architects, or Security Operations Centers (SOC) based on predefined escalation matrices.

Escalation Severity Level

- ☐ P1 - Critical (Total Outage)
- ☐ P2 - High (Degraded Performance)
- ☐ P3 - Medium (Partial Functionality Loss)
- ☐ P4 - Low (Minor Issue/Inquiry)

Primary Stakeholders Notified

- ☐ DevOps Team
- ☐ Security Operations (SOC)
- ☐ Cloud Infrastructure Architects
- ☐ Customer Success Managers
- ☐ IT Management

Escalation Reference ID

Write something...

Time of Escalation Trigger

Enter time...

Incident Summary for Management

Write something...

System Logs or Error Screenshots

 Upload File

Infrastructure Remediation & Recovery

Actionable steps for executing failovers, restarting containerized services, restoring snapshots, or re-provisioning failed resources.

Primary Remediation Action Taken

- ☐ Instance/Container Restart
- ☐ Snapshot/Backup Restoration
- ☐ Scaling Event (Vertical/Horizontal)
- ☐ Network/Security Group Update
- ☐ Configuration Rollback
- ☐ Traffic Re-routing/Failover

Affected Cloud Services

- ☐ Compute (EC2/VM)
- ☐ Storage (S3/Blob)
- ☐ Database (RDS/SQL)
- ☐ Networking (VPC/DNS)
- ☐ Identity (IAM/AD)

Recovery Command/Script Used

Write something...

Recovery Log/Error Logs

 Upload File

Completion Date of Recovery

Enter date...

Lead Engineer Approval

Communication & Stakeholder Updates

Templates and frequency requirements for updating internal management and end-users regarding service restoration progress and estimated time of recovery (ETR).

Stakeholder Impact Level

- ☐ Low (Individual User)
- ☐ Medium (Departmental)
- ☐ High (Enterprise-wide)
- ☐ Critical (Global/Public)

Primary Communication Channel

Update Summary for Stakeholders

Last Update Sent Timestamp

Recipient Groups Notified

- ☐ Engineering Team
- ☐ Product Management
- ☐ Customer Success
- ☐ Executive Leadership
- ☐ External Clients

Incident Lead Approval

Post-Incident Review & Root Cause Analysis (RCA)

Documentation steps for capturing the timeline of events, identifying the primary cause of failure, and documenting permanent architectural fixes.

Incident Occurrence Date

Time of Incident Detection

Primary Root Cause Category

- ☐ Hardware/Infrastructure Failure
- ☐ Software/Code Bug
- ☐ Configuration/Deployment Error
- ☐ Security Breach/Unauthorized Access
- ☐ Network/Connectivity Issue
- ☐ Human Error

Detailed Root Cause Description

Write something...

Impacted Cloud Services

- ☐ Compute (EC2/VMs)
- ☐ Storage (S3/Blobs)
- ☐ Database (RDS/SQL)
- ☐ Networking (VPC/DNS)
- ☐ Identity & Access (IAM)

Corrective Actions & Prevention Plan

Write something...

Upload System Logs or Error Screenshots

 Upload File

Lead Engineer Approval

Post-Resolution Verification & Monitoring

Procedures to confirm service stability, validate data integrity after recovery, and monitor resource utilization for any recurring patterns of instability.

Service Restoration Status

- ☐ Fully Restored
- ☐ Degraded Performance
- ☐ Partial Functionality

Monitored Cloud Components

- ☐ Compute Instances (EC2/VM)
- ☐ Database Clusters (RDS/SQL)
- ☐ Storage Buckets (S3/Blob)
- ☐ Load Balancers
- ☐ Network/VPC Connectivity

Error Rate Percentage Post-Recovery

Verification Completion Date

Observed Anomalies Post-Recovery

Cloud Engineer Validation

Incident Closure & Documentation Update

Final steps for closing the service desk ticket, updating the internal Knowledge Base (KB), and updating the 2026 Infrastructure Asset Register.

Incident Resolution Date

Time of Service Restoration

Root Cause Category

- ☐ Configuration Error
- ☐ Hardware/Provider Outage
- ☐ Security Breach/Unauthorized Access
- ☐ Software Bug/Deployment Issue
- ☐ Network/Connectivity Issue
- ☐ Human Error

Summary of Resolution Steps

Write something...

Documentation Updated

- ☐ Knowledge Base (KB) Article
- ☐ Incident Report/RCA Document
- ☐ Infrastructure Asset Inventory
- ☐ SLA Compliance Log

Final Incident Report (RCA) PDF

 Upload File

Service Desk Lead Approval

< Previous

> Next

✓ Finish

 **Generate Sample Report**