Alexander Frank · Identity & Endpoint Management

SAMPLE REPORT · FICTITIOUS DATA

Identity Check Microsoft 365 & Entra ID

Who gets to which data, with which account, from which device? Current state, risks and an action plan you can carry out.

4	7	2	16
high findings	medium findings	low findings	checks passed

CLIENT
Musterbau Nord GmbH (fictitious)

ENVIRONMENT
1 tenant · 85 users · Business Premium

DATE
11 Nov 2026 · Version 1.0

This report is a sample. Company, people, figures and findings are made up. Structure, method and level of detail match a real Identity Check. For system integrators, the report can be delivered in their own design and under their own name.

1 · MANAGEMENT SUMMARY

A stolen password is still enough today.

The Microsoft 365 environment of Musterbau Nord GmbH is well licensed but only partly secured. The existing licence (Business Premium with Entra ID P1 and Intune) includes almost everything that is needed. It simply has not been switched on.

9 of 85
accounts without a registered multi-factor method

143
sign-in attempts over legacy protocols in 30 days, from 6 countries

6
Global Administrators; at most 2 to 4 plus break-glass accounts are recommended

The three most important risks in plain words

1. **Invoice fraud through a hijacked mailbox.** Nine accounts can be taken over with a password alone, two of them in accounting. In one accounting mailbox, a rule forwards email to an external address. This is exactly the pattern used for fraud with a changed IBAN.
2. **Attacks are already running, they just aren't noticed yet.** Legacy protocols (IMAP, SMTP authentication) are being used to try out passwords automatically. So far without success, but these protocols bypass multi-factor authentication.
3. **Too many keys to the whole building.** Six people have full administrator rights, two of them use the same account for their daily email. If one of these accounts is taken over, the attacker owns the entire tenant.

What this means for insurance and customers: Cyber insurers regularly ask about multi-factor authentication for all accounts and the protection of administrative access. Customers in the NIS2 space increasingly ask their suppliers for evidence of access protection. In the current state, these questions could not honestly be answered with "yes".

Recommendation

The four high findings can be closed in **about one week**, without additional licences and without disruption for staff. After that comes a Conditional Access baseline that runs in report-only mode first and is enforced once its effects have been reviewed. Chapter 5 shows the plan.

AREA	RATING	SHORT REASON
Sign-in & MFA	critical	Gaps in MFA coverage, legacy protocols open, security defaults switched off without replacement
Privileged accounts	critical	Too many Global Administrators, no separation of daily and admin account, no break-glass account
Lifecycle (joiners/leavers)	critical	Accounts of former employees active and licensed
Guests & applications	needs work	Inactive guests, long-lived app secrets, users may consent to apps themselves
Email security	needs work	DMARC monitoring only, DKIM not active, external forwarding
Devices	needs work	Over a third of Windows devices not in Intune, device state not part of the access decision

2 · SCOPE AND METHOD

Read only, change nothing.

The check was carried out remotely and with read permissions only. No setting in the environment was changed.

Checked

- Microsoft Entra ID: users, groups, roles, authentication methods, Conditional Access, security defaults, guests, app registrations and enterprise applications, consent settings
- Sign-in and audit logs of the last 30 days
- Exchange Online: forwarding, inbox rules, authentication protocols
- Mail domain: SPF, DKIM, DMARC
- Intune: enrolled devices, compliance policies

Not checked

- On-premises Active Directory and servers
- Firewall, network, endpoint protection (EDR) in detail
- Contents of mailboxes and files
- Penetration test or active attacks

These areas can be covered in a follow-up engagement or by the system integrator in charge.

Procedure

STEP	WHAT HAPPENS	DURATION
1 Access	The client creates a time-limited account with the roles *Global Reader* and *Security Reader* (for Exchange: *View-Only Organization Management*). Sign-in with a FIDO2 key only.	15 minutes for the client
2 Automated	Test runs with Maester (open source, test suites based on EIDSCA, CISA SCuBA and CIS) and my own Microsoft Graph PowerShell queries. Results are stored locally and deleted after the project.	½ day
3 Manual	Every deviation assessed in context: Is it intentional? Is there an exception with a reason? Which accounts are really affected? Cross-checked against the sign-in logs.	½ day
4 Report	Findings with risk, evidence and recommendation, action plan with effort, summary for management.	½ day
5 Review	Presentation of the results (60 minutes), questions, decision on next steps. The read-only account is removed afterwards.	1 hour

Rating scale

high	Allows accounts or data to be taken over without any further hurdle. Fix within 1–2 weeks.
medium	Raises the risk considerably or makes an attack harder to detect. Fix within 4–6 weeks.
low	Improvement for operations or auditability. As part of ongoing support.

3 · FINDINGS AT A GLANCE

13 findings, 4 of them urgent.

ID	RISK	FINDING	RECOMMENDATION	EFFORT
F01	high	9 of 85 active accounts without a registered MFA method, 2 of them in accounting. Security defaults are disabled, a Conditional Access policy for MFA is missing.	Require MFA for all users via Conditional Access (CA01), registration campaign with Authenticator or passkey.	0.5 PD
F02	high	Legacy authentication not blocked. 143 failed sign-in attempts over IMAP and SMTP authentication in 30 days, from 6 countries, a typical password spray pattern.	Block legacy authentication via CA (CA02), switch off SMTP AUTH tenant-wide, exception only for one documented scanner.	0.25 PD
F03	high	6 Global Administrators, 2 of them use the same account for email and daily work. No break-glass accounts.	Separate admin accounts, least-privilege roles, phishing-resistant MFA for admins (CA03), 2 break-glass accounts with FIDO2 and monitoring.	0.5 PD
F04	high	3 accounts of former employees are active and licensed; one of them last signed in 11 days ago.	Block immediately, revoke sessions, review sign-ins since departure. Define the leaver process as a checklist or script.	0.25 PD
F05	medium	2 inbox rules forward email to external addresses, one of them from accounting to a private mailbox.	Clarify the rule with the department and remove it, block automatic external forwarding organisation-wide.	0.25 PD
F06	medium	37 guest accounts, 21 of them without a sign-in for more than 180 days.	Remove inactive guests, restrict invitations to roles, quarterly access review for guests.	0.25 PD
F07	medium	4 app registrations with secrets valid for more than 12 months, one of them with the application permission *Mail.ReadWrite* on all mailboxes.	Limit the permission to the mailboxes needed, certificate instead of secret, max. 6 months validity, an owner for each app.	0.5 PD
F08	medium	Users may grant third-party apps access to their data themselves.	Restrict user consent, approval workflow for app requests.	0.25 PD
F09	medium	DMARC is set to *p=none*, DKIM is not enabled for the main domain.	Enable DKIM, evaluate DMARC reports, move step by step to *quarantine* or *reject*.	0.25 PD
F10	medium	31 of 72 Windows devices are not in Intune. Device state is not part of the access decision.	Enrol devices, compliance policy, CA05 in report-only mode first.	2–3 PD
F11	medium	Sign-ins with the device code flow are allowed but not used.	Block the device code flow via CA (CA04).	0.1 PD
F12	low	Self-service password reset is not enabled.	Enable SSPR with the MFA methods already registered.	0.1 PD
F13	low	Sign-in logs are only available for 30 days, no alert on changes to roles.	Export logs (e.g. Log Analytics), alert on role changes.	0.5 PD

PD = person-day. Estimated effort for implementation including testing and documentation.

What exactly was found, and how.

F01 · Accounts without multi-factor authentication

high

A password alone no longer protects an account once it becomes known through phishing or a data leak. Nine active accounts have no second method registered and therefore cannot be required to use one either.

```
# Evidence: registration status of all members (read only)
Connect-MgGraph -Scopes "AuditLog.Read.All","UserAuthenticationMethod.Read.All"
Get-MgReportAuthenticationMethodUserRegistrationDetail -All |
  Where-Object { -not $_.IsMfaRegistered -and $_.UserType -eq "member" } |
  Select-Object UserPrincipalName, MethodsRegistered

# Result (shortened, names pseudonymised)
UserPrincipalName              MethodsRegistered
-----------------              -----------------
accounting.01@musterbau.example    {}
accounting.02@musterbau.example    {}
… 7 more
```

Cause Security defaults were switched off in 2024 to connect a scanner. A replacement policy was never created.

Recommendation Policy CA01 “MFA for all users”, excluding the break-glass accounts, in report-only mode for 7 days first. Before that, a registration campaign using the Microsoft Authenticator onboarding.

F02 · Password spray over legacy protocols

high

The sign-in logs show evenly spread failed attempts against many accounts with a few common passwords. These attempts run over IMAP and SMTP authentication. These protocols cannot ask for multi-factor authentication. If an account has a weak password, it is open this way, even if MFA is registered.

PROTOCOL (CLIENTAPPUSED)	ATTEMPTS	ACCOUNTS	COUNTRIES	SUCCESSFUL
IMAP4	96	41	5	0
Authenticated SMTP	47	22	4	0
Exchange ActiveSync	0	0	0	0

Assessment No account has been taken over so far. The risk is that a single hit is enough, and after 30 days it would no longer be traceable in the logs.

Recommendation Enforce CA02 “Block legacy authentication” immediately (no legitimate use found apart from one scanner, which is moved to an app-specific solution).

F05 · External forwarding from accounting

medium

An inbox rule in the mailbox “accounting.02” forwards every email with “invoice” in the subject to a private address. Whether the employee created the rule herself or an attacker did cannot be told from the configuration alone. Rules like this are exactly what is set up in invoice fraud, to read along and intercept replies.

Recommendation Clarify with the employee, remove the rule, review the account's sign-ins of the last 30 days, reset the password and have MFA registered. Then block automatic external forwarding organisation-wide.

5 · ACTION PLAN

Three steps to a solid baseline.

The plan is cut so that the urgent points are closed first and nobody in operations is locked out. Every policy runs in report-only mode before it is enforced.

Step 1 Week 1	• Block accounts of former employees (F04) • Create break-glass accounts, separate admin accounts (F03) • Block legacy authentication (F02) • Clarify and block external forwarding (F05)	**approx. 1.5 PD**
Step 2 Weeks 2–4	• Conditional Access baseline CA01–CA05 in report-only mode, review, then enforce (F01, F11) • MFA registration for all users, SSPR (F12) • Restrict app consent, replace app secrets (F07, F08) • Enable DKIM, tighten DMARC step by step (F09)	**approx. 3 PD**
Step 3 from month 2	• Enrol devices in Intune, compliance, enforce CA05 (F10) • Quarterly guest review (F06) • Log export and alerts (F13) • Monthly control: new admins, new apps, deviations from the baseline	**2–3 PD** + ongoing

Policies of the Conditional Access baseline

NAME	EFFECT	START
`CA01-MFA-AllUsers`	Multi-factor authentication for all users and applications	report-only 7 days
`CA02-BlockLegacyAuth-AllUsers`	Blocks protocols that cannot do MFA	enforced at once
`CA03-StrongMFA-Admins`	Phishing-resistant sign-in (FIDO2/passkey) for administrator roles	after registration
`CA04-BlockDeviceCode-AllUsers`	Blocks the device code sign-in flow	enforced at once
`CA05-CompliantDevice-Pilot`	Access only from compliant devices, for a pilot group first	report-only

All policies exclude the group `GRP-CA-Exclude-BreakGlass`. Every change is recorded in the change log with date, reason and result.

Implementation: Steps 1 and 2 correspond to the *Identity Baseline* package (fixed price). Step 3 can be done as a project or as part of the ongoing *Managed Identity* service. Everything is documented so that the internal team or the system integrator in charge can run the environment on their own afterwards.

APPENDIX A · CHECK CATALOGUE (EXCERPT)

32 checks, a result for each.

CHECK	RESULT
MFA enforced for all users	✗
Legacy authentication blocked	✗
Phishing-resistant MFA for administrators	✗
Number of Global Administrators ≤ 4	✗
At least 2 break-glass accounts, excluded from CA, monitored	✗
No active accounts of former employees	✗
Automatic external forwarding blocked	✗
Guests: inactive accounts below 10 %	✗
User consent for apps restricted	✗
App secrets valid for ≤ 6 months	partly
DKIM active, DMARC at least quarantine	partly
Device code flow blocked	✗
Devices fully in Intune, compliance in CA	partly

CHECK	RESULT
SSPR enabled	✗
Alert on changes to privileged roles	✗
Security defaults or equivalent CA policies active	✗
Password expiry disabled (NIST/Microsoft recommendation)	✓
Users cannot create tenants	✓
Users cannot create app registrations	✓
Guest access to directory objects restricted	✓
Microsoft Authenticator with number matching	✓
SMS not a method for administrators	✓
Smart lockout active	✓
Named locations maintained	✓
A further 8 checks passed	✓

Appendix B · Terms for management

MFA	Sign-in with a second factor, e.g. a confirmation in an app or a security key. A stolen password is then no longer enough.
Conditional Access	Rules in Microsoft Entra ID that decide at every sign-in: who, from which device, from where, to which application, and whether MFA is also required.
Legacy authentication	Older sign-in methods (e.g. IMAP) that do not support MFA and are therefore popular for attacks.
Break-glass account	Two strictly protected accounts that can still manage the tenant if a policy accidentally locks everyone out.

Prepared by
Alexander Frank · Identity & Endpoint Management
SC-300 · MD-102 · Okta Certified Administrator
alexander-frank.org

Note
Sample with fictitious data. A real report contains the complete list of findings with evidence and is handed over confidentially. For system integrators, on request in their own design and under their own name.