



EXECUTIVE SUMMARY

Cloud Configuration Security Assessment

Exclusively prepared for:

Example Credit Union

October 2026 | Prepared by Rivial Data Security

SECURED

Executive Summary

Rivial Data Security (“Rivial”) assessed the security posture of Example Credit Union's (“Example CU”) Microsoft 365 tenant and Azure subscriptions. Rivial assessed the configuration of security controls to determine their effectiveness in mitigating common threats posed to cloud environments.

Of 499 individual security controls assessed, Example CU has implemented 155 effectively. Of the 220 noted as gaps, twenty-seven (27) of those are rated Critical due to the potential risk and exposure posed by the lack of control being implemented effectively to mitigate the threat.

Rivial identified the most significant control gaps in three areas:

- **Identity and sign-in:** multifactor authentication is not required for all users, and 370 of 469 internal user accounts have not registered a multifactor method.
- **Privileged access:** twelve (12) accounts hold the Global Administrator role, against a recommended maximum of four (4).
- **Backup and recovery:** most storage accounts and key vaults lack deletion safeguards, so a single administrative action could permanently remove data and its backups.

Results at a Glance



Current Strengths

- Soft delete is on for all 6 Recovery Services vaults, so deleted backup items can be recovered.
- Microsoft Authenticator is set to resist MFA fatigue attacks, and system-preferred multifactor authentication is on for all users.
- SMTP AUTH is turned off, and Exchange Online and SharePoint require modern authentication.

What an Attacker Could Do Today

Sign in with a stolen password

None of the eleven (11) enabled Conditional Access policies requires multifactor authentication for every user, 370 of 469 internal user accounts have not registered a multifactor method, and 24 of 30 shared mailboxes accept direct sign-in. For those accounts a phished or reused password is enough: it signs in on its own, or it lets whoever holds it register their own method and take the account over.

Take over the tenant through an administrator account

Twelve (12) accounts hold Global Administrator, the role that controls the whole tenant: eleven (11) as standing assignments, two (2) of them on disabled accounts, and one (1) eligible through Privileged Identity Management (PIM). Rival recommends two (2) to four (4) Global Administrators to minimize the attack surface. Making the remaining access eligible through PIM, so it is granted only when requested and for a set time, lowers the risk, but a better approach is to decrease the risk by using narrowly scoped roles, which limits what an attacker can do with any one compromised account. Twenty (20) administrative accounts sync from on-premises Active Directory, so a compromised local domain carries into Microsoft 365 and Azure. 10 of the 24 accounts that hold a Microsoft 365 administrator role are licensed for a mailbox, so they receive email like any everyday account. Phishing arrives by email, so one successful phishing message to one of these accounts can hand an attacker administrator access.

Destroy data and backups with no way back

17 of 21 storage accounts have soft delete turned off, 3 of 6 Recovery Services vaults are not immutable, and 4 of 5 key vaults have no purge protection. A ransomware operator holding an administrator account, or a mistaken bulk delete, removes that data and its backups outright.

Key Findings

#	Priority	Finding	Fix
1	CRITICAL	370 of 469 internal user accounts have not registered a multifactor method: 207 staff mailboxes, 118 accounts with no licensed mailbox and 45 shared or resource mailboxes nobody signs in to directly.	Turn on the MFA registration policy for staff, block sign-in on shared and unused room accounts, and confirm each account with no licensed mailbox.
2	CRITICAL	SMS and voice are off in the authentication methods policy, but the legacy MFA settings still allow them, and 30 users rely on a phone as their default MFA method.	Move those users to a phishing-resistant method first, then turn off SMS and voice call everywhere they are still allowed.
3	CRITICAL	21 accounts still use legacy per-user MFA instead of Conditional Access.	Once a Conditional Access policy requires MFA for all users, turn off per-user MFA for these accounts.
4	CRITICAL	20 administrative accounts are synchronized from on-premises Active Directory.	Give each administrator a separate cloud-only account for the role, then remove the role from the synced account.
5	CRITICAL	12 accounts hold Global Administrator: 11 standing and 1 eligible through PIM. The standard is two to four.	Keep two to four Global Administrators, remove the role from the two disabled accounts, and move the rest to narrowly scoped roles.
6	CRITICAL	10 of 24 accounts holding a Microsoft 365 administrator role are licensed for a mailbox and collaboration apps.	Give each administrator an admin-only account with no mailbox, and move the roles off everyday accounts.

Next Steps

When	Action	Result
Readout meeting	Assign an owner and a target date to each Critical finding.	Every Critical finding has an owner
Within 30 days of the readout	Return a management response for each recommendation in the Management Response table below.	Each decision is on record for the board and examiner
Within 30 days	Close the 27 Critical findings: MFA for all users, MFA registration, administrator accounts, shared mailbox sign-in, and delete protection on storage accounts, backup vaults and key vaults.	Score rises from 42.5% to about 49.9%
Within 90 days	Close the 87 High findings in tracker order.	Score rises to about 71.7%

Projected scores are estimates that assume every finding of that priority is closed. # is the finding's number in the Remediation Tracker.

Scope and Method

Rival collected the settings with read-only access provided by Example CU, and an analyst reviewed every finding against the evidence. Ratings follow NIST SP 800-30, and the methodology is available on request.

Management Response

Each recommendation below needs a management decision: implement it, with an owner and a target date, or accept the risk and record the reason. Where a recommendation depends on information only Example CU holds, the row states what Rival is asking for, how the answer affects the finding, and where the related list sits in the Remediation Tracker. Rival applies responses before the final report. Where a response narrows a control to the resources or accounts you designate, the finding is re-scored on those alone; exposure is measured against that smaller set, so the priority can move up or down. A response is optional; a finding without one keeps the status shown here.

#	Priority	Control and Finding	Recommendation	Management Response
6	CRITICAL	Administrative accounts carry licenses without mailbox and collaboration applications. Found: 10 of 24 accounts holding a Microsoft 365 administrator role are licensed for a mailbox and collaboration apps.	Remove the mailbox and collaboration apps from the licenses of dedicated admin accounts, and move the roles held by everyday accounts to separate admin accounts. Information requested: Which of the 10 accounts are dedicated administrative accounts and which are everyday accounts. The answer decides the fix (a license change or a separate admin account); the finding stays open until each listed account is corrected. Where to find the list: Remediation Tracker, finding #6. The Affected Objects sheet lists all 10 accounts; filter the Position column to 6.	

#	Priority	Control and Finding	Recommendation	Management Response
12	CRITICAL	Users cannot suppress the multifactor prompt by marking a device as trusted. Found: 13 users remain on per-user MFA, so the legacy remember-MFA setting applies to them.	Limit 'Trusted IPs' in the per-user MFA service settings to the credit union's own outbound addresses, and remove any address that is not. Information requested: Which of the Trusted IP addresses belong to the credit union. Addresses you own can stay as documented exceptions. The finding closes only when the remember-MFA setting is turned off or the 13 users move to Conditional Access. Where to find the list: Remediation Tracker, finding #12. The Trusted IP addresses are listed in the What Rival Found column.	
13	CRITICAL	Two emergency access accounts exist, excluded from Conditional Access, with credentials under documented custody and sign-in alerting in place. Found: Two cloud-only accounts hold permanent Global Administrator.	Designate these two accounts as the emergency access accounts and record that designation. Replace user0699 with an account on the examplecu.onmicrosoft.com domain, and exclude both accounts from at least one Conditional Access policy, or cover them with a dedicated policy. Beyond the control, store phishing-resistant credentials (FIDO2) for them securely, alert on every sign-in and test them periodically. Information requested: Whether user1144 and user0699 are the designated emergency access accounts, and how their credentials are held and monitored. Designated accounts excluded from Conditional Access, or covered by a dedicated policy, pass the control; with no designated accounts the finding stays Critical. Where to find the list: Remediation Tracker, finding #13. Both accounts are named in the What Rival Found column.	
20	CRITICAL	Privileged roles are held by accounts used only for administration, not for mail and everyday work. Found: 6 of 16 accounts holding owner-level roles on resource groups, subscriptions or management groups also carry a mailbox license, so they are used for everyday work.	Create separate admin accounts for these people, move the owner-level roles to them, and remove the roles from the everyday accounts. Information requested: Which of the 6 accounts are dedicated administrative accounts that are not used for daily work. Each one confirmed leaves the count, and the finding closes if all 6 are. Where to find the list: Remediation Tracker, finding #20. The Affected Objects sheet lists all 6 accounts; filter the Position column to 20.	

#	Priority	Control and Finding	Recommendation	Management Response
24	CRITICAL	Every secret in the RBAC-managed key vault carries an expiration date and a named rotation owner. Found: 2 of the 2 key vaults assessed did not match the expected state.	Set an expiration date on each of these secrets and rotate each one before it expires. If kv-0003 is meant to hold failover credentials, add them with expiration dates. Information requested: Whether kv-0003 is meant to hold failover credentials, and who owns secret rotation. The answer sets the scope for kv-0003; the finding on the 2 vaults with non-expiring secrets stays Critical until expiry dates are set. Where to find the list: Remediation Tracker, finding #24. The Affected Objects sheet lists the 2 key vaults with non-expiring secrets; filter the Position column to 24. kv-0003 is named in the What Rival Found column.	
44	HIGH	Containers holding business-critical blob data carry a locked immutability policy. Found: None of the 2,844 blob containers has a locked immutability policy.	Apply a locked time-based retention policy to the backup containers, above all stex0012 (Veeam supports immutable Azure Blob targets). Apply tamper-proof retention to the log archives where record-keeping requirements call for it, and classify the 5 unclassified containers. Information requested: Which blob containers hold backups or records that must be retained, including a classification for the 5 unclassified containers. The finding is re-scored on the containers you designate; caches and diagnostics containers drop out. Where to find the list: Remediation Tracker, finding #44. The Affected Objects sheet lists every blob container, with its storage account; filter the Position column to 44.	
52	HIGH	External mail forwarding is blocked, and no mailbox carries an external forwarding rule or address. Found: Automatic forwarding to outside addresses is not turned off in the Default remote domain or in two outbound spam policies.	Turn off 'Allow automatic forwarding' in the 'Default' remote domain, and limit the two outbound spam policies (Forward Account 0562, Forwarding ISE) to the recipients with a documented business need. Information requested: Who needs automatic external forwarding through the two outbound spam policies, and the business reason for each. A documented need is recorded as an accepted risk; the priority stays High until forwarding is off for everyone else in the 'Default' remote domain. Where to find the list: Remediation Tracker, finding #52. The Affected Objects sheet lists the 'Default' remote domain and the two outbound spam policies; filter the Position column to 52.	

#	Priority	Control and Finding	Recommendation	Management Response
53	HIGH	No SQL Database firewall rule starts at 0.0.0.0. Found: 1 of the 1 SQL server firewall rule assessed did not match the expected state.	On sql-0001, set 'Public network access' to 'Disable', or delete the firewall rule AllowAllWindowsAzureIps (shown in the portal as 'Allow Azure services and resources to access this server'). Delete the same rule on sql-0002 as cleanup. Treat both test servers as holding member data unless management records otherwise in its response. Information requested: Whether sql-0001 and sql-0002 hold member data, and whether anything in Azure needs to reach them. The answer is recorded with the finding but does not change the priority, which follows the exposed setting rather than the data behind it. Deleting servers that are no longer needed closes the finding. Where to find the list: Remediation Tracker, finding #53. The Affected Objects sheet lists the firewall rule, with its server; filter the Position column to 53.	
61, 78	HIGH	Every sending domain publishes an SPF record covering all legitimate senders. Found: 1 accepted domain lacks an SPF record: vendor10.example.	Remove any domain that is no longer used from 'Accepted domains'. For a domain that only routes mail through a third-party service, such as an email-signature service, the record sits in that vendor's DNS, so have the vendor publish it. Information requested: Whether the two accepted domains are still in use and, for a domain that routes through the email-signature service, confirmation that the vendor will publish the records. A domain removed from 'Accepted domains' leaves the count; a vendor-owned domain stays open until its SPF and DKIM records exist. Where to find the list: Remediation Tracker, findings #61 and #78. The Affected Objects sheet lists the domains; filter the Position column to 61, then 78.	
66	HIGH	The Strict protection preset is applied to the priority accounts and takes precedence for them. Found: The priority-account list is not readable with the app's Exchange role (Get-User -IsVIP not exposed).	Add every account tagged as a priority account (Microsoft 365 admin center > Users > Priority accounts) to the 'Strict protection' preset security policy, preferably through a group so new priority accounts are covered automatically. If user1328 is the only priority account, management can say so in its response. Information requested: The list of accounts tagged as priority accounts, which Rival's read-only access cannot see. If user1328 is the only one, the control passes; each priority account outside 'Strict protection' keeps the finding open. Where to find the list: Remediation Tracker, finding #66. The current 'Strict protection' recipient is named in the What Rival Found column.	

#	Priority	Control and Finding	Recommendation	Management Response
82	HIGH	Every public IP address has a named owner and a current purpose, reviewed on a schedule. Found: 2 of 10 public IP addresses are allocated and attached to nothing: pip-0002, pip-0003.	Release either of the two unattached public IP addresses that is not held on purpose (for example for DR failover), and review the public IP list on a set schedule with a named owner. Information requested: Whether pip-0002 and pip-0003 are held on purpose (for example for DR failover), and who owns the public IP review. Addresses held on purpose with a named owner and a review schedule satisfy the control. Where to find the list: Remediation Tracker, finding #82. The Affected Objects sheet lists both unattached public IP addresses; filter the Position column to 82.	
101	HIGH	Only extensions on the institution's approved list are installed on the virtual machine. Found: 97 VMs carry 280 extensions, 14 distinct, all Microsoft first-party (no third-party extensions).	Keep an approved extension list and check these 14 against it. Replace the legacy Log Analytics agent (MicrosoftMonitoringAgent) with Azure Monitor Agent on vm-0119 and vm-0029. Remove the VM Access extension (VMAccessAgent) from vm-0090 unless it has a documented purpose. Retire the legacy IaaSAntimalware (vm-0089) and IaaSDiagnostics (vm-0090) extensions where Defender for Endpoint and Azure Monitor Agent already cover them. Information requested: The institution's approved VM extension list, if one exists. Extensions on the list are compliant and the finding narrows to the rest; without an approved list the control cannot pass. Where to find the list: Remediation Tracker, finding #101. The installed extensions are listed, with the VMs that carry the legacy agents, in the What Rival Found column.	
104	HIGH	Keys covered by the institution's hardware-backed custody requirement reside in a Managed HSM pool. Found: No Managed HSM exists in the 6 subscriptions and all 5 key vaults are Standard tier (software-protected keys; none Premium/HSM-backed).	Decide whether any regulation, contract or data classification requires dedicated hardware key storage (FIPS 140-3 Level 3). If one does, move the keys it covers to Managed HSM, or at least to a Premium key vault. If none applies, management can record that basis in its response. Information requested: Whether any regulation, contract or data classification requires dedicated hardware key storage (FIPS 140-3 Level 3). If none applies, the control is recorded as not required and the finding closes. Where to find the list: Remediation Tracker, finding #104. This decision needs no resource list; the row has the full detail.	

#	Priority	Control and Finding	Recommendation	Management Response
110	MEDIUM	A Conditional Access policy blocks sign-ins from outside the countries the institution operates in. Found: None of the 11 enabled Conditional Access policies satisfies this control.	Remove user0878@examplecu.org from the exclusions of the 'Example US Access Policy', and keep user1653@examplecu.onmicrosoft.com excluded only if it is a designated emergency access account. Information requested: Whether user0878 and user1653 need to be excluded from the 'Example US Access Policy', and whether user1653 is an emergency access account. An emergency access exclusion is allowed; with no other exclusion the policy satisfies the control and the finding closes. Where to find the list: Remediation Tracker, finding #110. The policy and both excluded accounts are named in the What Rival Found column.	
138	MEDIUM	SQL auditing records are retained for more than 90 days. Found: 2 of the 2 SQL server auditing settings assessed did not match the expected state.	Turn on 'Auditing' for sql-0001 and sql-0002, with retention of more than 90 days. If they hold only synthetic data, management can record that in its response. Information requested: Whether sql-0001 and sql-0002 hold member data or synthetic test data only. The answer is recorded with the finding; the priority stays Medium until auditing is on with more than 90 days of retention. Where to find the list: Remediation Tracker, finding #138. The Affected Objects sheet lists both SQL servers; filter the Position column to 138.	
139	MEDIUM	External participants cannot give or request control in meetings. Found: 2 of the 7 teams policies assessed did not match the expected state.	Turn off 'External participants can give or request control' in the IT Meeting and PM Meeting policies, unless IT and Project Management have a documented need such as vendor support sessions, in which case record it as an accepted risk. Information requested: Whether IT and Project Management have a documented need for external participants to take control, such as vendor support sessions. A documented need is recorded as an accepted risk; otherwise the setting is turned off and the finding closes. Where to find the list: Remediation Tracker, finding #139. The Affected Objects sheet lists both meeting policies; filter the Position column to 139.	

#	Priority	Control and Finding	Recommendation	Management Response
165	MEDIUM	Every public group is one the organization approved, with an owner who confirmed the visibility is intended. Found: 33 of 112 Microsoft 365 groups are Public, so anyone in the tenant can see them and their content.	Give each group that should stay public a named owner, and set the rest to 'Private'. Information requested: Which of the 33 public groups should stay public, and who owns each. Groups confirmed as approved with a named owner leave the count, and the finding closes once every remaining public group is approved. Where to find the list: Remediation Tracker, finding #165. The Affected Objects sheet lists all 33 public groups; filter the Position column to 165.	
167	MEDIUM	Storage holding critical data is encrypted with a customer-managed key held in the institution's Key Vault. Found: All 22 storage accounts use Microsoft-managed keys; data is encrypted at rest, but the institution holds no key control.	Decide whether the data protection policy or regulators require keys the credit union controls. If they do, move the accounts holding member or critical data to customer-managed keys in a Key Vault with purge protection. Record the decision either way. Information requested: Whether the data protection policy or a regulator requires customer-managed keys, and which storage accounts hold member or critical data. If no requirement applies, the control is recorded as not required; if one does, the finding is re-scored on the accounts you designate. Where to find the list: Remediation Tracker, finding #167. The Affected Objects sheet lists all 22 storage accounts; filter the Position column to 167.	
174	MEDIUM	Data access policies on the cache are held by named identities and have been reviewed within the agreed interval. Found: Both Azure Managed Redis caches have access keys Disabled, so data access is only through these Entra access policy assignments, all on the default policy.	Review the access policy assignments on both caches on a set schedule and keep a dated record of each review and who performed it. Remove direct data access to the production cache for people who no longer need it, and move callers that only read data to a custom access policy with read permissions only. Management can attach the dated review record in its response. Information requested: The dated record of the most recent review of the access policy assignments on both caches, and who performed it. A review within the agreed interval satisfies the control and closes the finding. Where to find the list: Remediation Tracker, finding #174. The access policy assignments on each cache are listed in the What Rival Found column.	

#	Priority	Control and Finding	Recommendation	Management Response
186	LOW	A read-only lock is applied to storage accounts whose configuration is meant to stay fixed. Found: None of the 22 storage accounts carries a ReadOnly lock, directly or inherited (CanNotDelete only on stex0008 and stex0019).	Add a 'Read-only' lock (ReadOnly) to the accounts that hold backups, logs or other data that should not change, and a 'Delete' lock (CanNotDelete) to accounts that cannot take a Read-only lock. Information requested: Which storage accounts hold backups, logs or other data that should not change. The finding is re-scored on those accounts; the rest drop out. Where to find the list: Remediation Tracker, finding #186. The candidate accounts are named in the What Rival Found column; the full list of 22 storage accounts is on the Affected Objects sheet under Position 167.	
187	LOW	The web app requires incoming client certificates where mutual TLS is part of the intended access model. Found: All 47 App Service apps have incoming client certificates off.	Identify the apps that receive system-to-system or partner API calls. For each, either set 'Client certificate mode' to 'Required' on the app, or turn on 'Negotiate client certificate' on the API Management gateway with a validate-client-certificate policy and restrict the app to traffic from the gateway. Browser-facing apps such as app-0001 do not need client certificates, and management can list them in its response. Information requested: Which apps receive system-to-system or partner API calls, and which are browser-facing. Browser-facing apps drop out of scope, and the finding is re-scored on the API apps. Where to find the list: Remediation Tracker, finding #187. The Affected Objects sheet lists all 47 apps; filter the Position column to 187.	
190	LOW	The web app deployment slot requires incoming client certificates where mutual TLS is part of the access model. Found: All 11 deployment slots have incoming client certificates off, no API Management backend points at any slot, and neither gateway requests client certificates.	Apply the decision made for each app under #187 to its deployment slots as well. Information requested: The same app list as #187, applied to each app's deployment slots. Slots of browser-facing apps drop out of scope. Where to find the list: Remediation Tracker, finding #190. The Affected Objects sheet lists all 11 deployment slots; filter the Position column to 190.	

#	Priority	Control and Finding	Recommendation	Management Response
193	LOW	Critical storage accounts use geo-redundant storage. Found: 18 of 22 storage accounts are locally or zone-redundant only.	Move the accounts holding data that must survive a regional outage to geo-redundant storage ('GRS' or 'GZRS' under 'Redundancy'). stex0008 is on a Premium SKU, which offers no geo-redundant option, so the answer there is a cross-region backup or replication design. Information requested: Which storage accounts hold data that must survive a regional outage. The finding is re-scored on those accounts; the rest drop out. Where to find the list: Remediation Tracker, finding #193. The Affected Objects sheet lists the 18 storage accounts; filter the Position column to 193.	
200	LOW	Mission-critical resources carry a resource lock, with a documented owner and removal process. Found: 45 resource locks exist: 43 on managed disks and 2 on storage accounts (stex0019, stex0008), all CanNotDelete.	Add a 'Delete' lock (CanNotDelete) at minimum to the mission-critical resources in this list, starting with the production and DR backup vaults, the production key vaults, the App Service Environments and the hub network. Information requested: The list of mission-critical resources and who approves lock removal. The finding is re-scored on that list and closes once each resource on it carries a 'Delete' lock. Where to find the list: Remediation Tracker, finding #200. The resources with no lock are listed by type in the What Rival Found column.	
N/A	ADVISORY	The cache is on the Stable update channel, so security updates arrive on the vendor's standard schedule. Found: Not applicable today: maintenance windows for Azure Managed Redis are in preview.	Track Azure Managed Redis scheduled maintenance, now in preview, and once it is generally available define maintenance windows for redis-0001 and redis-0002.	