Good Consulting

Cloud Collaboration Service Runbook

Operational procedures and troubleshooting guidance for maintaining and restoring client cloud collaboration environments managed by Good Consulting.

Owner: Managed Cloud Services Team
Version: 1.0
Version date: February 2026

Table of Contents

Overview

This runbook provides operational guidance for maintaining, monitoring, and restoring cloud collaboration environments managed by Good Consulting.

These environments support distributed teams using Microsoft 365 or Google Workspace integrated with secure identity management and cloud infrastructure services.

This document standardizes incident response procedures to ensure:

- Consistent remediation across client environments
- Reduced downtime and faster resolution
- Secure handling of identity and access issues
- Clear escalation and communication pathways

Good Consulting empowers teams to do their best work in the cloud by delivering secure, scalable, and reliable digital workplace solutions.

When to Use This Runbook

Use this document when one or more of the following conditions occur:

- Users cannot access collaboration platforms
- Performance of cloud productivity tools is degraded
- Authentication or synchronization errors occur
- Monitoring systems report availability alerts

> ⚠ Critical production environments may support multiple client organizations. Always confirm the affected tenant or environment before performing remediation steps.

Architecture

Good Consulting manages cloud-first collaboration environments built on trusted public cloud platforms. These environments integrate identity, productivity, infrastructure, and backup services to ensure secure and scalable operations.

Each component plays a distinct role in maintaining availability, performance, and data protection.

Component	Description	Platform
Identity & Access	Authentication and user management	Microsoft Entra ID / Google Identity
Collaboration Platform	Messaging, file sharing, and productivity tools	Microsoft 365 / Google Workspace
Cloud Infrastructure	Hosts applications and integrations	AWS / Azure / Google Cloud
Backup & Recovery	Protects collaboration and user data	Managed Backup Services

Information

Architecture diagrams and environment-specific configuration details are maintained in client-specific documentation spaces and should be consulted before major changes.

Support Contacts

Clear ownership and escalation pathways are critical to maintaining service continuity. The following contacts should be used based on incident type and severity.

Role	Team	Contact Method
Service Owner	Managed Cloud Services	Slack #cloud-operations
Client Support	Customer Success Team	support@goodconsulting.com
Infrastructure Support	Cloud Engineering	PagerDuty

Runs (Operational Tasks)

Routine operational tasks reduce the likelihood of incidents and ensure continued compliance and performance optimization.

These recurring checks support proactive issue detection and long-term stability.

Task	Frequency	Owner
Environment Health Check	Daily	Cloud Operations
Security & Compliance Review	Monthly	Security Team
Backup Verification	Weekly	Infrastructure Team

Process

This section outlines the standard procedures for addressing common operational scenarios.

Service Access Issues

Access-related issues typically stem from identity configuration changes, licensing problems, or authentication failures.

1. Verify identity provider availability
2. Confirm user account status and group membership
3. Validate service licensing and subscription status
4. Test login through the admin console
5. Review recent configuration or policy changes

Expected Outcome:

User access is restored and authentication logs confirm successful login activity.

Performance Degradation

Performance issues may result from resource saturation, network latency, or recent configuration changes.

1. Review monitoring dashboards
2. Check infrastructure utilization
3. Validate network connectivity
4. Review recent deployments or configuration changes

System performance returns to normal operational thresholds.

Application Monitoring

Good Consulting uses centralized monitoring and alerting tools to maintain visibility across managed cloud environments. Monitoring enables early detection of anomalies and rapid response to potential service disruptions.

Metric	Tool	Alert Threshold
Service Availability	Cloud Monitoring Platform	< 99.5% uptime
Authentication Failures	Identity Monitoring	Spike in login failures
Resource Utilization	Cloud Provider Monitoring	> 85% utilization

> Alerts should be triaged within defined SLA timeframes.

Known Errors

The following common errors have been observed across managed environments. These should be reviewed before escalating incidents.

Error Code	Description	Suggested Resolution
AUTH-FAIL	Authentication service unavailable	Verify identity provider status
SYNC-ERR	Collaboration synchronization failure	Restart sync services
BACKUP-WARN	Backup job incomplete	Re-run backup job

Troubleshooting

This section provides structured diagnostic guidance for common incident types.

User Cannot Access Collaboration Tools

Access issues are often related to identity, permissions, or licensing inconsistencies.

Check:

- Identity service health
- User permission changes
- License availability

Resolution:

- Reset authentication session
- Reassign license if required
- Confirm user directory synchronization

Backup Failure

Backup failures can impact compliance and recovery readiness and must be addressed promptly.

Check:

- Backup job logs
- Storage availability
- Network connectivity

Resolution:

- Restart backup job
- Validate storage quotas
- Notify infrastructure team if failure persists

Post-Incident Actions

Once the incident has been resolved, the following actions must be completed to ensure continuous improvement and knowledge retention:

After resolving incidents:

- Document root cause
- Update monitoring rules if necessary
- Notify client stakeholders
- Update runbook if new scenarios are identified

Related Documentation

The following documents provide additional context and supporting procedures:

- Cloud Migration Playbook
- Security & Compliance Guidelines
- Disaster Recovery Procedures

Service Scope & Boundaries

This section defines what is covered — and not covered — under this runbook to prevent operational ambiguity.

In Scope

- Microsoft 365 / Google Workspace tenant management
- Identity provider configuration
- Backup and restore operations
- Collaboration performance monitoring
- User access management

Out of Scope

- End-user device troubleshooting
- Third-party SaaS applications not managed by Good Consulting
- Custom client-developed integrations
- Legal or compliance advisory services

> ℹ If an issue falls outside scope, escalate to Client Success for clarification before proceeding.

Environment Inventory

Maintaining an up-to-date inventory ensures accurate incident isolation.

Environment	Region	Cloud Provider	Purpose	Criticality
Production	EU-West	Azure	Primary Collaboration	High
Staging	EU-West	Azure	Testing & Validation	Medium
Backup Environment	Multi-Region	AWS	Data Protection	High
Identity Tenant	Global	Entra ID	Authentication	High

Access Control Model

Proper access control ensures secure and compliant collaboration environments.

Role	Description	Privilege Level
Global Admin	Full tenant access	High
Service Admin	Manages collaboration services	Medium
Security Admin	Manages security policies	High
Support Engineer	Troubleshooting access	Limited

⚠ Global Administrator access should be restricted and logged. Emergency elevation must follow change approval procedures.

Change Management

All production-impacting changes must follow structured change control procedures.

Change Type	Description	Approval Required
Standard	Pre-approved recurring change	No
Normal	Scheduled infrastructure change	Yes
Emergency	Incident-driven immediate change	Post-approval

Change Workflow

1. Submit change request
2. Perform risk assessment
3. Obtain approval
4. Execute change
5. Validate outcome
6. Document results

Security & Compliance Controls

Security is foundational to Good Consulting's managed cloud services.

Core Controls

- Multi-factor authentication enforced
- Conditional access policies configured
- Encryption in transit and at rest
- Regular access reviews
- Backup integrity verification

Control Area	Frequency	Responsible Team
Access Review	Quarterly	Security Team
Backup Audit	Monthly	Infrastructure Team
Policy Review	Bi-Annual	Cloud Engineering

Service Level Objectives (SLOs)

Defined service expectations ensure measurable reliability.

Metric	Target	Measurement Period
Availability	99.9%	Monthly
Incident Response	< 30 minutes	Per Incident
Backup Recovery Time	< 4 hours	Per Event
Authentication Latency	< 500ms	Continuous

Escalation Matrix

Escalation must follow severity definitions.

Severity Levels

Severity	Definition	Response Time
SEV1	Full service outage	Immediate
SEV2	Major degradation	< 1 hour
SEV3	Minor issue	< 4 hours
SEV4	Low impact	Next business day

Audit Logging & Reporting

Operational transparency is critical for compliance and accountability.

Logging Requirements

- Authentication logs retained 90 days
- Admin actions logged
- Backup execution logs retained
- Security alerts archived

Report	Frequency	Audience
Incident Summary	Monthly	Clients
Security Review	Quarterly	Stakeholders
SLA Performance	Monthly	Leadership

Continuous Improvement

Good Consulting continuously improves its managed services model through structured review and feedback cycles.

Improvement Activities

- Quarterly service reviews
- Monitoring threshold refinement
- Runbook updates after incidents
- Automation enhancement

ℹ This runbook is a controlled operational document. Unauthorized modification may result in inconsistent service delivery.

Appendix A – Command References

Command	Purpose
Reset-UserSession	Reset authentication session
Get-UserLicense	Validate license assignment
Invoke-BackupJob	Trigger backup
Test-CloudHealth	Run system health check

Appendix B – Glossary

Term	Definition
Tenant	Dedicated cloud environment
RTO	Recovery Time Objective
RPO	Recovery Point Objective
MFA	Multi-Factor Authentication

Revision History

Version	Date	Notes
1.0	February 2026	Initial template content