Backup & Recovery

Initial Evidence Pack

PARTICIPANT MATERIAL / RELEASE AT 00:40

ROUND	INITIAL ITEMS	REQUESTS	WORK TIME
01 of 03	B-01 to B-04	Maximum 3	35 minutes

Purpose

This module tests whether MW180's broad backup claim is supported by evidence of control design, consistent operation and recoverability within business requirements.

Do not assume that a green backup job is a successful recovery

Use only B-01 to B-04 for your initial assessment. Then formulate up to three focused evidence requests. The facilitator will release matching follow-up material.

The claim under assessment

01	BACKUP & RECOVERY **“Backups for all business-critical systems are performed regularly and can be restored within business requirements.”**

Initial evidence inventory

ID	DOCUMENT	PRIMARY USE
B-01	NIS-2 self-assessment response	Claim, scope and management rationale
B-02	Backup and Recovery Policy extract	Control design, responsibilities and required evidence
B-03	System Recovery Register extract	Business-critical scope and RPO/RTO targets
B-04	Backup Operations Summary - July 2026	Recent job execution and alert information

All organisations, products, people, identifiers and records in this pack are synthetic. Document formatting is part of the exercise context, not proof of authenticity.

DOCUMENT	OWNER / ORIGIN	DATE	STATUS
B-01	Head of IT / NIS-2 workstream	03 Aug 2026	Management reviewed

NIS-2 readiness questionnaire - response extract

FIELD	RECORDED RESPONSE
Question ID	BC-04 - Backup management and recovery
Question	Are backups for all business-critical systems performed regularly and recoverable within business requirements?
Answer	YES
Scope recorded	All systems classified Recovery Class 1 in the System Recovery Register
Response owner	Head of IT
Management reviewer	CFO
Next review	January 2027 or after a major system change

Recorded rationale

Management statement

The managed backup service covers all relevant servers. The provider dashboard is reviewed and was mostly green in July. An annual restore test was completed in April 2026, so recovery capability is considered confirmed.

Evidence cited by the response owner

- Backup and Recovery Policy, version 2.3
- System Recovery Register, version 1.4
- Managed backup dashboard / July 2026 summary
- Restore verification record dated 10 April 2026

Assessor note

A questionnaire response is the claim to be tested. Management review increases its relevance, but it does not make the underlying statement true.

Synthetic record ID: MW180-N2-SA-2026-07 / export page 14 of 31.

DOCUMENT	OWNER / ORIGIN	DATE	STATUS
B-02	Head of IT	Effective 15 Jan 2026	Approved • v2.3

Backup and Recovery Policy - relevant extract

1. Purpose

MW180 shall maintain protected copies and recovery procedures that allow systems and information to be restored after loss, corruption, ransomware, technical failure or operational error. Backup schedules and recovery arrangements shall reflect approved business recovery objectives.

2. Scope and classification

- The policy applies to services listed in the System Recovery Register and to the infrastructure required to recover them.
- Recovery Class 1 (RC1) identifies business-critical services. Recovery Class 2 (RC2) identifies important supporting services.
- The register shall name a business owner, Recovery Point Objective (RPO), Recovery Time Objective (RTO), protection method and validation responsibility for each service.

3. Protection requirements

1. Backup frequency shall be sufficient to meet the approved RPO for each in-scope service.
2. RC1 services shall retain at least 35 daily recovery points and 12 monthly recovery points unless an approved exception states otherwise.
3. At least one current recovery copy shall be isolated from production administrator credentials and protected against unauthorised alteration or deletion.
4. Backup scope shall include the data, configurations, application dependencies and recovery secrets required to return the service to operation.
5. Backup configuration changes shall be approved, recorded and checked against the System Recovery Register.

4. Roles and accountability

ROLE	ACCOUNTABILITY
Head of IT	Policy owner; ensures recovery arrangements and evidence exist for every RC1 service.
IT Operations	Maintains configurations, reviews alerts, resolves failures and retains records.
Managed service provider	Operates agreed monitoring and technical backup activities under the service schedule.
Business service owner	Approves RPO/RTO and validates that a restored service supports the required business process.
Application vendor	Provides specialist recovery support where separately contracted; it does not replace MW180 accountability.

DOCUMENT	OWNER / ORIGIN	DATE	STATUS
B-02	Head of IT	Effective 15 Jan 2026	Approved • v2.3

5. Monitoring and failure handling

- Automated backup alerts shall be generated continuously. A human review shall occur every calendar day for RC1 services.
- A failure that causes, or could cause, an RPO breach shall be escalated to the Head of IT and service owner within four hours of detection.
- A catch-up backup or documented workaround shall be initiated on the same day. Closure requires confirmation of a new valid recovery point and an assigned corrective action where recurrence is possible.

6. Recovery validation

- Each RC1 service shall undergo an end-to-end recovery test at least once every 12 months and after a material platform or application change.
- A test shall use a representative recovery point, measure actual RPO and RTO performance, include required secrets and dependencies, and obtain technical and business-owner validation.
- A failed or incomplete RC1 test shall generate tracked corrective actions and a repeat test within 30 calendar days.
- A file-level restore may verify a backup mechanism, but it does not replace an end-to-end service recovery test.

7. Required records

RECORD	MINIMUM CONTENT
Job evidence	Service/job mapping, schedule, result, protected recovery point, failures and resolution.
Recovery test	Scope, recovery point, start/end time, result, RPO/RTO comparison, failures, validation and sign-off.
Exception	Requirement affected, risk, compensating measure, owner approval, expiry and review date.
Quarterly review	Coverage, trends, overdue failures/tests, open corrective actions and management decision.

8. Exceptions and review

Exceptions require documented risk acceptance by the relevant business owner and Head of IT, must have an expiry date, and shall be reported in the next quarterly review. This policy is reviewed annually or following a material recovery failure.

Approval record: CFO approved 10 Jan 2026. Review due 15 Jan 2027. This is the complete extract relevant to the exercise.

DOCUMENT	OWNER / ORIGIN	DATE	STATUS
B-03	IT Operations / business owners	20 Jan 2026	Approved • v1.4

System Recovery Register - scope and targets

SERVICE	CLASS	BUSINESS OWNER	RPO	RTO
MW-ERP production	RC1	COO	4 h	8 h
Identity services (AD-01 / AD-02)	RC1	Head of IT	24 h	8 h
CAD/PDM service	RC1	Head of Engineering	8 h	24 h
Departmental file service	RC2	CFO	24 h	48 h
Microsoft 365	RC2	Head of Sales	24 h	24 h

Required protection and validation

SERVICE	EXPECTED PROTECTION	RECOVERY VALIDATION
MW-ERP	Nightly application-aware backup plus transaction-log protection sufficient for 4 h RPO	End-to-end isolated recovery; Production Planning validates orders and schedules
Identity services	Daily system-state protection of both domain controllers	Authoritative recovery procedure and authentication test
CAD/PDM	Four-hourly database and file-vault protection	Restore database, vault sample and engineering change record
File service	Daily backup	Representative file and folder restore
Microsoft 365	Daily protected copy of licensed users and selected sites	Mailbox and SharePoint item restore

Scope rule for this round

The words 'all business-critical systems' mean all three RC1 services in this approved register: MW-ERP, identity services and CAD/PDM.

All target rows were approved by the named business owner on 20 Jan 2026. No active exception is recorded in this register extract.

DOCUMENT	OWNER / ORIGIN	DATE	STATUS
B-04	Managed service provider	01-31 Jul 2026	Monthly export

Backup Operations Summary - July 2026

ACTIVE JOB	SCHEDULE	SUCCESS	FAILED / WARN	MAX POINT AGE	STATUS
ERP-FULL	Daily 23:00	30	0 / 1	24 h 13 m	Green
ID-STATE	Daily / 2 DCs	62	0 / 0	23 h 48 m	Green
CAD-INCR	Every 4 h	182	4 / 0	19 h 12 m	Amber
FILE-DAILY	Daily 21:00	31	0 / 0	23 h 05 m	Green
M365-DAILY	Daily 02:00	31	0 / 0	23 h 55 m	Green

Provider summary

Monthly service note

Overall job completion was 98.7%. No unrecovered failed job remained open at month end. The CAD/PDM repository capacity incident was resolved and the service returned to green.

Report conventions

- Only active jobs are included in this summary.
- Success means the backup application completed the configured job without a terminal error.
- Max point age is the oldest age of the newest available recovery point during the reporting period.
- Green/Amber status uses thresholds configured in the backup platform. It is not automatically calculated from the MW180 System Recovery Register.
- This report does not include recovery-test results.

Synthetic provider report ID: NMI-MW180-BKP-2026-07. Values are rounded to the nearest minute.

Round 01 worksheet - initial evidence

Complete this page before receiving follow-up evidence. Cite the evidence ID and the exact field, clause or record.

GROUP	LEAD	ANALYST	CHALLENGER	RECORDER / SPEAKER

1. Rewrite the exact claim and scope in your own words

2. Map the initial evidence

ID	WHAT DOES IT SHOW?	LAYER	LIMIT / CONTRADICTION / QUESTION
B-01			
B-02			
B-03			
B-04			

3. Initial layer assessment

LAYER	STATUS: D / P / N / C	RATIONALE AND EVIDENCE REFERENCE
Design		
Operation		
Effectiveness		

D = Demonstrated • P = Partially demonstrated • N = Not demonstrated • C = Cannot be determined

Ask for evidence that could change your judgement

Maximum three requests. Make each request specific enough that another person could retrieve the right record.

Evidence request 1
Evidence request 2
Evidence request 3

After follow-up evidence is released

LAYER	REVISED STATUS	DECISIVE EVIDENCE AND RATIONALE
Design		
Operation		
Effectiveness		

Finding: state the condition, scope, decisive evidence and consequence
Improvement action: owner, deadline and evidence of completion
One-sentence management message