Azure & Entra ID Assessment

Belrive Services

01 September 2026 - 05 September 2026

Prepared by Vulnotes Security Consulting

Version 1.0.0

CONFIDENTIAL

1. Document control

Version	Issued	Author	Review
1.0.0	2026-09-17	Julien Perrin	Sophie Roux / 16 September 2026

Authorized distribution

Restricted distribution. Intended roles: Nora Petit, cloud operations lead; Julien Perrin, assessment author; Sophie Roux, quality reviewer.

This report describes observations within the agreed scope and assessment period. Subsequent changes may affect its conclusions. Distribution is restricted to authorized recipients.

Revision history

Version 1.0.0 issued 2026-09-16. Initial assessment period 1-5 September 2026; editorial review completed 16 September 2026. No remediation retest has yet taken place.

Table of Contents

2. Executive assessment

Conclusion

3 findings affect belrive-demo tenant / business-apps subscription: 1 High, 2 Medium, 0 Low. The assessment reviewed the agreed configuration and application records against the approved service baseline. Correction priorities reflect the impact, required access and dependencies documented in each finding.

01

Priority actions

Assign F-1 to Nora Petit, cloud operations lead for correction by 30 September 2026. Address F-2 and F-3 by 16 October 2026, then perform the documented acceptance checks before closure.

02

Verified strengths

Named administrative accounts and documented resource ownership were present for all six sampled resources.

3. Assessment analysis

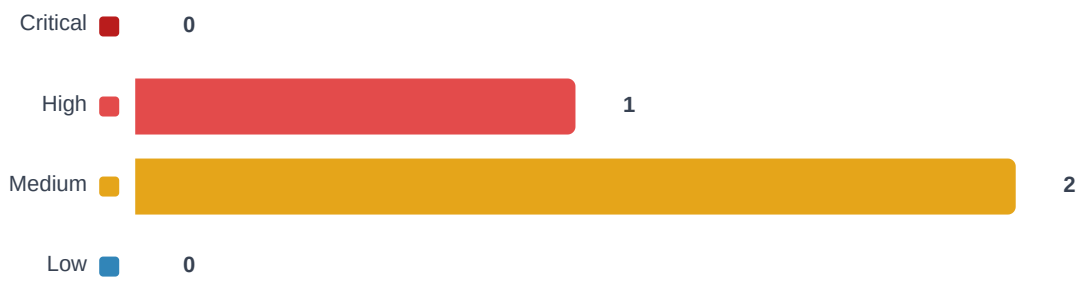
The assessment of belrive-demo tenant / business-apps subscription identified 3 findings: 0 Critical, 1 High, 2 Medium, 0 Low. One staging tenant, one subscription, eighteen sampled identities and six application resources. Read-only configuration evidence; authentication disruption and production changes excluded.

The principal improvement concerns standing privileged assignments lack an expiry. Compromise or misuse of an assigned identity could retain broad administrative impact without a fresh approval decision. Correction ownership rests with Nora Petit, cloud operations lead. The priority is to reduce this exposure without interrupting the service's required business functions.

The remaining observations concern central audit retention falls below the approved requirement and application credentials have no documented rotation owner. They require separate acceptance criteria because changing one policy does not establish that the other controls operate effectively. Review effective runtime behavior as well as the saved configuration.

Named administrative accounts and documented resource ownership were present for all six sampled resources. These controls provide a basis for remediation, but their presence does not compensate for the documented exceptions. The action plan separates implementation evidence from successful retest results.

Risk distribution



4. Scope and conditions

The following register defines the assessed assets, access conditions and accountable owners.

Tenant / subscription	Resource boundary	Access supplied	Accountable team
belrive-demo tenant / business-apps subscription	Identity governance and application landing zone	Read-only tenant and subscription evidence	Nora Petit, cloud operations lead

Detailed scope register

One staging tenant, one subscription, eighteen sampled identities and six application resources. Read-only configuration evidence; authentication disruption and production changes excluded.

Exclusions and restrictions

Only the supplied staging assets and evidence are in scope. Production changes, disruption, social engineering and third-party systems are excluded. Sampling does not establish complete coverage.

5. Assessment coverage

Record the method, reference version, observation date and supporting evidence for each assessed area. A reference mapping does not constitute certification.

Assessment area	Status	Evidence / reference
Identity lifecycle and privileged roles	Gap observed	E-01: privileged assignments
Conditional access governance	Not tested	Conditional access not assessed
Enterprise applications and consent	Gap observed	E-03: application credentials
Resource exposure and segmentation	Not tested	Resource exposure not assessed
Secrets and key management	Gap observed	E-03: rotation ownership
Logging and response ownership	Gap observed	E-02: central retention

Allowed statuses: Verified, Gap observed, Not tested, Not applicable. Justify exclusions and not-applicable decisions.

Coverage rationale

Configuration and documentary evidence were reviewed from 1 to 5 September 2026. Each observation is linked to E-01, E-02 or E-03. Areas without evidence remain Not tested; a successful sampled check does not imply coverage of the entire environment.

Reference: engagement baseline DEMO-2026-09, revision 1.0, approved for this engagement.

6. Environment context

Assessed environment

belrive-demo tenant / business-apps subscription. Identity governance and application landing zone. Service ownership: Nora Petit, cloud operations lead. The evidence bundle is frozen at assessment close; later changes are outside this issue.

Evidence requirements

Record the tenant and resource identifiers, observation date, effective configuration and inherited policy. Separate configured settings from controls actually verified.

Evidence register

E-01: E-01: redacted role-assignment register dated 3 September 2026; four permanent assignments among eighteen sampled identities.

E-02: E-02: retention configuration and approved logging baseline, documentary comparison dated 4 September 2026.

E-03: E-03: two redacted application-registration records and ownership register, reviewed 5 September 2026. Secret values were not collected.

7. Findings register

Findings use the report order. Keep the same reference in the action plan and retest record.

F-1 Standing privileged assignments lack an expiry

FINDING F-1	High / Not applicable

F-2 Central audit retention falls below the approved requirement

FINDING F-2	Medium / Not applicable

F-3 Application credentials have no documented rotation owner

FINDING F-3	Medium / Not applicable

8. Standing privileged assignments lack an expiry

FINDING F-1	High / Not applicable

Observation and affected context

Four administrative assignments in the reviewed identity register are permanent and have no recorded periodic approval. The internal baseline requires time-bounded privileged access.

Technical analysis

Permanent active role membership keeps administrative authorization available without a new activation decision. Entra directory roles and Azure resource RBAC are distinct permission planes; the review register must identify the role, scope and assignment type before choosing a control. An eligible assignment with constrained activation is not equivalent to permanent active access.

Affected scope and limits

Four assignments are identified in the eighteen-identity sample. The register does not prove identity compromise or that every assignment has tenant-wide scope. Emergency-access accounts and workload identities require separate treatment rather than automatic conversion to an interactive approval flow.

Impact

Compromise or misuse of an assigned identity could retain broad administrative impact without a fresh approval decision.

- Administrative exposure: unnecessary standing access lengthens the period during which identity misuse could affect the resources authorized by each role.
- Governance: without an owner and recurring justification, accumulated permissions may survive a change of duties. The High rating reflects administrative authority, not an asserted tenant takeover.

Correction

Review each assignment, remove unnecessary privilege and adopt time-bounded activation with recorded approval and periodic access review.

1. Reconcile each assignment with its owner, business task, permission plane and effective scope. Remove obsolete assignments and narrow retained scope.
2. Where supported and licensed, use PIM eligibility with bounded activation, authentication requirements and approval appropriate to the role. Record the rationale for exceptions.
3. Set review dates and expiry conditions; monitor activation and assignment changes. Preserve tested emergency access with independent oversight.

Accountable owner: Nora Petit, cloud operations lead. Preserve release and rollback evidence before requesting closure.

9. Supporting evidence

F-1 / Standing privileged assignments lack an expiry

evidence record

E-01: redacted role-assignment register dated 3 September 2026; four permanent assignments among eighteen sampled identities.

E-01 / AZURE ENTRA

Reviewed item	Scope	Recorded state
Population	18 sampled identities	4 permanent administrative assignments
Control gap	Approval / expiry register	No recorded periodic approval

Evidence register / Review window: 01-05 September 2026

E-01 - Reviewed record extract, September 2026.

Acceptance criterion

Each retained privileged assignment has an accountable owner, justified scope and approved activation or expiry policy.

Closure evidence to collect

1. Review the four corrected assignment records for owner, scope, eligibility or expiry, and approved exception where applicable.
2. Validate one planned administrative task under the chosen activation policy and confirm access ends as intended.
3. Retain approval and activation audit events; confirm emergency-access arrangements remain usable under the approved procedure.

Retest status: pending. These are planned validation requirements, not successful test results. Record the corrected version, review date, owner and residual exceptions before closure.

CVSS: not applicable. This is a control-assurance or hardening observation without an independently characterized exploit path. Its contextual risk rating remains applicable.

References

Engagement baseline DEMO-2026-09, revision 1.0; evidence E-01.

Microsoft Entra - Privileged Identity Management

10. Central audit retention falls below the approved requirement

FINDING F-2	Medium / Not applicable

Observation and affected context

The reviewed audit destination retains records for thirty days, while the service baseline requires ninety days. No additional destination was evidenced.

Technical analysis

The destination policy permits only thirty days of retention against a ninety-day internal requirement. Source emission, diagnostic routing, table-level retention and archive retrieval are separate controls. Increasing a workspace default alone may not correct an explicit table override or recover events already deleted.

Affected scope and limits

No second destination was evidenced in the supplied records. This is not proof that no archive exists elsewhere; such an archive would need ownership, coverage and retrieval evidence. The ninety-day requirement is engagement-specific, not presented as a universal Microsoft default or legal mandate.

Impact

Older events may be unavailable during a delayed incident investigation.

- Investigation: an incident discovered after the retained interval may lack the identity and administrative timeline needed for reliable reconstruction.
- Assurance: the organization cannot demonstrate its approved evidence-retention window. The gap affects historical visibility; it does not by itself prove logging stopped or an alert was missed.

Correction

Set retention to the approved period, confirm all required sources are routed to the destination and verify historical retrieval.

1. Map required identity and resource audit sources to destination tables, including source-specific export settings and retention overrides.
2. Configure analytics and total retention to meet the approved requirement; document retrieval latency and cost where archive tiers are used.
3. Add ingestion-health monitoring and protect retention changes with change approval. Record the date from which the full ninety-day window can actually be available.

Accountable owner: Nora Petit, cloud operations lead. Preserve release and rollback evidence before requesting closure.

11. Supporting evidence

F-2 / Central audit retention falls below the approved requirement

evidence record

E-02: retention configuration and approved logging baseline, documentary comparison dated 4 September 2026.

E-02 / AZURE ENTRA

Reviewed item	Scope	Recorded state
Configured retention	Central audit destination	30 days
Required retention	DEMO-2026-09 baseline	90 days
Alternative archive	Supplied evidence set	Not evidenced

Evidence register / Review window: 01-05 September 2026

E-02 - Reviewed record extract, September 2026.

Acceptance criterion

Verify ninety-day retention and complete source coverage; schedule a later historical-retrieval check.

Closure evidence to collect

1. Export the effective per-table retention settings and confirm each required source reaches the intended destination.
2. Retrieve a known recent administrative event with original timestamp, actor and resource identifiers.
3. Schedule a historical retrieval check after sufficient time has elapsed. Do not close the historical-evidence gap solely because a new setting is saved.

Retest status: pending. These are planned validation requirements, not successful test results. Record the corrected version, review date, owner and residual exceptions before closure.

CVSS: not applicable. This is a control-assurance or hardening observation without an independently characterized exploit path. Its contextual risk rating remains applicable.

Retention baseline

```
auditPolicy:
  retentionDays: 90
  changeApprovalRequired: true
  ingestionHealthAlert: enabled
```

References

Engagement baseline DEMO-2026-09, revision 1.0; evidence E-02.

Microsoft Azure Monitor - data retention

12. Application credentials have no documented rotation owner

FINDING F-3	Medium / Not applicable

Observation and affected context

Two service identities have long-lived application credentials without a named rotation owner or recorded replacement procedure.

Technical analysis

The credential lifecycle is not tied to an accountable service owner. App registration credentials, their deployment into consumers and service-principal permissions must be tracked together. An expiry date alone does not establish a workable rotation process if the consuming jobs, deployment locations and rollback sequence are unknown.

Affected scope and limits

The review covers two application identities and collected metadata only. No credential value was retrieved, and neither credential theft nor use outside its intended application is asserted. Actual permission scope must be reviewed before estimating the full business impact.

Impact

Credential replacement may be delayed, increasing exposure after a suspected disclosure and risking unplanned service interruption.

- Confidentiality and integrity: a disclosed credential may remain usable longer when nobody owns coordinated replacement.
- Availability: unplanned expiry or an incomplete cutover can interrupt dependent services. The finding concerns lifecycle assurance, not proof of an exposed secret or excessive API permissions.

Correction

Assign ownership, document replacement and rollback, reduce credential lifetime where supported and monitor approaching expiry.

1. Assign primary and backup owners; inventory consumers, credential identifiers, expiry dates and the permissions needed for the workload.
2. Prefer managed identity or workload identity federation when the hosting and trust model support it. For retained credentials, define short justified lifetimes and monitored expiry alerts.
3. Document staged replacement, consumer deployment, validation and retirement of the previous credential. Keep secret values in the approved store and out of tickets or report evidence.

Accountable owner: Nora Petit, cloud operations lead. Preserve release and rollback evidence before requesting closure.

13. Supporting evidence

F-3 / Application credentials have no documented rotation owner

evidence record

E-03: two redacted application-registration records and ownership register, reviewed 5 September 2026. Secret values were not collected.

E-03 / AZURE ENTRA

Reviewed item	Scope	Recorded state
Sample	2 service identities	Long-lived application credentials
Missing controls	Ownership register	No rotation owner or replacement procedure

Evidence register / Review window: 01-05 September 2026

E-03 - Reviewed record extract, September 2026.

Acceptance criterion

Each credential has an owner, expiry alert and tested replacement procedure using non-production credentials.

Closure evidence to collect

1. Use non-production credentials to validate the replacement procedure with every registered consumer.
2. Confirm expected service health during the cutover and verify the retired credential is no longer configured for use.
3. Record ownership, alert delivery, deployment version and cleanup confirmation using credential identifiers only.

Retest status: pending. These are planned validation requirements, not successful test results. Record the corrected version, review date, owner and residual exceptions before closure.

CVSS: not applicable. This is a control-assurance or hardening observation without an independently characterized exploit path. Its contextual risk rating remains applicable.

References

Engagement baseline DEMO-2026-09, revision 1.0; evidence E-03.

Microsoft identity platform - application security practices

14. Remediation and retest

Finding	Owner / target	Status	Acceptance evidence
F-1 to F-3	Nora Petit, cloud operations lead / 30 Sep-16 Oct 2026	Open; retest pending	Finding-specific acceptance checks in the action plan

Action plan

F-1: Nora Petit, cloud operations lead. Target 30 September 2026. Each retained privileged assignment has an accountable owner, justified scope and approved activation or expiry policy.

F-2: Nora Petit, cloud operations lead. Target 16 October 2026. Verify ninety-day retention and complete source coverage; schedule a later historical-retrieval check.

F-3: Nora Petit, cloud operations lead. Target 16 October 2026. Each credential has an owner, expiry alert and tested replacement procedure using non-production credentials.

Retest record

Not retested as of 16 September 2026. Proposed retest window: 19-20 October 2026, subject to delivery evidence. All three findings remain Open; no correction or risk acceptance is asserted.

15. Rating and limitations

Rating method

Technical vulnerabilities use CVSS v3.1. Each scored finding includes its vector and prerequisites. Business priority also considers exposure and service dependencies. Control-assurance and governance observations are rated contextually and marked Not applicable for CVSS. CVSS is owned by FIRST and used by permission.

Residual uncertainty

Conclusions apply to the recorded configuration versions and assessment window. Untested areas are listed in the coverage register. Changes after evidence collection require revalidation. All findings remain open until the documented acceptance evidence has been reviewed.

Technical severity and remediation priority may differ. Document the reason when exposure, business context or correction dependencies change the order of work.