AI Change Management Checklist

A practical checklist for governing the introduction of a new AI feature, tool, or capability through change management

ISO 42001 · AI Governance · Change Management · Data Privacy · Information Security

Introducing a new AI feature carries risks that a standard IT change request does not capture — data exposure, unreliable output, and unclear accountability for automated decisions. This checklist sets out a practical sequence for assessing and approving an AI-related change before it goes live.

A Scope, Ownership & Risk Classification

- [ ] Describe the AI feature, its purpose, and its intended business benefit
- [ ] Obtain business owner / product owner approval for the requirement
- [ ] Identify the system owner / technical owner accountable for the change
- [ ] Confirm the change type and risk rating, for example normal, major, or high-risk

B AI Use Case & Business Impact

- [ ] Define the AI use case, for example chatbot, search, summarisation, recommendations, document generation, analytics, or decision support
- [ ] Confirm whether the AI output is advisory only or whether it triggers automated actions
- [ ] Assess the impact on users, business processes, workflows, and existing controls
- [ ] Assess the impact on financial, HR, legal, procurement, customer, or compliance decisions

C Data Privacy & Data Flow

- [ ] Complete a privacy / data protection assessment for the change
- [ ] Confirm whether personal, confidential, or sensitive information will be processed by the AI feature
- [ ] Document the data flow, including what data is sent to the AI service, where it is processed, and where it is stored
- [ ] Confirm with the vendor whether organisational data, prompts, uploads, or outputs will be used to train AI models
- [ ] Confirm the hosting location, cloud region, and any cross-border data transfer

D Vendor & Security Review

- [ ] Review the AI vendor's terms, privacy policy, data processing agreement, and SLA
- [ ] Have Information Security review the AI feature and its integration
- [ ] Confirm authentication, SSO, MFA, and role-based access controls are in place
- [ ] Confirm API keys, tokens, and secrets are securely managed
- [ ] Confirm data is encrypted in transit and at rest

E Testing & Assurance

- [ ] Test the AI feature for accuracy, hallucinations, inappropriate outputs, and bias
- [ ] Confirm testing shows users cannot access unauthorised data through AI prompts or responses
- [ ] Complete UAT and obtain sign-off from business users
- [ ] Review and approve the updated architecture / integration design

F Operational Readiness

- [ ] Assess the performance, capacity, licensing, and cost impact of the change
- [ ] Confirm a clear support model for incidents, incorrect AI outputs, and user queries
- [ ] Brief the service desk / support team on the change

G User Communication & Safeguards

- [ ] Prepare user communication and training, including do's and don'ts for using the AI feature
- [ ] Warn users not to enter confidential, personal, or restricted data unless formally approved
- [ ] Provide a clear disclaimer that AI outputs must be reviewed and should not be treated as final decisions

H Rollout, Rollback & Post-Implementation Monitoring

- [ ] Confirm the AI feature can be disabled quickly through a feature toggle or configuration setting
- [ ] Document and, where possible, test a rollback / backout plan
- [ ] Consider a pilot or phased rollout before full implementation
- [ ] Check the go-live date against business-critical periods, month-end, year-end, or system freeze periods
- [ ] Agree a post-implementation review date
- [ ] Monitor usage, incidents, costs, accuracy issues, and user feedback after go-live

© XGRC® Software, a Strategix product. Strategix Application Solutions (Pty) Ltd, Reg No. 2015/192960/07. ISO 27001:2022 certified. info@xgrcsoftware.com