The 10-Minute Cyber Audit: Focus on Identity & Access

Why This Check Protects Your Business

This structured quick audit acts as a **preventive early warning system** for one of the most critical weaknesses in modern IT environments.

In today's cybersecurity landscape, a fundamental shift has taken place:
"Identity is the new perimeter."

What does this mean in practice?

In the past, companies invested heavily in firewalls, intrusion detection systems, and network segmentation.
Cybercriminals, however, have changed their strategy. Instead of attacking infrastructure directly, they now target the weakest link: **human identity**.

Once a login is compromised, even the best firewall becomes ineffective.
An attacker who uses legitimate credentials moves inside your systems **as an authorized user** — often invisible to traditional security controls.

This audit focuses on **five essential control points** that can be checked within minutes to assess your current risk level in identity and access management.

Objective

Within 10 minutes, determine whether your most important access points are unnecessarily exposed to attack.

How to Use This Audit

Check each item carefully.
If you answer **"No" or "Unclear" two times or more**, immediate action is strongly recommended.

Goal (10 Minutes)

Within 10 minutes, check whether your most important accounts are unnecessarily exposed to attack.

How to use this checklist

Tick the box. If you have **2× "No/Unclear" or more**, you should take action urgently.

1) Unique passwords

☐ Yes ☐ No/Unclear
Question: Does every service (email, Microsoft 365/Google, hosting, banking, shop, accounting) have its **own** password?

2) Password manager in use

☐ Yes ☐ No
Question: Do you use a password manager (not browser storage, not Excel/Word, not sticky notes)?

3) MFA enabled for email

☐ Yes ☐ No/Unclear
Question: Is multi-factor authentication (MFA) enabled for your email account (e.g., Microsoft 365/Google/IMAP)?

4) No insecure storage

☐ Yes ☐ No/Unclear
Question: Are passwords **not** stored on paper notes, in files (Word/Excel/Notes), or in the browser?

5) Shared logins identified

☐ Yes ☐ No/Unclear
Question: Do you know if shared accounts exist (e.g., “info@”, “admin”, “shoplogin”) — and where they are used?

☑ Quick Result

- **0–1× No/Unclear:** 🟢 Basic level looks okay
- **2–3× No/Unclear:** 🟡 Increased risk
- **4–5× No/Unclear:** 🔴 High exposure / urgent risk

Key message: Email is the master key. If email is compromised, everything often follows.

🛡 Immediate Actions (if you have at least 1× No/Unclear)

1. Enable MFA for email
2. Introduce a password manager
3. Replace shared logins (or at least document them)

☑ 1. The Uniqueness Principle – Your Shield Against Credential Stuffing

The key question

Does every business-critical service have a truly unique password that is never reused?

Technical background (Deep Dive)

Today, cybercriminals have access to massive databases with billions of leaked credentials from past breaches. Large-scale incidents at platforms such as LinkedIn, Adobe, Yahoo, or Dropbox have provided attackers with huge amounts of email-and-password combinations.

These credentials are not “gone.” They continue to circulate on dark web markets and in criminal forums. Attackers use highly automated tools for so-called **credential stuffing** attacks: bots try leaked combinations at other services — at scale, 24/7, across thousands of targets.

The real risk: the domino effect of password reuse

Imagine this scenario: An employee uses the same password for:

- a personal account at an online shop that gets breached
- the business email account
- VPN access into the company network
- the cloud storage login

Once the online shop is compromised, the attacker may gain far more than an address. They may gain access to your entire digital environment. From there, they can:

- move laterally through systems
- exfiltrate sensitive data
- deploy ransomware
- access customer data

A single reused password can become the entry ticket to your entire business infrastructure.

Practical check criteria

Review systematically:

1. **Written policy:** Is there a clear company rule that explicitly forbids password reuse — especially between private and business accounts?
2. **Understanding:** Have employees been actively informed about the risks of password reuse? Do they understand the impact a private breach can have on business security?

3. **Controls:** Is this covered during onboarding? Are there regular security awareness activities?
4. **Technical enforcement:** Do you use systems that can detect password reuse (some enterprise password managers offer this)?

☑ 2. Professional Password Management – The "Single Source of Truth" for Credentials

The key question

Is there a centrally managed, company-wide password management solution in place (e.g., Bitwarden for Business, 1Password Teams, KeePassXC with a synchronized database)?

Technical background (Deep Dive)

A professional password manager is far more than a digital notebook.

These systems use **strong encryption standards** (typically AES-256) and so-called **zero-knowledge architectures**. This means that even the provider of the password manager cannot read or decrypt your stored data.

In practice, this includes:

- **Secure password generation**
  Password managers create cryptographically strong, random passwords that are extremely difficult to guess or brute-force.
- **Encrypted storage**
  All credentials are encrypted with a master password known only to the user.
- **Auto-fill protection**
  Auto-fill functions reduce phishing risks, as credentials are only filled on the correct, legitimate website.
- **Audit trails (business versions)**
  Enterprise solutions log access and changes, supporting transparency and compliance.

Why common alternatives fail

Excel sheets & Word documents

- No or weak encryption
- Easy to copy and share without control
- No reliable version control
- Immediately readable during ransomware incidents

Browser password storage (Chrome, Firefox, etc.)

- Vulnerable to infostealer malware designed to extract saved browser credentials
- No central control when employees leave
- Often weakly protected (master password optional)
- Compromised if a device is lost or stolen

Post-it notes and notebooks

- Physically unsecured
- Impossible to update centrally
- Accessible to visitors, cleaning staff, or during break-ins

The real business benefit

Scenario: Employee offboarding

Traditionally, a marketing manager leaves the company with access to:

- social media accounts
- advertising platforms (Google Ads, Meta Business)
- design tools
- newsletter systems
- analytics platforms

Without a password manager:
Every password must be changed manually. Teams are informed one by one. Forgotten accounts are common.

With a password manager:
One click removes access to the “Marketing Vault.”

All passwords remain valid for remaining team members.
The former employee is fully excluded.

Additional advantages

- **Secure password sharing:** Temporary access for external partners without revealing passwords
- **Compliance support:** Logs show who accessed which system and when
- **Lower support effort:** Fewer “forgotten password” requests

The risk of “shadow IT”

If companies do not provide a practical, secure solution, employees will create their own:

- Private password managers without company oversight
- Personal Excel files in private cloud accounts
- Reused or weak passwords
- Credential sharing via insecure channels (email, messaging apps)

The principle is simple:
People choose the path of least resistance.
If no secure path exists, an insecure one will be created.

✅ 3. Multi-Factor Authentication – Your Digital “Life Insurance”

The Central Question

Is MFA (Multi-Factor Authentication) — at least via an authenticator app or a hardware token — enabled **and mandatory** for critical systems such as email, cloud storage, VPN access, and administrative accounts?

The Technical Background (Deep Dive)

Multi-factor authentication is based on the security principle:

“Something you know + something you have + something you are.”

- **Factor 1 – Knowledge:** Password, PIN
- **Factor 2 – Possession:** Smartphone with app, hardware key, smart card
- **Factor 3 – Biometrics:** Fingerprint, facial recognition (less common in business environments)

The logic:
Even if an attacker obtains your password via phishing, a keylogger, or a database breach, the attack fails at the second barrier because the attacker does not possess your physical device. This makes MFA one of the most effective single security measures in IT security.

Statistical reality:
According to Microsoft, **99.9% of all automated attacks are stopped by MFA**. Enabling this feature alone can therefore prevent almost all credential-based attacks.

MFA Methods — and Their Security Levels

🔴 *SMS Codes (TAN via SMS) – OUTDATED & INSECURE*

Why you should avoid SMS-based MFA:

- **SIM swapping:** Attackers convince your mobile carrier (via social engineering) to port your number to a new SIM card
- **SS7 vulnerabilities:** The mobile network signaling system has well-known security flaws
- **Phishing susceptibility:** SMS codes can be intercepted via man-in-the-middle attacks
- **No encryption:** SMS messages are transmitted in plain text

Real-world cases:
Numerous high-profile hacks (Twitter employees in 2020, cryptocurrency exchanges) were carried out via SIM swapping.

● *Email Codes – BETTER, BUT NOT OPTIMAL*

- More secure than SMS, but only if the email account itself is protected with strong MFA
- Vulnerable to email account takeovers
- Acceptable for non-critical systems

● *Authenticator Apps – RECOMMENDED*

Examples: Microsoft Authenticator, Google Authenticator, Authy, 2FAS

How they work:

- During setup, a secret key is exchanged between the server and the app
- The app generates a new 6-digit code every 30 seconds (TOTP – Time-based One-Time Password)
- Works offline, no network connection required
- Not vulnerable to SIM swapping

Best practice:
Use apps with cloud backup (Microsoft Authenticator / Authy) in case of device loss, or securely store the backup codes.

● ● *Hardware Security Keys – HIGHEST LEVEL OF SECURITY*

Examples: YubiKey, Titan Security Key, Nitrokey

How they work:

- Physical USB/NFC device that performs cryptographic operations
- Supports the FIDO2 / WebAuthn standard
- **Phishing-resistant:** The key verifies the domain and only works on the legitimate website
- Impossible to compromise remotely

Use case:
Especially recommended for administrators, executives, and access to critical systems.

Email as a Critical Anchor Account

Your email inbox is the **master key** to your digital identity. Why?

Almost every online service offers a “Forgot password” function — and it sends the reset link to... **your email address**.

The attack scenario:

1. An attacker compromises your email account (weak password or missing MFA)
2. They trigger “Forgot password” for:
   a. Your bank (online banking)
   b. Your CRM system (customer data)
   c. Your cloud storage (company data)
   d. Your hosting / domain provider (website control)
   e. Social media accounts (reputational damage)
3. All reset links arrive in the compromised inbox
4. Within minutes, the attacker gains access to dozens of critical systems

Consequence:
Email accounts require the strongest available MFA — **without exception**.

Implementation Roadmap

Phase 1 (Immediate):

- Email accounts of all employees
- Administrative access to all systems
- Cloud storage (Microsoft 365, Google Workspace, Dropbox)

Phase 2 (Within 4 weeks):

- VPN access
- CRM and ERP systems
- Accounting software

Phase 3 (Within 8 weeks):

- All remaining business systems that support MFA

✅ 4. Physical & Digital Shadow Copies – The Forgotten Attack Surface

The Central Question

Are login credentials free from insecure “analog” traces and unencrypted digital copies within your organization?

The Physical Security Walk (Deep Dive)

Cybersecurity starts in the office. Conduct a systematic walk-through:

Office Walk-Through Checklist

1. Workstations:

- Are Post-it notes stuck under keyboards, on the backs of monitors, or inside desk drawers?
- Are notebooks labeled “Passwords,” “Access,” or “Logins” lying openly on desks?
- Are handwritten lists stored in unlocked drawers?

2. Shared Areas:

- Are access codes for doors, alarm systems, or Wi-Fi visibly posted on notice boards?
- Are printouts containing credentials left in printers or next to copiers?
- Are login screens visible when desks are unattended?

3. Reception & Meeting Rooms:

- Can visitors gain unsupervised access to areas where credentials might be visible?
- Are meeting rooms left with passwords written on whiteboards?

Why This Is Critical

- **Cleaning staff:** Often work outside business hours, unsupervised
- **Maintenance technicians:** Have access to offices for repairs
- **Visitors & delivery personnel:** Even short, unsupervised moments are enough
- **Insider threats:** Disgruntled (former) employees
- **Social engineering:** Attackers posing as technicians or cleaning staff

A single photographed Post-it note can grant access to critical systems.

Digital Forensics: Finding Unencrypted Files

Ransomware groups and professional attackers follow a standard playbook.

Phase 1 After Network Compromise:

1. Scanning file servers for specific file names
2. Searching file contents for keywords

Typical Search Terms

File names:

- passwoerter.docx, passwords.xlsx, zugangsdaten.txt
- credentials.pdf, logins.doc, accounts.xls
- admin-access.docx, server-passwords.txt
- backup-codes.xlsx, recovery-keys.doc

Content searches:

- “Username:”, “Password:”, “Benutzername:”, “Passwort:”
- “Login:”, “Access:”, “Credentials:”, “API key:”
- IP addresses combined with credentials
- Server name + “admin”

Your Task

1. File Server Scan:

- Use your file server’s search functionality
- Search for the terms listed above
- Pay special attention to folders such as “IT,” “Administration,” and “Backups”

2. SharePoint / Cloud Storage:

- Apply the same approach in cloud environments
- Review shared links (are password documents publicly accessible?)

3. Email Archives:

- Search mailboxes for phrases like “Here is the password for...”
- Check whether credentials were shared via email — and whether those emails still exist

The Secure Alternative

- **For temporary sharing:** Use services like Bitwarden Send, 1Password Psst!, or Firefox Send alternatives
- **For long-term storage:** Store credentials exclusively in a password manager
- **For documentation:** Use encrypted notes inside the password manager — not separate documents

Red Flags That Should Alarm You

- Files named old_passwords.doc or passwords_backup.xls
- Unencrypted ZIP archives containing password collections
- Screenshots of login screens with visible credentials
- Scanned documents of handwritten password lists
- Word documents with tables full of access data
- Excel sheets with tabs labeled “Logins,” “Access,” or “Accounts”

✅ 5. The Problem of “Shared Accounts” – The Access Management Nightmare

The Central Question

Are all shared login accounts (info@company.com, admin, support, etc.) fully documented, managed via a password manager, and secured with clearly assigned personal responsibilities?

The Technical Background (Deep Dive)

From a security perspective, shared accounts (also known as generic or communal accounts) represent one of the biggest challenges.

What Are Shared Accounts?

Typical examples:

- **Email addresses:** info@, contact@, support@, careers@
- **Administrative accounts:** administrator, admin, root
- **Functional accounts:** marketing, sales, projectteam
- **Service accounts:** backup-user, monitoring, api-service

Why They Are Problematic from a Security Perspective

1. No Traceability (Non-Repudiation):

- If five people use the same login: who did what, and when?
- During security incidents or compliance audits, accountability is impossible
- Forensic investigations are severely hindered

2. Impossible Offboarding:

- Employee A leaves the company under conflict
- They know the passwords for admin, marketing@, and five other shared accounts
- All these passwords must be changed immediately
- Problem: the remaining four colleagues must all be informed
- High probability that accounts will be forgotten

3. Password Quality Degrades:

- Passwords that must be shared verbally tend to be simple (e.g., Marketing2024!)
- Each sharing event increases the risk of leakage
- Passwords are changed less frequently (too much effort, too many people to inform)

4. Uncontrolled Distribution:

- The password for info@company.com is sent via email
- That email is forwarded, printed, or stored in private notes
- After two years, no one knows who still has access

Concrete Risk Scenarios

Scenario 1: The Angry Former Employee

An employee is terminated and feels treated unfairly. They had access to:

- admin access to the website CMS
- the marketing@ email account
- the social_media account in the Facebook Business Manager

Retaliation options:

- Defacing or deleting the website
- Sending compromising emails from marketing@
- Hijacking social media channels or posting reputationally damaging content

Problem:
Changing all passwords immediately is complex, time-consuming, and error-prone.

Scenario 2: The Compliance Nightmare

GDPR data access request:
"Who accessed my personal data, and when?"

With a shared account such as *sales*:

- All 12 sales employees use the same CRM login
- Logs only show *sales* as the user

- Impossible to prove who actually accessed the data
- Potential GDPR violation due to lack of traceability

Scenario 3: Undetected Abuse

A compromised shared-account password:

- An attacker uses the support@ account for months
- Collects customer data from emails
- Activity goes unnoticed because many people use the account
- Unusual login times (e.g., at night) are not recognized as anomalies

The Solution: Personalization and Centralized Management

Strategy 1: Individual Accounts Wherever Possible

Modern cloud platforms and SaaS tools usually support multiple users:

- **Email:** Instead of one marketing@ login, each team member has an individual account, while all access a shared marketing@ inbox (shared mailbox)
- **CMS / Website:** Instead of admin, use individual admin accounts (e.g., max.mustermann@, anna.schmidt@) with role-based access control (RBAC)
- **Social media:** Business Manager tools allow individual access with different permission levels

Benefits:

- Complete audit trails
- Simple offboarding (disable the account — done)
- Personalized security settings (different MFA methods)
- Clear accountability

Strategy 2: If Sharing Is Unavoidable – Use Password Managers with Logging

For cases where true account sharing is required, leverage enterprise password manager features:

1. Access Logs:

- Who accessed which password, and when?
- Automatic alerts for access to critical accounts

2. Granular Permissions:

- User A can use the password but cannot see it
- User B can view and edit it
- User C (admin) has full control

3. Time-Limited Access:

- External service provider gets 48-hour access
- Automatically revoked after expiration

4. Password Rotation:

- Regular automatic password changes
- All authorized users are notified via the password manager
- Old passwords become invalid

Strategy 3: Secure Service Accounts Technically

For technical shared accounts (API keys, backup users, etc.):

- Store secrets exclusively in secret management systems (HashiCorp Vault, AWS Secrets Manager)
- No interactive logins
- Use only by automated systems
- Strict network segmentation
- Intensive monitoring of all access

Best-Practice Documentation

Create a **“Shared Account Register”**:

Account	System	Purpose	Access Granted To	Last Review	MFA Enabled?	Password Vault
admin	WordPress	CMS administration	IT team (5 people)	Jan 2026	Yes	IT vault
info@	Email	Customer inquiries	Support (3 people)	Dec 2025	Yes	Support vault
api_prod	API server	Production system	Servers only	Jan 2026	Key-based	DevOps secrets

Quarterly reviews:

- Are all listed users still with the company?
- Are the accounts still required?
- Are passwords up to date?
- Is MFA working correctly?

🚦 Evaluation & Your Personal Priority Plan

Now honestly assess your situation for each of the 5 checkpoints.

Rating System:

- ✅ **Fulfilled:** Fully implemented and actively practiced
- ⚠️ **Partial:** Measures exist, but gaps remain
- ❌ **Not fulfilled:** Not implemented or barely addressed

Count your ❌ (**Not fulfilled**) items.

Evaluation Matrix

Score	Risk Status	Action Required	Prioritization
0–1 points	🟢 **Stable**	You already have a solid foundation. Focus on continuous	**Recommended actions:**

		improvement and employee awareness.	• Annual security awareness refresher training • Quarterly review of password manager usage • Conduct phishing simulations • Keep documentation up to date • Consider advanced protection (hardware keys) for executives
2–3 points	🟡 **At Risk**	Your organization has significant weaknesses in identity management. A targeted attack would likely succeed. Immediate action is required.	**Immediate actions (4-week plan):** • Week 1: Enforce MFA for all email accounts (no exceptions) • Week 2: Evaluate and procure a password manager solution • Week 3: Roll out the password manager with training • Week 4: Enable MFA for cloud storage and VPN access **In parallel:** Audit all shared accounts and conduct password hygiene training

Final Conclusion: From Reactive Security to Controlled Access

The analysis clearly shows that most security incidents are **not caused by advanced hackers**, but by **everyday structural weaknesses**: reused passwords, missing MFA, undocumented shared accounts, and forgotten shadow copies.

Identity and access management is not a purely technical issue — it is an **organizational discipline**. Companies that take control of identities take control of their risk.

By implementing the measures outlined in these five checkpoints, an organization achieves:

- **Clear accountability** instead of anonymous access
- **Traceability** instead of blind spots
- **Fast, clean offboarding** instead of emergency password resets
- **Measurable risk reduction** with minimal operational overhead

The most important insight:

Security does not require perfection — it requires consistency.

Even partial improvements, such as enforcing MFA for email and moving shared credentials into a password manager, immediately eliminate entire attack classes used by ransomware groups and professional attackers.

This checklist is not a one-time exercise. It should be treated as a **living control framework**, reviewed quarterly and adapted as the organization evolves.

Companies that act now are not just protecting systems —
they are protecting **business continuity, trust, and reputation**.