Security, from every angle.

A practical review of your digital life, business, websites, communities and online tools.

32 checks | 8 areas | One score out of 20

Make the scope explicit.

Reviewer / role _____ Review date _____

People / organisation _____

Accounts, sites and groups in scope

_____

How to score honestly

1 **Inspect, then mark.**

Pass earns the full weight only if every condition is verified across the scope. Gap, partial, unknown and unanswered items earn 0.

2 **Explain what does not apply.**

N/A is only for an absent activity or asset. Record the reason. Outsourced services still apply: request evidence from the provider.

3 **Calculate and prioritise.**

Earned points / applicable points x 20. Critical gaps take priority over the total. Weights and score bands are Vamocles review judgments.

Weights: Critical 5, High 3, Routine 2. The 30/90-day intervals are Vamocles review targets.

Keep this form private. Use evidence references, never passwords, recovery codes or customer records. Fill on screen or print. Totals are manual. This is a baseline self-assessment, not a penetration test, compliance approval or security guarantee.

Identity and access

Protect the accounts that unlock everything else.

Full points only when every pass condition is verified.

Choose one: Pass / Gap / N/A

I1 Do I check and fix weak, reused or leaked passwords?

5 pts — Critical

Pass when Every password in scope is unique and long: aim for 16 or more characters. A trusted password manager or secure alternative stores them. Within 90 days, I used a trusted password-checking tool and replaced weak, reused or leaked passwords promptly.

Verify Record the tool, review date and fixes; start with email and financial accounts. Never record passwords.

☐ Pass ☐ Gap ☐ N/A

I2 Have I enabled multifactor authentication (MFA)?

5 pts — Critical

Pass when MFA is enabled wherever offered, especially email, financial and password-manager accounts. Passkeys or security keys are preferred where supported; an authenticator is an alternative. Unexpected approval prompts are refused.

Verify Inspect security settings and record the method for each important account; never record the secret.

☐ Pass ☐ Gap ☐ N/A

I3 Could I recover my accounts safely?

3 pts — High

Pass when Recovery contacts are current and secured. Recovery codes, where offered, are stored safely away from my phone. Every important account has a recovery route I can use after losing that phone.

Verify Check recovery settings; record only the storage location category, such as a locked offline copy.

☐ Pass ☐ Gap ☐ N/A

I4 Do I review Google sign-in and connected access?

2 pts — Routine

Pass when Within 30 days I reviewed Google, Apple or Microsoft sign-in connections, active sessions and app permissions, removed unwanted access, and checked recovery options for critical linked services.

Verify Inspect provider connections and service sign-in settings. Confirm another supported sign-in before removing a connection.

☐ Pass ☐ Gap ☐ N/A

Evidence / N/A reason _____

Earned _____ Applicable _____ Last checked _____

Know what one account can unlock

A Google-account takeover can put linked services at risk; each service may apply extra checks. A linked-site breach does not automatically expose your Google password. Review dependencies and recovery routes. Change passwords for compromise or reuse, not routine calendar rotation.

Review access monthly; act immediately on compromise.

Sources 1, 10, 11, 12, 13 on p10

Devices and recovery

Keep everyday technology maintained and recoverable.

Full points only when every pass condition is verified.

Choose one: Pass / Gap / N/A

D1 Are my devices supported and updated?

5 pts — Critical

Pass when Phones, computers and important apps still receive security updates. Available security updates are installed; automatic updates are on where supported. Settings were checked within 30 days, with urgent fixes applied promptly.

Verify Inspect update history and support status; list pending fixes and devices nearing end of support.

- [ ] Pass
- [ ] Gap
- [ ] N/A

D2 Can I restore important information?

5 pts — Critical

Pass when Important files have a separate protected backup, with a copy isolated from everyday account or device compromise. A sample restore succeeded within 90 days.

Verify Restore a sample file; record the date, result and backup location category.

- [ ] Pass
- [ ] Gap
- [ ] N/A

D3 Is my information protected if a device is lost?

3 pts — High

Pass when Devices use a strong screen lock, prompt automatic locking and encryption where available. Supported device-finding and remote-lock features are configured; I know how to activate them.

Verify Check lock, encryption and recovery settings on every phone, tablet and computer in scope.

- [ ] Pass
- [ ] Gap
- [ ] N/A

D4 Are my router and smart devices maintained?

2 pts — Routine

Pass when Router, TV, camera and smart-appliance firmware is current and was checked within 30 days. Default admin passwords are changed where configurable. Unsupported devices are disconnected; unnecessary remote administration is disabled.

Verify Inspect firmware and support status; record unsupported devices disconnected and needing replacement.

- [ ] Pass
- [ ] Gap
- [ ] N/A

Evidence / N/A reason _____

Earned _____ Applicable _____ Last checked _____

A copy must be recoverable

Cloud synchronization alone does not prove you have a usable backup. Keep a separate protected copy and test recovery. Inventory routers, cameras, TVs, appliances and other connected gadgets; their support and firmware matter too.

Check updates monthly; test a restore at least quarterly.

Sources 2, 5, 9 on p10

Messages and impersonation

Make verification a habit before trust becomes action.

Full points only when every pass condition is verified.

Choose one: Pass / Gap / N/A

M1 Do I independently verify urgent requests?

Pass when Requests for money, changed bank details, sensitive information or unusual access are checked through a known number or established independent channel, even when the voice or video appears familiar.

Verify Describe the verification route for a recent request or a realistic practice scenario.

3 pts

High

- [ ] Pass
- [ ] Gap
- [ ] N/A

M2 Do I check links before signing in or paying?

Pass when Unexpected message links are treated cautiously. For sign-in, payment or account alerts, I open the known app or saved address independently. A familiar sender or polished message is not sufficient proof.

Verify Demonstrate how you check a harmless example from WhatsApp, Telegram, email or social media.

3 pts

High

- [ ] Pass
- [ ] Gap
- [ ] N/A

M3 Do I control downloads and remote access?

Pass when Unexpected files, apps, QR codes and screen-sharing or remote-control requests are verified before use. Software comes from trusted sources; unwanted remote-access applications are removed.

Verify Review downloads and installed remote-access tools; identify who approved any tools still installed.

2 pts

Routine

- [ ] Pass
- [ ] Gap
- [ ] N/A

M4 Are my messaging settings appropriate?

Pass when Within 30 days I reviewed account verification, linked devices and privacy settings. Unknown linked devices were removed. I check recipients and channel protection before sharing sensitive information.

Verify Inspect linked-device lists, group permissions and the protection offered by the chat type you use.

2 pts

Routine

- [ ] Pass
- [ ] Gap
- [ ] N/A

Evidence / N/A reason _____

Earned _____ Applicable _____ Last checked _____

A familiar voice is not proof

AI can imitate voices, faces and writing. Verify unexpected requests through a known contact route. WhatsApp, Telegram, SMS and social messages deserve the same care. Do not assume every chat or group has end-to-end encryption.

Verify each unusual request; review linked devices monthly.

Sources 2, 4, 7 on p10

Privacy and social exposure

Know what is public, shared, stored and searchable.

Full points only when every pass condition is verified.

Choose one: Pass / Gap / N/A

P1 Have I checked whether my details appear in breaches?

Pass when Within 90 days, I checked my email addresses with a trusted breach-monitoring service and reviewed credible account alerts. Known exposed credentials were replaced promptly, and affected accounts were checked for misuse.

Verify Record the service, review date and actions. Check email addresses, not passwords, in breach searches.

3 pts

High

- [ ] Pass
- [ ] Gap
- [ ] N/A

P2 Have I checked data brokers and public searches?

Pass when Within 90 days I reviewed public searches and relevant people-search or data-broker listings. Unnecessary personal details were removed or removal requests submitted where available; unresolved requests have a follow-up date.

Verify List sites checked, request dates and unresolved listings; include old addresses and contact information.

3 pts

High

- [ ] Pass
- [ ] Gap
- [ ] N/A

P3 Are my social accounts sharing what I intend?

Pass when Within 90 days I reviewed audiences, tagging, contact discovery, location, public profiles and connected apps on each platform. Unnecessary exposure and unused app access were removed.

Verify View profiles while signed out; inspect location settings and third-party app permissions.

2 pts

Routine

- [ ] Pass
- [ ] Gap
- [ ] N/A

P4 Have I reduced unnecessary stored information?

Pass when Unused accounts and old sensitive files were deleted or secured. Shared links are restricted to intended people. Unnecessary access to contacts, photos, location, microphone and camera has been removed.

Verify Review cloud-sharing links, old accounts and device app permissions; record the review date.

2 pts

Routine

- [ ] Pass
- [ ] Gap
- [ ] N/A

Evidence / N/A reason _____

Earned _____ Applicable _____ Last checked _____

Removal needs a recheck

People-search and data-broker listings can reappear. Record where you checked, removal requests and the follow-up date. Search results are not a complete inventory of your data, and a clean search does not prove that no exposure exists.

Review exposure and sharing quarterly; respond to alerts promptly.

Sources 2, 3, 14 on p10

Business operations

Assign ownership to access, continuity and response.

Full points only when every pass condition is verified.

Choose one: Pass / Gap / N/A

B1 Can only the right people access business systems?

Pass when People use individual accounts. Privileged access is limited and protected with MFA where available. Leavers' access is removed promptly. Staff, contractor and service-account permissions were reviewed within 30 days.

Verify Compare staff and contractor records with actual user lists, including cloud systems and supplier access.

5 pts

Critical

- [ ] Pass
- [ ] Gap
- [ ] N/A

B2 Could the business recover from disruption?

Pass when Essential systems and data have owners, protected backups and recovery arrangements. A recovery exercise within 90 days met the business's agreed downtime and data-loss limits; no critical recovery failure remains unresolved.

Verify Record the recovery test, result, responsible owner and any remaining operational gaps.

5 pts

Critical

- [ ] Pass
- [ ] Gap
- [ ] N/A

B3 Are payments and sensitive records controlled?

Pass when Payment-detail changes are independently verified. Significant payments have an approval process appropriate to the business. Customer and staff records are accessible and shared only with authorized people.

Verify Review a sample payment approval and data-sharing workflow; check who can approve and access each.

3 pts

High

- [ ] Pass
- [ ] Gap
- [ ] N/A

B4 Does everyone know how to report an incident?

Pass when A named lead, trusted reporting route and practical response instructions exist. Staff know how to report suspicious activity. Essential supplier contacts are available offline, and a response scenario has been rehearsed.

Verify Ask a team member what they would do; record the exercise date and improvements.

2 pts

Routine

- [ ] Pass
- [ ] Gap
- [ ] N/A

Evidence / N/A reason _____

Earned _____ Applicable _____ Last checked _____

Responsibility follows the service

Include contractors, suppliers, service accounts and outsourced systems. Record who owns each control and who can provide evidence. A supplier's promise or a paid subscription is not, by itself, proof that the control works.

Review access monthly and on staff changes; exercise recovery quarterly.

Sources 2, 5, 9 on p10

Websites and digital services

Verify ownership, maintenance and protection with your provider.

Full points only when every pass condition is verified.

Choose one: Pass / Gap / N/A

W1 Are domain and administrator accounts protected?

5 pts — Critical

Pass when Domain, DNS, hosting, CMS and release access have named owners, individual credentials, limited privileges and MFA where offered. Domain renewal and account recovery details are current. Outsourced controls have provider evidence.

Verify Inspect access lists and registrar settings, or obtain dated evidence from the responsible provider.

☐ Pass ☐ Gap ☐ N/A

W2 Is the site supported and maintained?

5 pts — Critical

Pass when CMS, plugins, frameworks and dependencies are supported and security updates are current. Unused components are removed; no known critical finding remains unresolved. Maintenance was reviewed within 30 days, including provider-managed components.

Verify Request update records, support status and an open-findings list with deadlines from your maintainer.

☐ Pass ☐ Gap ☐ N/A

W3 Are site information and functions protected?

3 pts — High

Pass when HTTPS works correctly; secrets are absent from public code. Forms collect only needed data. A competent reviewer checked access controls and input handling for accounts, forms, uploads and APIs; serious findings are resolved.

Verify Obtain dated review evidence from the developer or provider, including remediation of serious findings.

☐ Pass ☐ Gap ☐ N/A

W4 Could I detect trouble and restore the site?

2 pts — Routine

Pass when Relevant monitoring and logs have an owner. Protected backups were successfully restored within 90 days. The site owner has a working provider escalation route and knows who handles a compromise.

Verify Record the restore result, monitoring owner and verified provider contact; obtain evidence if outsourced.

☐ Pass ☐ Gap ☐ N/A

Evidence / N/A reason _____

Earned _____ Applicable _____ Last checked _____

Outsourced still needs evidence

Ask your developer or hosting provider for evidence against these checks. Missing technical knowledge is a gap to resolve, not N/A. Include the domain, DNS, hosting, CMS, code, integrations and any customer-facing service in scope.

Monitor continuously; review maintenance monthly and recovery quarterly.

Sources 5, 6, 9 on p10

Organizations and groups

Protect shared spaces through clear ownership and membership.

Full points only when every pass condition is verified.

Choose one: Pass / Gap / N/A

G1 Are group owners and administrators accountable?

3 pts

High

Pass when Owners and administrators are named, access is limited and accounts are protected with MFA where available. A backup owner or documented recovery route exists if the main owner leaves.

Verify Review role lists and recovery arrangements, or obtain dated confirmation from the administrator.

- [ ] Pass
- [ ] Gap
- [ ] N/A

G2 Are membership and shared-file permissions current?

3 pts

High

Pass when Within 30 days an administrator reviewed former members, external guests and access to restricted channels or files. Unwanted access was removed; shared information is limited to intended recipients.

Verify Inspect membership and a sample shared link, or request evidence from the responsible administrator.

- [ ] Pass
- [ ] Gap
- [ ] N/A

G3 Are invitations and member information controlled?

2 pts

Routine

Pass when Join and invite settings match the group's purpose. Stale public invite links are revoked where appropriate. Members know what contact or profile information others can see.

Verify Review invite links, join approval and contact visibility with an administrator where necessary.

- [ ] Pass
- [ ] Gap
- [ ] N/A

G4 Can the group respond to impersonation or abuse?

2 pts

Routine

Pass when Members know how to verify official requests and report suspicious activity through a trusted route. Administrators have a practical process for removing harmful access and escalating incidents.

Verify Identify the official contact route and walk through an impersonation scenario with a responsible person.

- [ ] Pass
- [ ] Gap
- [ ] N/A

Evidence / N/A reason _____

Earned _____ Applicable _____ Last checked _____

Members can ask for evidence

Include communities, social pages, professional groups and shared workspaces. If you are a member rather than an administrator, ask the responsible administrator to verify the controls. Lack of administrator access does not automatically make a check N/A.

Review membership monthly and whenever roles change.

Sources 2, 5, 7 on p10

AI tools and online services

Keep data, permissions and consequential actions under control.

Full points only when every pass condition is verified.

Choose one: Pass / Gap / N/A

A1 Do I know which tools can access my information?

Pass when An inventory reviewed within 90 days covers cloud services, browser extensions, integrations and AI tools. Each has a purpose and owner. Unused services and connections have been removed.

Verify Inspect authorized apps, extensions, integrations and service credentials; record ownership without recording secrets.

3 pts

High

- [ ] Pass
- [ ] Gap
- [ ] N/A

A2 Do I check unfamiliar apps before signing in?

Pass when I check the operator, privacy and security information, and requested access before sign-in, including apps built by friends or with AI. Sensitive data is shared only when authorized. Retention, model-training and sharing settings suit the approved use; prohibited data is understood.

Verify Review current accounts and the actual plan; record checks, denied permissions and concerns.

3 pts

High

- [ ] Pass
- [ ] Gap
- [ ] N/A

A3 Are automation permissions limited and reviewed?

Pass when Integrations and AI agents receive only needed access. Credentials are protected. Consequential actions, including payments, publication and deletion, require appropriate human review; untrusted content cannot authorize broader permissions.

Verify Inspect connection scopes, enabled actions and approval settings; revoke unnecessary access.

2 pts

Routine

- [ ] Pass
- [ ] Gap
- [ ] N/A

A4 Do I verify outputs and keep a recovery route?

Pass when Important AI outputs are checked against reliable sources. Each essential service has an owner who can stop automation or revoke access. Export or recovery of essential information has been tested.

Verify Check a consequential output, test an export and identify who can stop the integration.

2 pts

Routine

- [ ] Pass
- [ ] Gap
- [ ] N/A

Evidence / N/A reason _____

Earned _____ Applicable _____ Last checked _____

Settings and purpose matter

A familiar creator or polished design is not proof of security. Check the actual service and plan. Treat messages, documents and websites processed by AI agents as untrusted; they cannot authorize new access or consequential actions.

Check before sign-in; review tools and permissions quarterly.

Sources 2, 5, 8, 11, 12 on p10

Turn findings into protection.

Transfer the eight subtotals. Give each gap an owner and a date.

Review area	Max	Earned	Applicable
01 Identity and access	15		
02 Devices and recovery	15		
03 Messages and impersonation	10		
04 Privacy and social exposure	10		
05 Business operations	15		
06 Websites and digital services	15		
07 Organizations and groups	10		
08 AI tools and online services	10		
Totals	**100**		

Your score

/20

Earned / applicable x 20

Example: 60 / 80 x 20 = 15.0.

Round only the final result to one decimal.

Applicable = 100 minus justified N/A weights. Show this denominator with the score. If it is 0, report "not assessed". Compare reviews only when their scope is the same.

18-20 Strong baseline 14-17.9 Improve 8-13.9 Significant gaps 0-7.9 Urgent

Any Critical gap takes priority, regardless of the score. Critical gaps

Fix first / control ID	Owner	Due

Next review After fixes, repeat the affected checks.

Suspect compromise? Use a trusted device; contact your bank, service or IT lead via a known route.

Reference guidance Checked 29 October 2026; scoring is Vamocles-designed.

1. NIST: Authentication and recovery
2. CISA: Four security habits
3. FTC: People-search opt-outs
4. FTC: AI voice impersonation
5. NCSC: Small organisations guide
6. OWASP: Top 10 web risks, 2025
7. Telegram: Encryption and chats
8. NCSC: The risks of shadow AI
9. NCSC: Backing up personal data
10. CISA: Strong passwords
11. Google: Review linked services
12. Google: Shared sign-in and data
13. Google: Password Checkup
14. Have I Been Pwned: Breach checks