Choosing a cloud managed service provider

A practical MSP selection guide that tests proposals against incident scenarios

A practical IXC resource for adoption decisions and delivery

Published 2026.09 · English edition · PDF + Excel worksheets

Using this resource

Compares each provider's operating scope and incident response evidence against the same criteria and settles open items before the contract is signed.

Technology leaders, procurement staff and service owners considering outsourcing cloud operations

Contents

01 Attach responsibilities to the server list 3

02 Follow one incident through to the end 4

03 Compare operational responsibility by candidate 5

04 Settle price and exit terms as well 6

How to complete and reuse it

Read the criteria in this PDF, then fill the blank fields with your actual conditions and anything still unconfirmed. The Excel file for the same practice area has a worksheet for each resource. Keep the worked examples separate from real customer cases and confirmed quotes.

With attribution, you may quote and adapt this material for internal review and your own work. The latest files are at www.ixc.co.kr/en/assets.

Attach responsibilities to the server list

The scope of managed operations can only be compared when it lists both the number of resources and the types of work. Start by settling whether server management includes fixing application errors.

Before requesting proposals, break the services you run down into named business functions. The best units are ones whose impact you can explain when they stop, such as order intake, member login and the settlement batch. Link each function to its servers, databases, external integrations and internal owner. Even with access to the account, response stops right there without the authority to deploy code or approve a data recovery.

Responsibility boundary	Question for the provider	Evidence to request
Detection	Who confirms user impact first?	Alert rules and on-call paging path
Recovery	How far do you act on prior approval?	Runbook, permitted commands and recovery approval matrix
Change	Who confirms after a patch that the business function works normally?	Change request and verification results
Improvement	Who finishes the follow-up work on recurring incidents?	Action owner and completion criteria

Where quote comparison starts

Before counting response staff, agree on the work you are handing over and the evidence you will receive. When every candidate gets the same service list and question sheet, missing items and extra scope become visible.

Follow one incident through to the end

A line promising ‘24/7 response’ does not by itself show what happens after intake. Take a night-time order failure and have the provider walk you through it from detection to confirmed recovery.

Worked example: At night, order API errors rise while server resource metrics stay normal. The provider explains which alert it receives and on which screen it checks the scope of impact. Next, settle who has the authority to roll back recent changes, who checks the data and who writes the customer notice. Only by recording first response time and actual recovery time as separate items can you pick out a contract that is fast only at intake.

- Break the provider's explanation down into detection time, acknowledgement time, action time and recovery confirmation time.
- Separate the actions that can go ahead when no one internal can be reached from those that must wait.
- Assign emergency recovery and root cause analysis as separate tasks, and name who shares progress updates.
- Check that the closing report records recent changes, user impact, temporary measures and residual risk.

> **When the evidence is missing**
>
> If the walkthrough relies only on the assigned engineer's skill, also ask for a draft runbook and the contact path. Leave the item unsettled until the function's criticality and response authority are agreed.

Compare operational responsibility by candidate

Record answers as who actually does the work and where the evidence is kept, not as ‘supported’. If a critical function has no one responsible, resolve that before signing, regardless of the total score.

MSP candidate comparison worksheet

Question	Evidence required	Candidate answer and owner	Open items and due date
Who recovers incidents at night?	On-call and escalation chart		
Who approves recovering data?	Recovery test records and approval matrix		
What is rolled back when a change fails?	Change history and the rollback procedure		
How are monthly cost changes explained?	Bill breakdown and change comparison table		
What is returned when the contract ends?	Return list for accounts, settings and documents		

Decide which items are mandatory based on the impact if the function stops and whether an alternate owner exists. First confirm that every candidate received the same request. If unanswered items are simply scored low, the price score can hide a gap in responsibility. Track each open item through four elements: the question, who will answer, the evidence required and the reply date.

> **Worked example**
>
> An answer of ‘backup operations available’ is the starting point for asking again about ‘who checks for backup failures, who runs the recovery test, the test environment and who approves the recovery result’. Ask for separate evidence that a backup file exists and that the business function was successfully recovered.

Settle price and exit terms as well

In the selection result, record the monthly operations fee alongside one-off work and the work that stays in-house. Operations can be handed over reliably only when both the start and the end are explained.

Cost item	Scope to confirm	Values for the internal purchase request
Regular operations	Checks, patches, reviews and on-call	Frequency, covered resources and report items
Initial takeover	Asset discovery and runbook consolidation	Takeover completion criteria
Additional work	Migration, major changes and new setups	Request, sizing and approval procedure
Tools and accounts	Monitoring, backup and access management	Owner and who bears the cost
Exit handover	Settings, history and access revocation	Return format and receiving owner

The selection memo records both the reasons for choosing and the reasons for any hold. Record READY when response responsibility and recovery evidence are in order, and READY WITH CONDITIONS when the items still to be addressed have owners and due dates. If a critical function has no approver or recovery procedure, record HOLD and schedule when they will be confirmed. These verdicts follow a procurement review template proposed by IXC.

> **Scope to review with IXC**
>
> IXC's Managed Cloud covers monitoring and incident response; patch, change and security operations; and SLO review and improvement. The scope of action between your internal development team and IXC is set against your current asset inventory and comparison sheet.

IXC

Publication and use

Send your asset inventory, recent incident history and the open items in your candidate comparison sheet, and we can discuss what Managed Cloud would cover and the order of takeover.

IXC Corp.

CEO Nam Kichul | Business registration no. 109-86-56732
4F 408, Chuncheon ICT Venture Center
7 Huseok-ro 462beon-gil, Chuncheon-si, Gangwon-do, Republic of Korea
+82-33-242-0210 | info@ixc.co.kr

www.ixc.co.kr

www.ixc.co.kr/en/services/managed-cloud

www.ixc.co.kr/en/assets/cloud-managed-service-guide

References

IXC Managed Cloud

https://www.ixc.co.kr/en/services/managed-cloud

Google SRE Workbook: Incident Response

https://sre.google/workbook/incident-response/

Google SRE Workbook: Implementing SLOs

https://sre.google/workbook/implementing-slos/