EFAA for SMEs - Cybersecurity Checklist

A practical, right-sized overview for SME/SMP practices and their clients

Why this matters

Accountancy and advisory practices hold some of their clients' most sensitive information — tax, payroll, financial statements and identity data — which makes them an attractive target for ransomware, invoice and payment fraud, and business email compromise. A single incident can disrupt filing deadlines, breach client confidentiality and damage the trust the practice depends on. Cybersecurity is therefore a business and professional-responsibility issue, not only a technical one, and it increasingly overlaps with GDPR and NIS2 obligations.

This checklist helps you review the key safeguards when planning and performing work, and to discuss basic actions with owners, staff and clients. It is deliberately high-level and scaled to firm size — work through it, not around it.

The six domains covered by this checklist

How to use it

Work through the six domains with the owner or partners and key staff, and tick ☐ each safeguard genuinely in place. The XS / S / M columns show the level expected for very small, small and medium practices:

- ● the safeguard should be in place (and, where relevant, written down).
- ○ a simpler, informal version is acceptable — scale it up as the firm grows.

The ● items are the non-negotiable baseline for every practice, whatever its size. Re-run the checklist at least once a year and after any major change (new system, office move, key hire or departure).

Right-sizing by practice

Practice size	Typical headcount	What "good" looks like
Very small (XS)	Sole practitioner up to ~5 people	Often no in-house IT. Security comes mainly from reputable cloud providers, updated devices, MFA and good habits. Keep policies short and practical.
Small (S)	Around 6–20 people	Name a cyber contact, put the core policies in writing, and formalise backups, access reviews and the basic incident steps.
Medium (M)	Around 20–50+ people, possibly multiple offices	Expect documented controls and policies, periodic review of access, backups and key security settings, evidence that training and core checks have been carried out, and testing where relevant (e.g. restore tests or incident walkthroughs). Consider aligning to a recognised baseline (national essentials scheme / light ISO 27001).

1 Governance and awareness

✓	Safeguard For M, policies should not just exist; they should be reviewed periodically, responsibilities should be clearly assigned, and training completion should be recorded.	XS	S	M
☐	Management treats cyber risk as a business risk (not only an IT issue), and a named person is responsible for basic cybersecurity follow-up.	●	●	●
☐	Staff receive at least annual basic training on phishing, social engineering, and safe use of email, cloud tools and mobile devices.	●	●	●
☐	There is a simple, written policy on acceptable use of email, internet, personal devices and cloud services (including storage of client data).	○	●	●
☐	The firm knows which external IT/cyber expert it would call in the event of a serious incident.	●	●	●

2 Access, identity and passwords

✓	Safeguard For M, access reviews should follow a documented cycle, administrator accounts should be separately controlled, and joiner/mover/leaver changes should be evidenced.	XS	S	M
☐	Unique user accounts are used for all systems holding client or financial data; shared generic logins are avoided.	●	●	●
☐	Strong passwords or passphrases are required (minimum 12 characters), not reused across systems; a password manager is encouraged.	●	●	●
☐	Multi-factor authentication (MFA) is enabled wherever possible (email, cloud accounting, remote access, administrator accounts).	●	●	●
☐	Access follows the “need to know” principle, is reviewed periodically, and ex-employees are removed promptly.	○	●	●

3 Devices, patching and malware protection

✓	Safeguard for M, maintain a basic device/software inventory, track higher-risk patches or vulnerabilities, and be able to show that key updates were applied.	XS	S	M
☐	All laptops, desktops and servers used for professional work run supported operating systems and receive automatic security updates.	●	●	●
☐	Up-to-date anti-virus / anti-malware protection is installed on all endpoints, including mobile devices where feasible.	●	●	●
☐	Local firewalls are enabled, office Wi-Fi is secured, and default router / admin passwords are changed.	●	●	●
☐	Only licensed, trusted software is installed, from official app stores or vendor sites.	●	●	●

European Federation of Accountants and Auditors for SMEs – International Non-Profit Organisation
Rue Jacques de Lalaing 4 | B-1040 Brussels | Enterprise number: 0524.824.834 | Transparency Register Identification Number: 002077217226-17

4 Data protection, cloud and backups

✓	Safeguard for M, cloud/supplier arrangements should be documented and reviewed, retention responsibilities should be clear, and restore testing should be structured and recorded.	XS	S	M
☐	The firm keeps an overview of key information assets (client files, working papers, payroll, tax files, email archives).	●	●	●
☐	Confidential client data is encrypted; laptops and portable media use full-disk encryption.	●	●	●
☐	Use of cloud services is documented, with clarity on who owns the security settings (the shared-responsibility split).	○	●	●

5 Email, phishing and remote work

✓	Safeguard for M, remote access rules should be more tightly governed, BYOD should be limited or subject to conditions, and higher-risk access patterns should be reviewed where feasible.	XS	S	M
☐	Staff are trained to spot suspicious emails, attachments, links and payment-change requests, and know how to report them.	●	●	●
☐	Basic email security controls are in place (spam filtering, attachment scanning, blocking obvious dangerous file types).	●	●	●
☐	Remote access (VPN, remote desktop, cloud portals) uses MFA and is restricted to approved devices.	●	●	●
☐	Rules cover use of personal devices for work (BYOD): minimum security settings and where client data may be stored.	○	●	●

6 Incident response and continuity

✓	Safeguard for M, keep an incident log, record follow-up actions, assign response roles, and run an occasional walkthrough or tabletop test.	XS	S	M
☐	There is a simple, written incident-response checklist (who to inform, how to isolate systems, when to notify clients and authorities).	○	●	●
☐	Critical processes are identified (payroll, VAT returns, statutory reporting, audit fieldwork) with at least a basic continuity plan.	○	●	●
☐	Key contact details (decision-makers, IT support, advisers, insurers) are stored offline and kept up to date.	●	●	●
☐	Significant incidents are reviewed afterwards and lead to concrete follow-up (extra training, process or control improvements).	○	●	●

Quick self-assessment

- All essentials ticked, most others too — a solid foundation; keep it current and tested.
- Essentials mostly in place, some gaps — prioritise the unticked ● items first.
- Several essentials missing — treat as a priority; start with MFA, backups, updates and staff training.

Note *This checklist is a high-level aid and does not replace detailed NIS2/GDPR or national cybersecurity guidance. Tailor it to your firm and your clients.*

European Federation of Accountants and Auditors for SMEs – International Non-Profit Organisation
Rue Jacques de Lalaing 4 | B-1040 Brussels | Enterprise number: 0524.824.834 | Transparency Register Identification Number: 002077217226-17