IXC

Cloud kickoff and operations handover checklist

From account handover to a recovery test, a template for confirming with evidence that the handover is complete

A practical IXC resource for adoption decisions and delivery

Published 2026.09 · English edition · PDF + Excel worksheets

Using this resource

Finds gaps in assets, access, escalation and recovery during an operations transition, and sets the criteria for completing the handover.

Owners preparing the kickoff meeting after signing a cloud contract, and handover leads taking over operations

---

Contents

01 Link each asset to its owner and business function 3

02 Verify access with real actions 4

03 Handover evidence and open items log 5

04 Run one recovery and one change 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.

Link each asset to its owner and business function

Handover starts with receiving the account list. The business functions to be operated, each asset's management location and the owners of its cost and access must connect in the same table.

Separate production, staging and development environments under each service name. Beyond each environment's servers and databases, include domains, DNS, certificates, repositories, deployment paths and external integrations. Sign in to each asset's management console to confirm that it exists and which environment it belongs to, then mark its handover status. If accounts registered to individuals or contact details of departed employees remain, assign a responsible department and a schedule for changing them.

Handover group	What to check	Evidence checked
Services and environments	Business function, critical hours and environment split	Architecture diagram and sign-in check
Accounts and billing	Account holder, billing recipient and renewal owner	Account settings and billing history
Domains and certificates	Registration, DNS and renewal locations	Management locations and expiry list
Deployment and external integrations	Repositories, deployment permissions and dependent services	Run history and integration list

Decisions to record at the first meeting

Do not delete unaccounted-for assets or make assumptions about them. Classify each as owner unconfirmed, no access or document mismatch, then assign a reviewer and a completion date. When the handover scope changes, update the architecture diagram and the inventory together.

Verify access with real actions

Being able to sign in to a console is not the same as being able to take the action required. Verify the access needed for daily operations and for emergency recovery separately.

- Split read, change and approval permissions by job function. Check whether cost-viewing and operational change permissions need to be granted together.
- Instead of shared accounts, set an access method that identifies each person. Record who approves requests to add, change or revoke access.
- Do not write secret values into handover documents. Record the storage location, access roles, rotation owner and date last checked.
- For emergency access, define both the reasons for using it and the procedure for revoking it afterward. Run tests within an approved environment and scope.

Worked example: An operator can view monitoring but cannot run a database recovery. This may not simply be missing access. First confirm whether the operating model grants a separate role once recovery is approved, or whether another team performs the recovery. Connect the required permissions to the approval procedure, then decide whether the handover is complete.

> **Completion criteria for access verification**
>
> An approved test task must succeed, and the person who ran it and the task history must be recorded. Set the order for revoking the previous owner's access after confirming the new owner's access and operational readiness.

Handover evidence and open items log

Record document receipt, access confirmation and test success as separate statuses. Reading the blanks as they stand at the handover meeting lets you set the next owner and deadline.

Cloud handover confirmation worksheet

Question to confirm	Evidence required	Status and evidence location	Owner and deadline
Do the production environment and the assets match?	Architecture diagram and asset comparison results		
Does emergency contact actually get through?	Contact test and alternate contacts		
Has the business been restored from a backup?	Recovery test and business check results		
Are you ready to roll back a change?	Deployment and configuration rollback records		
Have the items to hand over at exit been agreed?	Return list and owner table		

Record the status as not received, under verification, confirmed or needs remediation. “Backup exists” does not mark a recovery test as complete. The record includes the test date, the target data, the recovery environment and who verified the business. If access to production data is restricted, verify the procedure with approved test data and note under open items the conditions that differ from a real production recovery.

> **Handover with conditions**
>
> For each open item on a critical business function, set an interim workaround and an owner for resolving it. A recovery or contact gap with no interim workaround is not marked as handover complete; escalate it to the kickoff lead with a resolution schedule.

Run one recovery and one change

Scheduling a small change and a recovery test in the first operating cycle shows where the documents differ from the real environment. The person who will confirm that the business is running normally takes part too.

Verification stage	Activities	Record to keep
Preparation	Confirm the target, change window, approval and stop conditions	Test plan and contact list
Execution	Backup restore or an approved configuration change	Run timestamps and task results
Business check	Verify sign-in, lookups and key transactions	Owner confirmation and error list
Close	Return to the original state, clean up permissions and update documents	Final state and follow-up tasks

RTO is the time allowed until recovery, and RPO is the span of data loss that can be tolerated. Compare the backup frequency and the recovery test results against these two targets. Confirming only that the system starts can leave external integration and data consistency problems behind. In the actual operations transition, also include the escalation path and change approval in the same test.

> **Handover close-out meeting**
>
> Review the completion evidence and the remaining remediation items, then set the date operations begin. IXC continues from infrastructure build into managed operations, and agrees on the handover scope based on your asset, deployment, access and backup documentation.

IXC

Publication and use

Working from your current architecture diagram, your handover table and your backup and recovery records, we set access permissions and the scope of the operations transition together with you.

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-kickoff-checklist

References

IXC Cloud Infrastructure Build

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

IXC Managed Cloud

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

Google SRE Workbook: Incident Response

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