AIT TECHNOLOGY | BUSINESS IMPLEMENTATION SERIES

AI implementation manual for business teams

Select useful workflows, protect information, test results and deploy controlled AI with named owners. Adapt the process to your departments and existing systems.



AI-generated editorial illustration; fictional people and systems.

Tailored to your business

AIT Technology can customise these procedures and build bespoke software, AI workflows and integrations. Scope, testing, pricing and support are agreed before implementation.

Version 1.0 | 18 November 2026 | UK business context

Starting framework: approve company-specific scope and owners before adoption. No certification, guaranteed compliance or emergency response service is implied.

How to use this manual

Business owners, process owners, IT, data/privacy leads and staff using or building AI-supported workflows.

Read the operating framework, assign department owners, select relevant sector scenarios, and adapt each procedure. The companion interactive PDF contains one reusable record per procedure. Save a separate copy for each case. Do not put passwords, API keys or recovery codes in these records.

Contents

Process at a glance

Operating framework

Department responsibilities

Business and sector scenarios

Step-by-step procedures

Records, approvals and maintenance

Custom implementation and sources

Process at a glance

01. Choose one workflow	02. Approve data and access	03. Build a bounded pilot	04. Test with people	05. Release, measure and improve

Use a named owner and recorded result at every handoff. Pause affected actions when safety, access or approval conditions are not met.

Operating framework

1. Start with a business outcome

Choose one repeated task with a clear input, output and reviewer. Record the current time, errors, rework and cost before changing it. Examples include drafting responses, extracting document fields or searching approved procedures. A process should not be automated solely because a model can produce a convincing demonstration.

AIT Technology can customise this manual and create bespoke AI applications, integrations, approval flows and dashboards around your company. We can help connect an agreed workflow to existing tools without assuming every system has a suitable API. Discovery establishes feasibility, data access, licence needs, acceptance tests and support scope.

2. Assign accountable roles and define boundaries

The business sponsor owns value and risk. The process owner defines the workflow and signs off results. The data owner authorises the information used. IT controls identity, integrations and operation. A reviewer checks outputs. The privacy/security lead reviews sensitive data and potential harm. One release owner can pause or roll back the system.

Define permitted inputs, outputs, users and external actions. Distinguish drafting from sending, recommending from approving and searching from modifying records. Keep money movement, employment decisions, health/safety decisions and other high-impact actions outside an unsupervised pilot. Obtain relevant specialist assessment before expanding scope.

3. Approve services and information handling

Maintain an AI service register: account type, owner, contract, purpose, permitted data, retention, processing locations, access, subprocessors, export/deletion and integration permissions. Check the current configuration and terms, not a general claim that a product is "private". Keep secrets out of prompts and logs.

Begin with fictional or suitably de-identified samples. De-identification itself requires assessment; removing a name may not make data anonymous. Where personal data is involved, assess lawful use, transparency, minimisation, retention and whether a data protection impact assessment is required. ICO guidance is a starting point; review the current position for the actual use case.

Microsoft documents enterprise protections for eligible Copilot Chat experiences, including specific handling of prompts, responses, uploads and web search. These are product/account-specific commitments, not a blanket statement about every chatbot or connected tool. Verify the approved tenant, feature and data route before using real business information.

4. Build a controlled and testable workflow

Write the task specification: approved source, expected fields, output format, missing-value behaviour, evidence links and escalation conditions. Use deterministic checks for totals, required fields and permitted destinations. Prompt instructions help shape behaviour but cannot replace access controls or validation.

Treat uploaded documents, web pages, email and retrieved passages as untrusted data. Separate them from controlling instructions. Give tools the smallest necessary permissions; use a restricted integration layer that validates actions and approvals independently of the model. Never give a draft generator authority to grant itself access or change its spending limit.

Define per-job call, token, time, retry and spend limits. Stop on repeated failure; maintain a queue/dead-letter route for human review. A timeout should not trigger an uncontrolled retry that sends the same message or creates the same order twice. Use idempotency and reconcile uncertain outcomes.

5. Evaluate before production

Build a representative, authorised test set including normal cases, missing fields, conflicting data, unusual layouts and malicious instructions. Keep a held-out set for release checks. Compare the reviewed result with the existing process; measure correction time and errors as well as generation speed.

Set acceptance thresholds before examining results. For an invoice extractor, test exact field accuracy and route uncertain or inconsistent records to a person. For an assistant, test whether it cites the right approved source and admits missing information. Do not publish invented benchmark results. Have the process owner approve release evidence.

6. Operate, review and improve

Release to a limited group with clear ownership, user guidance, a visible reporting route and an accessible non-AI fallback. Log model/configuration versions, actions, approvals, costs and failures with appropriate minimisation and retention. Protect logs because they may reveal confidential business information.

Review quality, incidents, cost per accepted output and actual time saved. Re-evaluate after model, prompt, source, permission or workflow changes. Pause when error thresholds, budget or security conditions fail. An apparent time saving that shifts unrecorded work to reviewers is not a verified improvement.

In the first 30 days, select a workflow and complete a synthetic pilot. By day 60, test approved representative data and controlled integrations. By day 90, assess a limited release against agreed quality and cost criteria. These are planning milestones to tailor, not guaranteed delivery dates.

Department responsibilities

Assign real names and deputies. A small company may combine roles, but must preserve accountability and approval boundaries.

Leadership

Owner: Sponsor / risk owner

Routine: Approve the business case, prohibited uses, budget and stop conditions.

Escalate when: Uncontrolled cost, harmful output, unclear ownership or proposed scope expansion.

Evidence: Use-case register and release/risk decisions.

Finance

Owner: Finance process owner

Routine: Use AI for draft extraction/classification with deterministic checks and human approval.

Escalate when: Changed bank details, inconsistent totals or suggested payment actions.

Evidence: Source reference, validation and payment approval outside AI.

HR

Owner: HR + privacy lead

Routine: Draft general onboarding and policy explanations from approved material.

Escalate when: Sensitive employee data, ranking people or consequential employment recommendations.

Evidence: Approved sources, review and fairness/privacy assessment where relevant.

Sales and marketing

Owner: Commercial owner

Routine: Draft accurate copy and follow-up suggestions; verify price, product features and claims.

Escalate when: Invented benefits, unapproved outreach, misleading claims or disclosure of client material.

Evidence: Reviewed draft, source facts and sending approval.

Customer service

Owner: Service owner

Routine: Prepare suggested answers from a controlled knowledge base.

Escalate when: Unanswered policy question, refund/contract commitment or vulnerable customer issue.

Evidence: Evidence source, reviewer and actual response sent.

Operations and logistics

Owner: Operations lead

Routine: Draft instructions and identify exceptions without altering physical control systems.

Escalate when: Unsafe recommendation, wrong order/stock record or conflicting source data.

Evidence: Validated exceptions and reconciliation with the system of record.

IT and development

Owner: Technical owner

Routine: Control model integrations, source access, secrets, evaluations, deployment and logs.

Escalate when: Prompt injection, leaked credentials, privilege escalation or repeated tool failure.

Evidence: Versioned specification, test results, permissions and rollback record.

Privacy and legal

Owner: Designated assessment lead

Routine: Review data purpose, notices, contracts, retention and affected-person risks.

Escalate when: Unapproved personal-data use or consequential automated decisions.

Evidence: Assessment, authorised data categories and agreed safeguards.

Business and sector scenarios

Planning scenarios, not assessments of named businesses. Add sector-specific safety, contractual and regulatory requirements before adoption.

Retail / e-commerce

Priorities: Product descriptions, catalogue cleanup and draft customer responses.

Scenario: An AI invents a product specification or refund promise.

Adaptation: Ground in approved product/policy records; block unsupported claims and review before publication.

Manufacturing

Priorities: Document search, maintenance-note summaries and quality exception review.

Scenario: An answer suggests an unsafe machine setting.

Adaptation: Keep control/safety decisions with competent staff; use approved versioned documentation and prohibit autonomous machine commands.

Logistics / warehousing

Priorities: Document extraction, order exceptions and reporting.

Scenario: An extraction assigns an order to the wrong customer.

Adaptation: Validate identifiers and totals against the system of record; send conflicts to human review before import.

Professional services

Priorities: Drafting, matter search and document comparison.

Scenario: A response mixes two clients' information.

Adaptation: Enforce project/client permissions in retrieval, not only in a prompt; use confidentiality review.

Care / health-related services

Priorities: Low-risk administration and approved information assistance.

Scenario: A draft makes a clinical or care recommendation.

Adaptation: Limit to agreed administrative scope; assess sensitive-data and safety requirements with qualified sector leads.

Construction / field services

Priorities: Job-note structure, quotation drafts and documentation search.

Scenario: An outdated drawing drives the recommendation.

Adaptation: Validate document revision and approval status; preserve engineer sign-off and site-specific safety processes.

Hospitality

Priorities: Draft guest communications and internal knowledge search.

Scenario: An assistant promises an unavailable room or service.

Adaptation: Check actual availability and policy through approved interfaces; prevent autonomous booking commitments during the pilot.

Education / charities

Priorities: General content drafts, grant-document organisation and internal FAQs.

Scenario: Personal information about a learner or beneficiary enters an unapproved service.

Adaptation: Define restricted categories and safeguarding escalation; use fictional samples before approved data handling.

Step-by-step procedures

01. Approve a new AI use case

Owner: Sponsor + process/data owners

Start when: A team proposes an AI workflow.

1. Describe the problem and baseline; identify affected users and decisions.

2. List data, services, tools, costs and risks; define prohibited actions.

3. Review privacy/security and contract requirements; assess whether simpler automation is adequate.

4. Set acceptance thresholds, pilot budget and stop conditions.

5. Approve only the bounded pilot, with a named reviewer and fallback.

Evidence: Use-case record, assessment and approval.

Completion / handoff: Scope and success criteria agreed before access is granted.

02. Run a document-extraction pilot

Owner: Process owner + technical owner

Start when: Repeated documents need structured fields.

1. Select authorised synthetic samples and define a schema with required fields.

2. Require missing/uncertain values to be flagged; prohibit guessed facts.

3. Validate identifiers, amounts and allowed categories deterministically.

4. Compare to a verified answer set and measure correction time.

5. Route failed validation to a person; no automatic accounting/payment entry in the initial pilot.

Evidence: Dataset version, exact-match errors, review effort and failure cases.

Completion / handoff: Owner accepts measured quality or rejects/revises the workflow.

03. Release a knowledge assistant

Owner: Knowledge owner + IT

Start when: Staff need answers from internal procedures.

1. Choose current approved sources and their access restrictions.

2. Enforce user permissions during retrieval; test cross-client and restricted-document isolation.

3. Require source references and "not found" handling.

4. Test conflicting/outdated pages and embedded malicious instructions.

5. Release to a limited group with reporting, review and a fallback to the source owner.

Evidence: Source inventory, access tests and evaluated answers.

Completion / handoff: No demonstrated access-boundary failure and agreed quality threshold met.

04. Connect an action tool

Owner: Integration owner + business approver

Start when: AI is proposed to send, update or create something.

1. Separate suggestion from execution; define exact allowed actions and destinations.

2. Use least-privilege credentials outside the prompt/workspace.

3. Validate schema, permissions, cost and human approval in the execution service.

4. Test duplicates, timeout-after-success and malicious payloads using synthetic data.

5. Enable only the authorised scope with audit and a tested disable switch.

Evidence: Permission matrix, tool tests, approvals and action receipts.

Completion / handoff: External effects match the approved request and uncertain outcomes are reconciled.

05. Respond to unsafe or incorrect AI output

Owner: User + process owner + IT

Start when: Invented fact, leaked information or harmful instruction.

1. Do not act on or forward the output as fact.

2. Record a minimal authorised example and version; restrict access to sensitive material.

3. Pause the affected workflow if boundaries or significant harm are involved.

4. Assess data exposure and use the incident process if needed.

5. Correct root causes and rerun relevant evaluations before reactivation.

Evidence: Incident/defect record, impact and retest.

Completion / handoff: Owner authorises resume with documented evidence, not only a rewritten prompt.

06. Control cost and model changes

Owner: Service owner

Start when: Budget threshold, recurring failure or provider/model update.

1. Measure calls, tokens, retries and accepted outputs per workflow.

2. Enforce local per-job and cumulative limits independently of provider alerts.

3. Pause queued paid execution at limits; retain data and logs.

4. Evaluate the new version on a held-out set before promotion.

5. Require the authorised owner to approve budget or scope increases.

Evidence: Cost ledger, evaluation comparison and change approval.

Completion / handoff: Approved budget and tested quality restored; no automatic limit bypass.

Records, approvals and maintenance

Use the companion forms to record company/case reference, owner and time zone, scope/trigger, verified facts, actions, approvals, completion and next review. Preserve original evidence in a restricted approved location; use references rather than copying sensitive material unnecessarily.

Company adoption checklist

- Define legal entities, sites, systems, information categories and exclusions.

- Assign accountable owners, deputies and escalation contacts, including agreed coverage hours.

- Agree retention, access, response objectives, budgets and stop conditions.

- Test representative workflows, exceptions, recovery and approval boundaries.

- Approve a version, train users, record evidence and set the next review date.

Urgent, significant and routine work

Urgent: suspected active compromise, sensitive-data exposure, fraud, safety risk or critical loss of service. Contact the named lead immediately through a trusted route. Significant: contained material disruption or weakness, with a coordinated owner and deadline. Routine: low-impact requests tracked to closure. Define actual response times and reclassify if impact changes.

The manual and AIT contact form are not emergency channels. Do not delay bank, safety or incident escalation while completing a form.

Custom implementation with AIT Technology

We can adapt this manual to your organisation and departments, map existing processes and build bespoke software, controlled AI workflows, integrations, approval queues and practical dashboards. Begin with discovery, agree scope and tests, implement reversibly, validate with users, and agree ongoing ownership and support separately.

Sources and limitations

Sources checked 18 November 2026. This is original AIT operational guidance. Suggested roles, frequencies, templates and workflows must be tailored; they are not verbatim official requirements. Linked guidance may change. Regulated or safety-critical use requires appropriate specialist assessment.

NCSC: guidelines for secure AI system development

https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development

ICO: guidance on AI and data protection

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/

Microsoft: Copilot Chat privacy and protections

https://learn.microsoft.com/en-us/copilot/privacy-and-protections

Discuss a tailored implementation: https://aittech.co.uk/contact/