



ASCENDEA

AI / BUSINESS GROWTH / PROMPT PACK

Online Business Cybersecurity — 45 AI-Assisted Planning Prompts

A UK-focused, beginner-friendly AI prompt workbook that helps small-business owners and managers document practical account, website, payment, privacy, phishing, incident-response and review actions without presenting AI output as a security or compliance guarantee.



Author: Rob Arnold

ascendea.ai

ASCENDEA EDITION · OCTOBER 2026 · v1.0

Free Ascendea resource

Your route through this resource

Before you use an AI assistant	3
A simple rollout sequence.....	4
1. Account security and password management	4
2. Website, checkout and payment security	7
3. Customer data, privacy and cloud storage	9
4. Phishing and social-engineering defence	12
5. Fraud, refunds and ecommerce operations.....	14
6. Budget-conscious tools and service choices	17
7. Incident response and business continuity	19
8. Team training and security culture	21
9. Monitoring, supplier management and review	23
Keep the work usable	26
Publication and use notice.....	26
References and current guidance	26

Chapter links and PDF bookmarks support navigation. Writing areas are for handwritten or separate notes, not interactive PDF forms.

Author: Rob Arnold · Ascendea · Edition v1.0 · October 2026

<https://ascendea.ai/>

Educational guidance; not a guarantee of business results or legal, tax or personalised financial advice. This is a non-exclusive licensed-content adaptation. For your own learning and permitted end use only; no resale, redistribution, editable-source or private-label rights are granted.

A practical prompt workbook for UK small businesses

Author: Rob Arnold · Ascendea · <https://ascendea.ai/>

Edition v1.0 · October 2026

This workbook helps a UK small business turn a basic security concern into a documented, reviewable set of actions. It is designed for owners and managers who are not security specialists: a trade business sharing job photos, a professional-services firm with a client portal, a retailer taking online orders, or a B2B business using cloud email and accounting software.

It is not a promise that your systems are safe or compliant. Use it to prepare questions, policies and working documents; then check important decisions with your software provider, insurer and an appropriate security, legal or data-protection professional. The NCSC's current small-organisation guidance is a sensible starting point for accounts, devices, backups and scams. 1

Before you use an AI assistant

Do **not** paste passwords, recovery codes, API keys, card numbers, full customer records, private staff information, live security logs or unredacted contracts into a general AI chat. Replace details with labels such as [payment provider], [number of staff] or [sensitive-data type]. Check your AI provider's current data terms and your own data-protection responsibilities before entering any personal or confidential information.

Use this working instruction at the start of every prompt in this workbook:

You are helping a UK small business prepare a **working draft**, not a compliance certificate. Use plain UK English. Do not invent facts, legal requirements, software features, prices, incident details or citations. Ask up to five essential questions where information is missing. Separate **facts supplied**, **assumptions**, **actions**, **owner**, and **open questions**. Do not request passwords, recovery codes, bank details, card data or personal data. Flag when current official provider, ICO, NCSC, payment-provider, insurer or qualified-adviser guidance must be checked by a human.

When the AI replies, use this four-step review:

1. **Compare it with reality.** Check every account, supplier, person and process named in the draft.

2. **Check current sources.** Use the official help page for the actual product; do not follow a generic menu path from an AI response.
3. **Assign a person and date.** A task without an owner and a review date is only a suggestion.
4. **Store the approved version safely.** Keep policies, system lists and incident contacts in a controlled location that the right people can access during an outage.

A simple rollout sequence

Start with the systems that could stop you trading, expose customer information or move money. Do not try to implement all 45 prompts at once.

Suggested stage	Start with	Practical output
Baseline	6, 11, 26	Website/system inventory, data map and priority list
Foundations	1, 2, 3, 9, 10	Account rules, MFA plan, access register and tested backup plan
People and suppliers	16, 18, 19, 20, 36	Simple team guidance, email plan and supplier questions
Response and continuity	14, 31, 32, 33, 34, 35	Incident contacts, first-actions card, communications drafts and rehearsal notes
Ongoing review	42, 44, 45	Monthly check, useful measures and annual improvement plan

This is a suggested order, not a timetable or assurance outcome. Security controls work best as layers: strong account protection, prompt updates, sensible permissions, tested backups, alert staff and a rehearsed response. The NCSC provides a free Cyber Action Toolkit for sole traders and small businesses, as well as guidance for organisations with up to 250 staff. [1](#)

1. Account security and password management

1. Write a usable account and passphrase policy

Gather first: staff/contractor roles, the accounts they use, whether the service supports passkeys or MFA, where recovery information is held, and who approves exceptions.

Prompt:

Create a one-page account and passphrase policy for [business type] with [team size] people. Our key systems are [systems]. Explain, in plain language, how we create unique sign-ins, use a password manager or passkeys where available, enable MFA, keep recovery methods controlled, share no individual passwords, and report a suspected compromise. Include a short “what to do when a person joins, changes role or leaves” section. Do not impose an arbitrary password-change schedule unless a real provider, insurer or risk reason requires it. Mark any requirement that needs checking against a provider or insurer rule. Produce a staff version and an owner/manager version.

Human check: confirm the policy matches every key supplier’s current sign-in and recovery options. Do not assume a password manager or passkey is supported everywhere.

2. Make an MFA rollout plan

Gather first: business email, domain/website administrator, banking and payment accounts, cloud storage, accounting, payroll, social accounts, remote access and password-manager accounts.

Prompt:

Make a beginner-friendly MFA rollout plan for the following accounts: [list]. Rank each as critical, high, standard or low based on money movement, customer data, administrative power and service interruption. For each critical/high account, give numbered steps: identify the account owner; open the provider’s official security guide; choose the strongest method the provider supports; enrol at least one authorised recovery method; record ownership without recording the secret; test sign-in and recovery; and note completion. Include a safe process for a lost phone and a rule that no person approves an unexpected sign-in prompt. Use a table with account, owner, priority, MFA status, recovery custodian, evidence link and next review.

Human check: NCSC guidance explains that MFA methods differ in strength and encourages organisations to choose methods appropriate to the service and risk. 2 Never approve a sign-in or reset prompt you did not initiate.

3. Set up a least-privilege access process

Gather first: roles, systems, current administrators, external bookkeeper/agency/IT support, approver and offboarding contact.

Prompt:

Design a lightweight access-management process for [business]. Apply “least privilege”: people receive only the access needed for their role. Give numbered procedures for (1) requesting access, (2) manager approval, (3) granting access, (4) recording it in an access register, (5) reviewing access quarterly, and (6) removing/changing access when somebody leaves or changes role. Include separate handling for owners, administrators, contractors and agencies. Give a simple access-register table and an urgent offboarding checklist. Include a manual fallback if the usual approver is unavailable.

Human check: name a backup owner. A process that depends on one unavailable director is not resilient.

4. Compare password-management options without a stale ranking

Gather first: staff count, shared-account needs, MFA/passkey requirements, budget range, device types, support needs and whether regulated/client requirements apply.

Prompt:

Create a neutral comparison framework for three business password-management options. Do not name a “top three” or state prices unless I supply current official links. Compare our shortlisted providers on: business administration, individual vaults, controlled sharing, MFA/passkey support, recovery/admin controls, export/offboarding, audit events, supported devices, support, data terms, current price source and known limitations. Our needs are [needs]; shortlisted providers are [names and official URLs]. Give a recommendation only if the evidence supports it; otherwise state the unanswered questions and a small pilot plan using test accounts. Include implementation steps and a rollback plan.

Human check: read the provider’s current security, privacy, support and pricing pages. Do not upload an unencrypted vault export to an AI tool.

5. Run a quarterly account-security audit

Gather first: account inventory and last review date.

Prompt:

Build a quarterly account-security audit checklist for [systems]. Include account owner, active users, administrator count, MFA status, recovery contacts, unused accounts, shared credentials, recent suspicious activity, software/support status and evidence checked. Use a table with “pass / action needed / not applicable”, owner and due date. Add a final section that sorts actions into urgent (money, admin or sensitive-data access), this month, and planned. Keep the wording suitable for a non-technical manager.

Human check: a completed checklist is not proof of safety; investigate “unknown” and “action needed” answers.

2. Website, checkout and payment security

6. Assess your website safely

Gather first: web address, platform, hosting, developer/support contact, plugins/apps, administrator accounts, backup arrangement, contact forms, customer accounts and payment flow.

Prompt:

Create a non-invasive website-security self-assessment for [website], built with [platform] and hosted by [provider]. Do not perform scanning, testing or exploitation. Ask questions about named ownership, admin MFA, updates, supported software, plugins/apps, HTTPS, backups and restore tests, least-privilege access, forms, customer-account controls, payment redirection, logging/support contacts and a plan if the site is unavailable. For each answer, state the evidence to request from our provider or developer. Finish with a short list of questions to send them and a priority action register.

Human check: only a suitably authorised professional should perform intrusive security testing. Make sure your hosting/development agreement explains who applies updates and who responds to a security issue.

7. Evaluate ecommerce platforms on evidence

Gather first: products/services, online order volume band, fulfilment model, customer accounts, integrations, countries served, payment provider and developer capability.

Prompt:

Help us evaluate [platform A], [platform B] and [platform C] for a UK small online business. Use only the official URLs I provide and identify the date accessed. Build a comparison table covering: checkout/payment architecture, what payment data reaches our site, current provider documentation on PCI responsibilities, account/admin controls, MFA availability, update/plugin responsibility, backup/export options, fraud tools, support/escalation, app permissions, privacy/data-location questions and total implementation effort. Do not claim that any platform makes us automatically PCI compliant or UK-GDPR compliant. Recommend a next step, not a guaranteed “most secure” choice, when evidence is incomplete.

Human check: PCI DSS applies to entities involved in payment processing, although the validation required is determined by relevant payment brands/acquirers. Ask your acquirer or payment provider what applies to your actual flow. [6](#)

8. Review payment-gateway choices

Gather first: official documentation links for your shortlisted providers, how customers pay, whether card details touch your systems, currencies, refund process and fraud/chargeback concerns.

Prompt:

Compare [gateway A], [gateway B] and [gateway C] for our payment flow: [describe]. Use only supplied official documentation. Explain in plain English what tokenisation, hosted checkout and fraud screening mean **when the documentation confirms those features**. Identify what remains our responsibility: account security, access control, checkout configuration, refunds, customer communication, evidence retention and following acquirer instructions. List questions for our payment provider about PCI scope, supported authentication, incident contacts and dispute evidence. Do not state that encryption or a hosted checkout removes all PCI duties.

Human check: encryption alone does not automatically take an environment out of PCI DSS scope. [6](#)

9. Make a tested website-backup plan

Gather first: website components, update frequency, where orders/files live, current backup destination, who can restore and acceptable downtime/data-loss expectations.

Prompt:

Write a simple website-backup and restore plan for [website]. Identify what must be copied separately: site files, database, configuration, media, ecommerce/order records, integrations and domain/DNS records where applicable. For each item, give: owner, backup method, frequency, storage location, access protection, retention, restore test method and evidence of the test. Include a numbered restore drill using a safe staging/test environment where possible. Include a rule that backup access is protected and that recovery is not attempted until the device/environment is considered safe. List questions to ask our host if their backup scope is unclear.

Human check: NCSC guidance stresses regular, tested backups, separate/offline or suitably protected copies, and awareness that attackers may target connected backups. [3](#)

10. Check HTTPS and certificate responsibility

Gather first: domain, host/platform, current certificate status, third-party content, developer contact and renewal owner.

Prompt:

Create a beginner checklist for checking HTTPS on [website]. Explain the difference between having a valid certificate and safely maintaining a website, without claiming that HTTPS alone secures the site. Give numbered steps to: identify the certificate/renewal owner; confirm that our official provider documents the current setup; check normal pages, forms and checkout load with HTTPS; ask the developer to investigate browser warnings or mixed-content warnings; record renewal/auto-renewal evidence; and test a renewal/change in a controlled way. Include a short escalation email to the host or developer. Do not give command-line instructions or bypass browser warnings.

Human check: the platform or host may manage certificates, but someone in your business must own the supplier relationship and notice warnings.

3. Customer data, privacy and cloud storage

11. Build a customer-data inventory

Gather first: lead forms, enquiries, ecommerce, bookings, email marketing, CRM, finance, cloud drives, staff devices, suppliers and paper records.

Prompt:

Create a customer-data inventory for [business]. Use a table with: business activity; data categories; whose data; source; purpose; system/location; supplier; access roles; retention/deletion trigger; international-transfer question; security measure; and evidence/owner. Include data from website forms, inboxes, CRM, accounting, booking, payment, marketing and spreadsheets. Do not put live names, email addresses, account numbers or special-category details into the table. Flag unknowns and questions for our privacy lead or adviser. End with the three biggest data-mapping gaps.

Human check: this is an operational map, not a legal determination. Keep it updated as tools and processes change.

12. Screen UK and overseas privacy obligations

Gather first: organisation type, customers/visitors by country, personal-data uses, marketing channels, cookies/analytics, processors and any overseas activity.

Prompt:

Produce a UK-focused privacy and marketing compliance **question list**, not a declaration of compliance, for [business]. Cover UK GDPR accountability, transparency/privacy information, lawful basis, processor contracts, security, retention, individual-right handling, breach procedures, cookies/analytics and PECR electronic marketing. Add a separate “other jurisdictions” screen that asks where people are located and whether local advice is needed; do not present CCPA/CPRA or any overseas law as automatically applicable. For every question, identify an evidence item and who should verify it. Flag matters for an ICO resource or qualified adviser.

Human check: ICO guidance on electronic marketing is under review following changes made by the Data (Use and Access) Act; recheck it before a campaign or policy decision. [5](#)

UK outreach note: ICO guidance distinguishes corporate subscribers from individual subscribers. A company or LLP can generally receive B2B electronic marketing without PECR consent, but the sender must identify itself, offer a valid opt-out route and respect objections; UK GDPR still applies where personal contact data is used. Sole traders and some partnerships are treated as individual subscribers, so consent or the limited soft opt-in may be needed. If the status is unclear, take the more protective route. Direct messages can count as electronic mail. This guidance is under review, so check the current ICO page before sending a campaign. [5](#)

13. Prepare a privacy-notice briefing, not a finished legal policy

Gather first: data inventory, actual purposes, suppliers/processors, retention approach, contact details and current website notices.

Prompt:

Turn this approved data inventory into a plain-English **privacy-notice briefing** for a qualified reviewer: [redacted inventory]. List the facts a notice needs to reflect, including identity/contact details, data categories, purposes, lawful-basis questions, recipients/processors, transfers, retention, rights, complaints route, cookies and changes. Separate confirmed facts from missing facts. Draft only an illustrative reader-friendly structure; do not claim it is legally complete or compliant. Provide a pre-publication fact-check list and identify which statements require legal/privacy sign-off.

Human check: never publish an AI-generated privacy notice unchanged. It must reflect what you actually do, including third-party tools.

14. Prepare a personal-data-breach first-response plan

Gather first: incident contacts, insurers, IT/developer/host contacts, systems holding personal data, communication channels and secure out-of-band contact method.

Prompt:

Create a first-72-hours personal-data-breach response plan for [business]. Give a numbered, beginner-friendly sequence: keep a timed incident log; protect people and contain the issue safely; preserve relevant facts; identify affected data/systems; assess likely impact on people; consult our incident, insurer and specialist contacts; decide whether regulator/individual notification is required; and record the decision and follow-up actions. Include roles, backups if the role-holder is away, an out-of-band contact method, a decision log and “do not do” warnings such as guessing, destroying evidence or sending premature public statements. Do not decide legal notification for us.

Human check: a reportable personal-data breach must be reported to the ICO without undue delay and within 72 hours; not every incident is reportable, but keeping a log and assessing risk are important. The ICO’s guidance is under review, so check the current page at the time. [4](#)

15. Compare cloud-storage arrangements

Gather first: file types, sensitivity, collaborators, external sharing, existing provider, retention needs, recovery needs and official URLs for options.

Prompt:

Create a cloud-storage decision worksheet for [business] and [shortlisted providers]. Use supplied official documentation only. Compare business administration, MFA, sharing controls, access logs where documented, data recovery/versioning, export, offboarding, device access, retention/deletion, support, data-location/transfer questions and contract/privacy documentation. State what we must configure ourselves and what we need to verify with a provider or adviser. Finish with a 10-user pilot, permission-review and exit plan. Do not claim a certification or encryption statement makes a provider suitable for every use.

Human check: test sharing with a non-sensitive file first. Review public links and departed-user access before moving important data.

4. Phishing and social-engineering defence

16. Plan practical phishing awareness

Gather first: team size, normal communication channels, typical suppliers, previous issues, training owner and reporting route.

Prompt:

Design a short phishing-awareness programme for [business]. Make it supportive, not punitive. Include a 20-minute starter session, a simple “pause, check, report” card, a private reporting route, three realistic examples relevant to [industry], and a monthly reinforcement topic. Explain what staff should do with a suspicious email, text, link, attachment, login alert or invoice-change request. Include safe handling instructions: do not reply, click, forward widely or use a telephone number supplied in the message; verify through a known contact route. Add a manager checklist for recording reports and improving controls.

Human check: NCSC offers current phishing guidance and staff-training resources. [1](#)

17. Create five safe social-engineering scenarios

Gather first: customer/supplier interactions, payment approvals, delivery process, recruitment, IT support and senior roles.

Prompt:

Create five **fictional, non-operational** social-engineering training scenarios for a [industry] small business. Cover a fake supplier bank-detail change, fake IT/password reset, urgent customer request, delivery/courier request and senior-person impersonation. For each, provide: story setup; warning signs; a safe verification route; the expected response; who to report to; and a facilitator debrief question. Do not include real names, malicious links, realistic spoof domains, scripts for bypassing controls or instructions that would help someone attack us.

Human check: frame the exercise as learning. Do not publicly name or shame someone who reports or misses a scenario.

18. Improve email security settings and habits

Gather first: email provider, domain host, administrator, current MFA, shared mailboxes, forwarding rules, mobile devices and external IT support.

Prompt:

Make an email-security improvement plan for [email provider]. Start with an inventory of administrator accounts, users, shared mailboxes, external forwarding, aliases, devices and domain/DNS owners. Then give numbered, provider-neutral tasks: enable MFA; review admins and recovery methods; remove leavers; update software; review forwarding/delegation rules; use official provider guidance for spam/phishing protection and domain authentication; and define staff reporting. For each task, state the owner, official documentation to consult, evidence to retain and what to do if we cannot find the setting. Do not invent provider menu names or promise that email filtering catches every scam.

Human check: make changes through an authorised administrator and test normal mail flow after a change.

19. Send suppliers a proportionate security questionnaire

Gather first: service type, data shared, system access, contractual relationship and your most important risks.

Prompt:

Draft a short, plain-English supplier-security questionnaire for a [business] that will share [data/access] with [supplier type]. Include only proportionate questions on contact/escalation route, access controls/MFA, staff access, incident notification, backups/continuity where relevant, sub-processors, return/deletion at contract end, security updates, evidence they can share, and whether they will access payment or personal data. Add “not applicable” and “explain” options. Create a simple scoring note that does not treat a questionnaire response as a security guarantee. Flag where a contract or privacy adviser should review terms.

Human check: a supplier's answer is evidence to investigate, not a substitute for a contract, due diligence or ongoing review.

20. Give staff a phone-scam response guide

Gather first: normal callers, high-risk processes, verification contacts, payment process and escalation owner.

Prompt:

Write a one-page phone-scam guide for staff at [business]. Cover fake bank, IT-support, delivery, supplier, customer and director calls. Give a simple script: “I cannot approve or share that on this call. I will verify through our published/known contact route.” Explain that callers should not share codes, reset links, account details, personal data or payment information; should not install software; and should never call a number provided by an unexpected caller. Include an incident-reporting step and a manager escalation process for suspected payment or account compromise.

Human check: if banking details may be compromised, use a trusted number already held by your business to contact the bank's fraud team. 1

5. Fraud, refunds and ecommerce operations

21. Build a fair suspicious-order review process

Gather first: products/services, normal order pattern, delivery/collection process, payment-provider tools, fraud losses and fulfilment owners.

Prompt:

Create a human-reviewed suspicious-order process for [business]. Identify evidence-based order signals we may check, such as a mismatch with our normal pattern, failed verification from our payment provider, repeated attempts, inconsistent contact/delivery information, or a customer request to bypass our usual process. Do not use protected characteristics or assumptions about a person's identity. Give a numbered review workflow: pause fulfilment where justified; check the payment-provider dashboard; contact the customer through an established channel if appropriate; document the reason and outcome; escalate uncertain/high-value cases; and release, cancel or seek advice under our approved policy. Include a case log and customer-service wording that is neutral and respectful.

Human check: use your payment provider's current fraud/dispute guidance. Do not let an AI automatically decline, fulfil or accuse a customer.

22. Strengthen chargeback prevention and response

Gather first: common dispute reasons, fulfilment proof, refund terms, customer-service process, payment-provider dispute deadlines and owner.

Prompt:

Create a chargeback-prevention and response playbook for [business]. Cover clear descriptors and contact routes, accurate product/service descriptions, order confirmation, delivery/collection evidence, refund handling, customer support, secure payment-provider configuration and a documented response to a dispute. Include a table with event, evidence to retain, owner, provider deadline, customer contact step and decision. Do not promise that any action prevents all chargebacks or that we will win a dispute. Ask for the current payment-provider rules before drafting a deadline.

Human check: retain only necessary evidence and follow your provider's current dispute process.

23. Evaluate customer-authentication choices

Gather first: current checkout, customer account model, fraud concerns, accessibility/customer-support needs and official payment-provider docs.

Prompt:

Prepare a decision brief on customer authentication for [checkout flow]. Explain the difference between account sign-in, payment authentication and order verification without using unexplained jargon. Compare the options offered by our payment provider or platform using only supplied current documentation. For each, list security purpose, customer friction, accessibility/support considerations, operational burden, fallback behaviour and evidence to test. Recommend a small controlled test only where we can measure complaints, abandonment and fraud signals responsibly; do not predict a conversion rate or a fraud reduction.

Human check: payment authentication settings may affect liability, customer experience and regional rules. Confirm the configuration with the provider/acquirer.

24. Review your returns and refund process for abuse risks

Gather first: published terms, order system, refund authorisation levels, return methods, typical exceptions and evidence retained.

Prompt:

Review this returns/refund process for operational and fraud weaknesses: [redacted process]. Produce improvements that remain fair to genuine customers. Cover verified order lookup, payment-method refunding, approval levels, evidence for high-value exceptions, return tracking, duplicate-refund checks, account takeover concerns, staff escalation and clear customer communication. Separate a policy decision from a technical control. Flag consumer-law, contractual or sector issues for qualified review; do not draft unfair terms or make unsupported claims about customer rights.

Human check: publish only terms that are accurate for your products, sales channel and legal context.

25. Check your checkout end to end

Gather first: each checkout step, scripts/apps, forms, payment method, confirmation emails, customer accounts and support contact.

Prompt:

Create a regular checkout review checklist for [website]. Walk through product selection, basket, address/contact collection, account creation, payment hand-off, confirmation and post-order support. Ask what data is collected at each stage, whether it is needed, who can access it, whether the page uses the approved provider integration, what third-party scripts/apps run, how failures appear to staff/customers, and how the process is tested after a change. Include a test-order procedure using permitted test tools or a low-risk test route, plus a rollback/incident contact list. Do not suggest collecting or storing card details ourselves.

Human check: PCI SSC notes that card-not-present and ecommerce channels need to be evaluated and protected; confirm your own payment flow with the provider/acquirer. [6](#)

6. Budget-conscious tools and service choices

26. Prioritise low-cost foundations before new tools

Gather first: current devices, systems, protection already included, budget, skills and biggest risks.

Prompt:

Create a low-cost cyber-security priority plan for [business]. Begin with an inventory and the existing protections included in our email, device, hosting, banking and payment services. Prioritise: account MFA and access cleanup; automatic updates/supported software; backups and restore testing; scam reporting; device screen locks; and documented contacts. For every suggestion, state the risk addressed, owner, setup effort, ongoing maintenance, official source/provider page to check, cost status as “confirm”, and a manual fallback. Do not recommend a product simply because it is free, and do not tell us to disable built-in protection or install multiple conflicting security tools.

Human check: the NCSC Cyber Action Toolkit is a no-cost, small-business starting point; decide on tools only after the basics are understood. [1](#)

27. Decide on security spend without invented ROI

Gather first: proposed control, affected systems, cost, time to maintain, current weakness, consequence if it fails, alternatives and decision owner.

Prompt:

Build a security-investment decision sheet for [control]. Do not calculate or promise a return on investment unless I supply evidence and assumptions. Use columns for: problem/risk; affected asset; plausible consequence; current controls; proposed change; setup cost; recurring cost; staff time; dependencies; residual risk; evidence source; decision owner; and review date. Compare “do nothing”, “improve an existing control”, “buy/contract a service” and “remove/reduce the risky activity” where relevant. State uncertainties clearly and suggest a small pilot or specialist assessment if needed.

Human check: security spending is a risk decision. Avoid treating a single score or percentage as proof that a purchase is justified.

28. Build a staged improvement roadmap

Gather first: priority risks, staffing capacity, budget constraints, dependencies and planned business changes.

Prompt:

Turn our priority register into a staged cyber-security roadmap for [business]. Use three horizons: “now”, “next review” and “later, if justified”, rather than fixed promises. Place foundational controls first, then supplier/process improvements, then specialist services or certification decisions where appropriate. For each item include purpose, owner, dependency, indicative cost status (“confirm”), evidence of completion, review date and manual fallback. Make clear that any dates, prices and results are illustrative planning assumptions until confirmed.

Human check: amend the roadmap after an incident, material system change or supplier change.

29. Choose between DIY and managed support

Gather first: systems, internal skills/time, business hours, budget, data sensitivity, insurer/client requirements and shortlist.

Prompt:

Compare managing [security function] internally with using a managed provider. For each option, describe required skills, time commitment, scope, handover, account ownership, access permissions, reporting, incident escalation, support hours, contract exit, costs to confirm and risks. Then build a supplier-interview checklist: “What exactly do you monitor/manage?”, “What access do you need?”, “How do we contact you during an incident?”, “What is excluded?”, “How can we export our data?”, and “Who owns each account?” Do not assume outsourcing transfers all legal or operational responsibility.

Human check: keep a named internal owner, even when a supplier operates the control.

30. Map your tools without false integration claims

Gather first: email, identity, devices, backups, website, payment, cloud storage, accounting, CRM, IT support and existing alerts/reports.

Prompt:

Create a simple security-tool map for [business systems]. Show each system's owner, administrator, data type, key access control, backup/restore arrangement, supplier support route, alert/report available and connection to another system. Identify duplicated controls, gaps and single points of failure. For proposed integrations, ask for official compatibility documentation and security/privacy implications; do not claim tools integrate or share data unless documented. Finish with a one-page "who to call and where to look" reference for an incident.

Human check: minimise access between systems and review connected apps before approving them.

7. Incident response and business continuity

31. Draft an incident-response plan

Gather first: incident lead/deputy, system owners, IT/host/payment/bank/insurer contacts, secure contact route and critical services.

Prompt:

Draft a practical incident-response plan for [business] that covers account compromise, phishing, website outage, suspected malware/ransomware, lost device, payment concern and personal-data issue. For every incident type, use the same first actions: protect people; record time/facts; contain safely; use trusted contacts; preserve evidence; assess impact; communicate through an approved owner; recover carefully; and record lessons. Include role/deputy, contact register, decision log, escalation to insurer/specialist/authority where appropriate, and a paper/offline copy location. Include "do not pay, erase, reboot or publicise until the right evidence and advice are considered" cautions rather than a rigid universal instruction.

Human check: NCSC recommends incident planning and rehearsing roles/resources. [3](#)

32. Plan minimum viable continuity

Gather first: processes needed to serve customers, critical systems/data, manual workarounds, staff locations, suppliers, recovery order and maximum tolerable interruption set by management.

Prompt:

Create a business-continuity plan for a cyber disruption at [business]. Identify the minimum services we must sustain, such as taking urgent calls, checking appointments, fulfilling safe orders or updating customers. For each service, list system dependency, data dependency, owner/deputy, manual fallback, customer communication, priority to restore and decision to pause work. Include a start-of-incident checklist and a recovery checklist. Mark every time estimate as an internal planning assumption, not a recovery guarantee, and include a step to test the manual fallback.

Human check: keep the continuity plan separate from everyday systems so it is still available when email or cloud storage is not.

33. Prepare a ransomware response card

Gather first: critical data, backup owner, IT support, insurer, legal/privacy contact, devices/network setup and offline contacts.

Prompt:

Make a one-page ransomware response card for [business], suitable for a non-technical manager. Give immediate steps: stop using the affected device/system where safe; contact the named IT/incident lead through a known route; record what is seen and when; protect backup access; do not connect unknown media or attempt unapproved fixes; and use insurer/specialist/law-enforcement guidance. Then provide sections for containment, fact finding, personal-data assessment, communications, recovery from known-good backups, evidence log and lessons learned. Explain that any decision about a ransom needs specialist, insurer and legal consideration; do not promise recovery or recommend payment.

Human check: NCSC says law enforcement do not encourage, endorse or condone ransom payment and there is no guarantee of restored access if a ransom is paid. [3](#)

34. Prepare honest communications drafts

Gather first: approved spokesperson, customer/employee/supplier channels, facts known, facts unknown, service impact and review contacts.

Prompt:

Draft adaptable, fact-led communication templates for [business] covering: service disruption; suspected account compromise; confirmed personal-data incident after legal/privacy review; and recovery update. Each template must state only confirmed facts, what we are doing now, what the recipient should do if anything, a genuine contact route and when we will update. Use placeholders for facts, dates and approvals. Add a sign-off checklist that prohibits speculation, blame, minimising, legal conclusions or promises of safety. State that notification decisions must follow the actual circumstances and current official advice.

Human check: keep a version history. Do not use a customer template before the incident lead and relevant adviser have reviewed it.

35. Rehearse three tabletop exercises

Gather first: participants, systems, likely risks, 45–60 minutes, facilitator and note-taker.

Prompt:

Design three beginner-friendly tabletop exercises for [business]: (1) a director's email account is compromised, (2) the website/booking system is unavailable, and (3) a supplier reports a possible data issue. For each, give a fictional opening scenario, timed injects, participant roles, decisions to make, safe answer prompts, evidence to find, observer notes and a debrief/action log. Do not simulate a real attack or ask participants to open suspicious files. Include facilitator instructions to stop the exercise if real incident evidence appears.

Human check: focus on whether people know who decides and how they communicate, not on scoring individuals.

8. Team training and security culture

36. Build a short security-awareness curriculum

Gather first: roles, devices, remote/hybrid working, key systems, training time, known risks and reporting contact.

Prompt:

Create a six-part, plain-English security-awareness curriculum for [business]: accounts/MFA; phishing and safe reporting; browsing/downloads; device and update habits; handling customer information; and what to do in an incident. Each module should take no more than 20 minutes before discussion, use a relatable UK SME example, include three behaviours to practise, one short knowledge check and an escalation route. Do not claim training prevents every incident. Include accessibility options for staff who do not work at a desk or who need a different format.

Human check: new starters need the essentials before they receive sensitive access; refresh the material after relevant incidents or system changes.

37. Define a security-champion role carefully

Gather first: team structure, volunteers, manager sponsor, time available and escalation contact.

Prompt:

Design a modest security-champion role for [business]. Define purpose, selection criteria, time allowance, training topics, permissible activities, confidentiality boundary, reporting route and when a champion must hand the issue to IT, management or a specialist. Include a monthly agenda and a simple feedback loop for staff. Make clear that champions are not expected to investigate attacks, make legal decisions or approve risky access.

Human check: a champion is an extra pair of eyes, not a substitute for accountable owners or expert support.

38. Turn policies into everyday actions

Gather first: existing policies or notes, most important behaviours, staff roles and current tools.

Prompt:

Rewrite the following security policy into a one-page “what I do at work” guide: [redacted text]. Use short headings for sign-ins, suspicious messages, device updates, sharing information, payments and reporting. For each heading give: the expected action; an example; and who to contact if unsure. Preserve any confirmed mandatory wording separately. Remove jargon, but do not weaken approval or escalation steps. List ambiguities that the policy owner must resolve before issue.

Human check: ask two non-technical team members to read it and explain the actions back in their own words.

39. Send a quarterly security update

Gather first: changes made, relevant incident lessons, current scams, actions due and staff feedback.

Prompt:

Draft a concise quarterly security update for [business]. Include one change we made, one current behaviour to reinforce, one anonymised/fictional learning scenario, one action staff must take, reporting details and a date for the next update. Keep it factual and avoid fear-based statistics, blame or claims that a tool makes us fully secure. Add a manager version with open actions and owners.

Human check: only describe a threat trend if you can link to a credible current source or explain it arose from your own documented experience.

40. Encourage reporting, not concealment

Gather first: existing recognition practices, team preferences, reporting route, privacy expectations and manager sponsor.

Prompt:

Propose a low-cost security-reporting and recognition approach for [business]. The aim is early, honest reporting—not competition or surveillance. Include a private route to report a mistake or suspicious event, an acknowledgement standard, a learning review, optional team recognition for helpful reporting, and protections against public blame. Explain how managers should handle repeated risky behaviour fairly and when to seek HR, IT or legal support. Do not reward staff for finding vulnerabilities by probing live systems without permission.

Human check: measure reporting quality and follow-up, not simply how many reports people submit.

9. Monitoring, supplier management and review

41. Create a simple management dashboard

Gather first: key systems, risk owners, available provider reports, unresolved actions, backup tests, access reviews and training records.

Prompt:

Design a monthly cyber-security management dashboard for [business] that a non-technical owner can read in 10 minutes. Include only useful measures: critical-account MFA status; overdue access removals; update/support exceptions; backup restore-test status; high-priority supplier questions; reported suspicious events; open incident actions; and overdue policy/training reviews. For each metric give its definition, data source, owner, target status wording and action if red/amber. Do not invent a universal benchmark or aggregate unrelated counts into a misleading “security score”.

Human check: a dashboard should drive a decision. Remove measures that nobody uses.

42. Run a monthly security review

Gather first: system inventory, previous action register, access register, backup test record, supplier changes, incidents and business changes.

Prompt:

Write a monthly security-review checklist for [business]. Cover: new/removed users and administrators; MFA/recovery issues; critical updates/support status; backup completion and recent restore test; suspicious-email/account/payment reports; website/plugin changes; new third-party apps/suppliers; customer-data process changes; open incident actions; and next month's owners/dates. Use a printable table with evidence reference, status, action, owner and due date. Include a “no change confirmed” option rather than encouraging invented updates.

Human check: escalate gaps affecting money movement, administrator accounts, personal data or recovery before the next routine meeting.

43. Manage security suppliers with clear ownership

Gather first: all technology/security suppliers, contract renewal dates, account owners, service scope, data/access and incident contacts.

Prompt:

Create a supplier-management framework for [business] covering website host, IT support, email/cloud provider, payment provider, software vendors and any managed-security provider. Create a register with service, business owner, technical contact, data/access level, contract/renewal date, support channel, incident route, backup/exit arrangement, last review and open questions. Add a pre-engagement question set and an annual review agenda. Make clear that supplier reports or certifications do not remove our need to manage our own accounts, permissions and business decisions.

Human check: keep contract and support contacts available outside the supplier account where possible.

44. Use decision-useful security measures

Gather first: security objectives, baseline records, owner and meeting cadence.

Prompt:

Propose up to eight security measures for [business] based on these objectives: [objectives]. For each measure state: precise definition; numerator/denominator or status rule; data source; owner; reporting frequency; what a change might mean; and what decision it informs. Include measures for completion of critical MFA, leaver access removal, restore-test outcome, overdue high-priority actions, incident response time from discovery to triage, and training/reporting only where we can record them responsibly. Do not present a metric as evidence of compliance or safety. Add a data-quality check for each measure.

Human check: track trends and context. A low incident count may mean good prevention, weak detection or weak reporting.

45. Hold an annual security-strategy review

Gather first: previous plan, current systems/data map, incidents, supplier changes, contracts, dashboard, budget constraints and business plans.

Prompt:

Facilitate an annual cyber-security strategy review for [business]. Structure it around: what changed in the business; critical services/data; controls that worked or failed; incidents/near misses; access and supplier risks; backup/recovery evidence; team capability; legal/contract/insurer questions; planned investments; and an action plan. Use a table with risk/opportunity, evidence, decision, owner, deadline, dependency and review date. Separate confirmed findings from assumptions. End with a one-page management decision record and an agreed date to revisit it. Do not label the result a certification, audit opinion or compliance guarantee.

Human check: recheck official guidance and provider documentation after significant change, not only once each year.

Keep the work usable

Keep one controlled folder or register containing the approved account list, system map, access register, data inventory, supplier register, backup-test evidence, incident contacts, action list and review notes. Restrict access to people who need it, and make an offline or independent copy of critical contacts and response steps. Avoid keeping secrets in the same place as general planning documents.

If you suspect a real compromise, stop treating it as an AI-planning exercise. Use your incident plan, trusted provider contacts, insurer and qualified support. The NCSC directs UK organisations to current reporting and recovery routes; your actual steps depend on the incident and systems involved. [1](#)

Publication and use notice

This Ascendea draft is a **non-exclusive licensed adaptation** of private source material with UK-focused editorial guidance and practical prompts added. It is general education, not legal, data-protection, payment-compliance, insurance or cyber-security advice. Technology, provider terms and UK guidance can change; primary references below were checked on **10 October 2026** and should be rechecked before implementation.

Provided for your own learning and permitted end use. **No resale, private-label, redistribution, editable-source, underlying-source or PLR rights are granted.** This finished edition is available as a free Ascendea resource.

References and current guidance

1. [NCSC: Cyber security advice for small to medium sized organisations](https://www.ncsc.gov.uk/section/advice-guidance/small-medium-sized-organisations)
https://www.ncsc.gov.uk/section/advice-guidance/small-medium-sized-organisations
2. [NCSC: Multi-factor authentication for your corporate online services](https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services)
https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services
3. [NCSC: Mitigating malware and ransomware attacks](https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks)
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
4. [ICO: 72 hours — how to respond to a personal data breach](https://ico.org.uk/for-organisations/advice-for-small-organisations/personal-data-breaches/72-hours-how-to-respond-to-a-personal-data-breach/)
https://ico.org.uk/for-organisations/advice-for-small-organisations/personal-data-breaches/72-hours-how-to-respond-to-a-personal-data-breach/
5. [ICO: Business-to-business marketing](https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/business-to-business-marketing/)
https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/business-to-business-marketing/
6. [PCI Security Standards Council: Merchant resources](https://www.pcisecuritystandards.org/merchants/)
https://www.pcisecuritystandards.org/merchants/