CYGNUSTECH

DR ASSURANCE

DR Assurance Sample Report

An evidence-led view of recovery readiness for two named services, prepared for Northbridge Community Services Ltd, an example organisation.

Document	SAMPLE-DR-001
Version	1.1
Issued	21 August 2026
Classification	Sample report

Document control

Field	Value
Organisation	Northbridge Community Services Ltd
Reference	SAMPLE-DR-001
Evidence cut-off	11 September 2026
Scope	Two named services and stated disruption scenarios
Status	Sample report
Distribution	Unrestricted

Contents

The report moves from the executive outcome through service conclusions and findings to a prioritised action plan.

1. Executive assurance outcome
2. Purpose, scope and boundaries
3. Service conclusions
4. Cross-service observations
5. Findings and priorities
6. Prioritised action plan
7. Limitations and next evidence

1. Executive assurance outcome

OVERALL OUTCOME — LIMITED CONFIDENCE

Northbridge has credible component-level recovery arrangements and useful technical records, but the available evidence does not yet show that either assessed service can be recovered from invocation to business acceptance within its stated objective. Identity, external DNS, supplier coordination and representative validation remain material constraints.

Service	Scenario	Outcome	Reason in brief
SVC-01 Member portal	Loss of Azure UK South	Limited confidence	A repeatable deployment and database recovery route exists, but UK West data, secrets, DNS and service acceptance have not been exercised together.
SVC-02 Case management	Loss of primary hosting and office connectivity	Insufficient basis	The supplier carries the principal recovery duty, but no current execution evidence or complete client access route was supplied.

What leadership should decide

Decision	Reason	Owner and timing
Treat the case-management evidence and network-access gap before further reliance on the eight-hour target.	The service conclusion has an insufficient evidence basis and the client retains access and acceptance duties.	Service Delivery Director — begin now
Complete the portal recovery design for data, identity, secrets, certificates and DNS.	The current exercise proved only part of the service chain.	Cloud Platform Lead — within 60 days
Plan a client-operated portal recovery exercise after the design and runbook changes.	Current uncertainty is best resolved by controlled service execution and business acceptance.	Operations Director — target November 2026

2. Purpose, scope and boundaries

The engagement was commissioned to support a decision about reliance on the member portal and case-management service after the stated disruptions. It was a focused service review based on existing records, interviews and read-only technical evidence.

Scope item	Agreed position
Services	SVC-01 Member portal and SVC-02 Case management
Shared foundations	Identity and privileged access; recovery network and DNS
Scenarios	Azure regional loss; loss of supplier service combined with loss of ordinary office connectivity
Evidence cut-off	11 September 2026
Activities	Structured intake, five interviews, document and configuration review, prior exercise review, factual review and technical readout
Optional exercise	Not commissioned in the initial review
Explicit exclusions	Payroll and collaboration service conclusions; supplier internal cloud controls; cyber forensics; live restore or failover

Boundary

- The review is not an audit, certification, penetration test or guarantee.
- Cygnus did not operate a restore, failover, authentication test or production change.
- Supplier responsibility was considered, but supplier controls were not independently examined.
- The conclusions apply only to the named services, scenarios and evidence available by the cut-off.
- Material change can invalidate evidence regardless of age.

Proportionate scope

Northbridge is an organisation of about 380 staff. Staff count did not determine the work. Scope was driven by two essential services, distinct recovery routes, a hybrid identity boundary, a managed network provider, a SaaS supplier and recent portal change.

3. Service conclusions

SVC-01 — Member portal

LIMITED CONFIDENCE

Northbridge has a credible route to redeploy the portal and recover its Azure SQL data. The February simulation started the application in an isolated environment, but DNS, certificates, secrets, member authentication, the UK West database route and business acceptance were supplied or excluded. The four-hour RTO and 30-minute RPO are not yet supported for the service as a whole.

Field	Assessment
What is supported	Controlled deployment definitions, current protection records and a timed isolated application start.
Material dependencies	Entra ID, Key Vault, certificates, Azure SQL recovery, external DNS and network path.
Principal limitations	The latest exercise pre-dates material portal change and ended at technical health rather than member transaction acceptance.
Next evidence	Client-operated recovery in the stated region-loss scenario, including data, secrets, DNS and representative member acceptance.
Finding links	FND-01, FND-02 and FND-04

SVC-02 — Case management

INSUFFICIENT BASIS

The supplier contract states an eight-hour recovery objective, but no current supplier exercise or incident record was supplied. Northbridge has not demonstrated the alternate network path, privileged access or a representative user’s ability to retrieve and update a case after the combined scenario. A positive service conclusion cannot be supported.

Field	Assessment
What is supported	Named ownership, supplier contact and a documented normal access route.
Material dependencies	Supplier recovery, Entra ID, managed network change, user devices and service-owner acceptance.
Principal limitations	Supplier assertion is not corroborated; the client access and acceptance route is not exercised.
Next evidence	Supplier execution evidence and a controlled client access and representative case-validation exercise.
Finding links	FND-03 and FND-04

4. Cross-service observations

Area	Observation	Why it matters	Services
Service objectives	Owners and minimum service are defined, but the recovery-time end points need correction.	Targets cannot be tested consistently until the start, finish and acceptance points are agreed.	Both
Backup and data recovery	Portal data protection appears credible, but recovery in the alternate region has not been shown. Supplier data recovery is supported only by a statement.	Protected data must still be recoverable in the conditions set by the scenario.	Both
Identity and privileged access	Emergency access has been checked, but hybrid identity recovery and service-team access have not been exercised with either service.	A restored application remains unusable if recovery staff or users cannot authenticate.	Both
Network and DNS	Routes and provider duties are recorded, but timings and combined execution remain unproven.	Connectivity and name resolution are required before users can reach the recovered service.	Both
Supplier recovery	Responsibility is clear, while current execution evidence and client coordination remain weak.	The client retains invocation, access, communication and acceptance duties.	SVC-02
Procedures and exercises	The portal procedure omits several service dependencies; case-management invocation is incomplete. The earlier portal simulation covered only part of the service.	Incomplete procedures and partial exercises leave material uncertainty during an incident.	Both

Systemic theme

Recovery ownership is organised by platform and supplier. Business acceptance, shared identity, managed network change and external name resolution sit between those owners. This creates a credible risk that individual technical steps succeed while the service remains unusable.

KEY OBSERVATION

For Northbridge, the useful portal deployment evidence does not resolve the missing evidence for data, identity, DNS and business acceptance.

5. Findings and priorities

ID	Class	Finding	Impact	Timing	Services	Required outcome
FND-01	Control weakness	Portal recovery does not cover the complete service chain	Major	Near-term	SVC-01	Extend the recovery design and runbook to data, identity, secrets, certificates, DNS and business acceptance.
FND-02	Evidence gap	Portal RTO and RPO are not measured to usable service	Major	Near-term	SVC-01	Define measurement points and capture recovery point and acceptance evidence in the next exercise.
FND-03	Evidence gap	Case-management supplier recovery is unsupported by current execution evidence	Severe	Immediate	SVC-02	Obtain suitable supplier evidence and establish an interim client access and communication plan.
FND-04	Control weakness	Shared identity and network recovery are not exercised with the services	Major	Near-term	Both	Agree the minimum shared-foundation route and include it in controlled service exercises.

Finding detail — FND-03

Element	Assessment
Condition	The contract extract and supplier statement describe an eight-hour objective, but no exercise, incident, independent assurance or current recovery record was supplied. The client's alternate access and case-validation route is also untested.
Expected outcome	Supplier and retained client duties form a complete, evidenced route from invocation to representative user acceptance.
Consequence	Northbridge may be unable to recover or validate the essential case-management service within the stated tolerance and may not know when or how to escalate.
Required outcome	Obtain proportionate supplier recovery evidence, agree invocation and communication, validate alternate client access and run a representative case check.
Closure evidence	Supplier evidence accepted after review; documented client procedure; timed access and case-update validation; retained limitations stated.
Impact and timing	Severe / Immediate. Establish an interim access, contact and decision route while stronger evidence is obtained.

6. Prioritised action plan

When	Outcome	Owner	Evidence for review
Now	Agree the case-management supplier escalation, alternate access and acceptance route; obtain current supplier evidence.	Service Delivery Director	Approved procedure, contacts, supplier evidence and client validation record
Within 30 days	Define consistent RTO and RPO start, end and data points for both services.	Operations Director and service owners	Approved definitions and acceptance criteria
Within 60 days	Complete the portal recovery design and runbook for UK West, data, identity, secrets, certificates and DNS.	Cloud Platform Lead	Controlled design, runbook and walkthrough record
Within 90 days	Exercise the shared identity and network route with the member portal in a client-operated, controlled scenario.	IT Manager and Cloud Platform Lead	Signed authority, event log, timings, deviations, data and business validation
After treatment	Reassess FND-01 to FND-04 and the affected service conclusions.	Independent reviewer	Closure evidence matched to each original condition

What is optional

- Cygnus can help design and witness a client-operated exercise under a separate authority schedule.
- Runbook and recovery-architecture improvement can be scoped separately; later validation will disclose and manage the resulting independence risk.
- Hands-on restore or failover operation is a separate engineering engagement with access, change, rollback, competence, insurance and safety controls.
- A reassessment updates only the findings and conclusions supported by new evidence.

7. Limitations and next evidence

Limitation	Effect on conclusion	Next evidence
No current service-level recovery execution	Substantial confidence is unavailable and the portal conclusion remains Limited.	Controlled service exercise after recovery design correction.
Supplier controls not independently examined	The case-management conclusion relies on weak supplier evidence and remains Insufficient basis.	Current supplier execution or suitable independent assurance plus client validation.
Identity and network tested separately	Shared-foundation readiness cannot be inferred for either service.	Integrated access, name-resolution and administration evidence.
Recent portal and supplier change	Older evidence may not represent the current service chain.	Post-change evidence or a reasoned, reviewed equivalence record.
Payroll and collaboration excluded	No conclusion is made for those services.	Separate scope if a decision is required.

Interpreting the conclusions

The conclusion labels are specific to the named service, disruption scenario, scope and evidence date. They are not a general rating of the organisation and should not be compared with another organisation as a score or benchmark.