

# ALM Release Checklist

Deployment standards, governance baseline, and quality gates for managed solution releases - IT Helpdesk Assistant.

**Leila Marchant**

Power Platform & Copilot Studio Developer

AZ-900 · AI-900 · PL-900

Winchester, UK · Remote / Hybrid

**7**

Sections

**9**

DoD Criteria

**5**

Release Stages

**3**

Environments

PR

CORE PRINCIPLES

Six rules that govern every build, release, and deployment decision on this project.

<p><b>Unmanaged = Build</b> Dev environment only. Never deploy Unmanaged to UAT or Production.</p>	<p><b>Managed = Deploy</b> UAT + Prod only. Managed solutions are locked - no editing flows post-import.</p>	<p><b>Dataverse = System of Record</b> Every ticket event - creation, notification, decision, escalation - stored as structured data, not in run history.</p>
<p><b>Config Externalised</b> Env Vars + Connection Refs. No endpoints, API keys, channel IDs, or recipient addresses hard-coded in flow actions.</p>	<p><b>Watchers = Idempotent</b> NotificationSent and AlreadyEscalated flags prevent duplicate manager cards and duplicate director escalations.</p>	<p><b>No Prod Hot Fixes</b> Fix in Dev → version → redeploy. No editing flows in UAT or Production. There are no exceptions.</p>

01

SOLUTION IDENTITY

The solution is the unit of deployment. Every artefact that ships to UAT or Production must be inside the managed solution. Everything else stays out.

Solution Naming

**Unmanaged (Dev):** lai\_ITHelpdeskPortfolio

**Export filename:** lai\_ITHelpdeskPortfolio\_1.1.0.0\_managed.zip

**Publisher:** Your owned publisher - never the Default publisher

**Prefix:** lai\_ applied to all tables, columns, choices, choice sets, relationships, and flows

Solution Contents

✓ Must be inside the solution	✗ Must NOT be inside
<ul style="list-style-type: none"> <li>- Copilot Studio agent (IT Helpdesk bot - V1 and V2 topics)</li> <li>- Dataverse table: IT Helpdesk Tickets + choice sets (Category, Priority, Status)</li> <li>- Flow: Helper-CreateTicket (Copilot-triggered)</li> <li>- Flow: Helper-CheckStatus (Copilot-triggered)</li> <li>- Flow: Helper-EscalateTicket (manual or watcher-triggered)</li> <li>- Flow: SummariseTicket_BYOM (child flow - called by CreateTicket)</li> <li>- Flow: Automation-NotifyManager (scheduled watcher)</li> <li>- Security roles: End User, Manager, Director, Admin, Automation (Service)</li> <li>- Field Security Profiles for ManagerDecision, DecisionNotes, EscalationError, AiSummary</li> <li>- Environment variables + connection references</li> </ul>	<ul style="list-style-type: none"> <li>- Transactional data (live IT ticket rows - never export production data)</li> <li>- Personal maker connections - always use connection references</li> </ul>

## 02 CONFIGURATION RULES

No endpoint, key, channel ID, SLA threshold, or recipient address may be embedded inside a flow action. Every configurable value must be externalised before export.

### Environment Variables

Variable Name	Purpose
<b>lai_BYOM_Endpoint</b>	Azure OpenAI endpoint URL for the SummariseTicket_BYOM child flow
<b>lai_BYOM_DeploymentName</b>	Model deployment name - set per environment (dev/UAT/prod may differ)
<b>lai_BYOM_ApiVersion</b>	Azure OpenAI API version string
<b>lai_BYOM_ApiKey</b>	Secret ★ - store in Key Vault, never in plain-text environment variable
<b>lai_BYOM_SystemPrompt</b>	System prompt used for ticket summarisation - editable without flow change
<b>lai_SLA_ThresholdHours</b>	Hours before an open ticket is treated as SLA-breached by the watcher
<b>lai_EscalationRecipient</b>	Director UPN or Teams channel for SLA escalation notifications
<b>lai_ManagerChannelId</b>	Teams channel ID or mailbox for manager notification delivery

### Connection References

All connectors must be abstracted behind connection references - resolved by the importing admin at import time, never pre-bound to a maker account.

Connector	Usage
<b>Dataverse (Current Environment)</b>	All ticket table read/write operations across all flows
<b>Microsoft Teams</b>	Manager Adaptive Card delivery and director escalation messages
<b>HTTP</b>	Azure OpenAI REST calls from the SummariseTicket_BYOM child flow
<b>Office 365 Outlook</b>	Optional fallback notification if Teams delivery is unavailable

#### ALM CONFIGURATION RULE

If you cannot change an endpoint, API key, SLA threshold, or notification channel at import time without opening a flow action and editing it, the release is not done.

## 03

## VERSIONING RULES

Use MAJOR.MINOR.PATCH.BUILD format. Increment the version before every export. Versions are immutable - never re-export the same version number with different content.

## Version Tiers

Version Tier	Applies When
<b>PATCH</b> · 1.0.0.1	Bugfix or logic tweak. No schema change. Deploy: Update (overwrite in place).
<b>MINOR</b> · 1.1.0.0	New capability or new column - e.g. adding V2 Entra auth, new watcher branch. Deploy: Update or Upgrade.
<b>MAJOR</b> · 2.0.0.0	Breaking change to ticket state model, idempotency behaviour, or FLS profile structure. Deploy: Upgrade (staged release).

## Version Impact Reference

Change Type	Version Impact	Example
<b>New column used by flows or FLS profiles</b>	Minor → 1.1.0.0	Added lai_AlreadyEscalated flag column
<b>Rename/remove a column referenced by flows</b>	Major → 2.0.0.0	Renamed lai_NotificationSent to lai_ManagerNotified
<b>Idempotency flag behaviour or SLA logic change</b>	Major → 2.0.0.0	Changed when AlreadyEscalated is stamped in watcher
<b>Bugfix to notification card format, no schema change</b>	Patch → 1.0.0.1	Fixed manager card not displaying AiSummary field
<b>New auth mode added (e.g. V2 Entra ID topics)</b>	Minor → 1.1.0.0	Added authenticated intake topic and AadObjectId field
<b>FLS profile updated - new field added to profile</b>	Minor → 1.1.0.0	Added EscalationError to manager FLS read scope

04

**UPDATE vs UPGRADE**

Choosing the wrong deployment strategy risks data loss or broken solutions in Production. Apply this decision every time before promoting a release.

Decision Point	Details
<b>Use Update for</b>	Patch and most Minor releases - safe, no parallel solution, lower risk of disruption.
<b>Safe for Update</b>	Watcher logic improvements (idempotency flags unchanged); notification card redesign; new Copilot topic added; new optional columns with no flows depending on removal of old columns.
<b>Use Upgrade for</b>	All Major releases - a parallel solution is held alongside the existing one during import; the old solution is removed only after full validation passes.
<b>Required Upgrade</b>	Ticket state model change; idempotency flag behaviour change; FLS profile restructure; column renamed or removed that is referenced by existing flows or views.

## 05

## RELEASE PIPELINE

Five stages, in order, without exception. Do not skip stages. Do not re-export from Dev after UAT passes.

## A

**Pre-Export Validation** · Dev environment

- ✓ Happy path end-to-end: ticket submitted via Copilot → Dataverse row created → manager Teams card posted → decision written back → resolved state stamped
- ✓ V2 path: Entra ID sign-in → AadObjectId and UPN captured in ticket row → authorisation gate prevents unauthenticated create
- ✓ AI path: SummariseTicket\_BYOM returns summary → AiSummary populated in Dataverse row
- ✓ Fallback path: Force BYOM failure → fallback string returned → ticket creation completes without blocking
- ✓ Idempotency: Automation-NotifyManager watcher re-triggered manually → NotificationSent flag prevents second card
- ✓ Escalation idempotency: SLA watcher run with AlreadyEscalated = true → no duplicate director notification sent
- ✓ No hard-coding: no endpoints, API keys, channel IDs, or addresses embedded in any flow action
- ✓ All connectors abstracted behind connection references - no personal maker connections present

## B

**Export** · Dev environment

- ✓ Export Managed solution only - never export Unmanaged for deployment
- ✓ Increment version before export (MAJOR.MINOR.PATCH.BUILD)
- ✓ Filename: lai\_ITHelpdeskPortfolio\_1.1.0.0\_managed.zip
- ✓ Write release notes: what changed, version number, any new env vars or connection references required
- ✓ Retain the previous managed zip as the rollback artefact before importing the new release

## C

**UAT Import & Configuration** · UAT environment

- ✓ Import the managed zip - no import errors expected
- ✓ Set all environment variable values: BYOM config (endpoint, deployment, version, key), SLA threshold, escalation recipient, manager channel
- ✓ Bind all connection references to appropriate service identities (not maker accounts)
- ✓ Assign security roles to test accounts: End User, Manager, Director, Admin, Automation (Service)
- ✓ Apply Field Security Profiles to all test accounts as per role assignments
- ✓ Enable environment-level and table-level auditing on the IT Helpdesk Tickets table

## D

**UAT Smoke Tests** · UAT environment

- ✓ Submit one ticket via Copilot - V1 public variant - Dataverse row created with TicketId and AiSummary
- ✓ Submit one ticket - V2 Entra ID variant - AadObjectId and UPN confirmed in Dataverse row
- ✓ Automation-NotifyManager watcher posts exactly one Teams card (NotificationSent = true confirmed)
- ✓ Re-trigger watcher manually - no second card posted (idempotency confirmed)

- ✓ Manager uses write-back action on card - ManagerDecision and DecisionNotes written to Dataverse
- ✓ Age a ticket past the SLA threshold - watcher posts director escalation, AlreadyEscalated = true
- ✓ Re-trigger SLA watcher - no second escalation sent (AlreadyEscalated idempotency confirmed)
- ✓ Force BYOM failure - fallback summary returned, ticket row created, CreateTicket flow not blocked
- ✓ Check-status topic returns correct state for each ticket lifecycle stage tested

## E

### **Production Promotion** · Production environment

- ✓ Import the identical managed zip that passed UAT - do not re-export from Dev
- ✓ Repeat post-import configuration: all env vars, connection reference bindings, role and FLS assignments
- ✓ Repeat smoke tests: one ticket submitted, one manager card posted, one write-back action confirmed
- ✓ Confirm SLA watcher schedule is active and running on expected interval
- ✓ Retain the previous managed zip as the rollback artefact

06

GOVERNANCE

These controls must ship with every managed release and be validated in UAT before production promotion. None are optional.

Security Roles

Role	Permissions
IT Helpdesk – End User	Create tickets and read own records only. Cannot view other users' tickets. Ticket fields are read-only once Status leaves Open.
IT Helpdesk – Manager	Read assigned open tickets. Write ManagerDecision and DecisionNotes via FLS profile. Cannot create or delete records.
IT Helpdesk – Director	Read escalated tickets and SLA breach records. No edit access to ticket fields. Receives escalation notifications.
IT Helpdesk – Admin	Full control. Assigned to service accounts and platform admins only - not to individual staff.
IT Helpdesk – Automation	Least-privilege service identity for all flow operations. Scoped to required tables only.

Field-Level Security (FLS)

Field	FLS Rule
ManagerDecision	Write: Manager + Automation roles only. End User has no read or write access.
DecisionNotes	Write: Manager + Automation roles only. Director has read access for escalation review.
AiSummary	Write: Automation role only. Manager and Director have read access. End User has no access.
EscalationError	Write: Automation role only. Admin has read access for support investigation.
SlaBreachedOn	Write: Automation role only. Director and Admin have read access.

Controls, Auditing & Observability

Control	Details
TicketId	Unique correlation ID generated at creation - ties all flow run events to a single ticket lifecycle.

<b>Audit Fields</b>	NotificationSent, SentOn, AlreadyEscalated, EscalatedOn, ManagerDecision, SlaBreachOn, NotifyError, and EscalationError are all included in Dataverse table audit configuration.
<b>CATCH Scope Pattern</b>	Automation-NotifyManager and the SLA watcher both use Try/Catch. Failures write to NotifyError or EscalationError - no silent errors, no disappearing run history.
<b>FLS Audit</b>	Field security profile assignments are audited at the environment level. Confirm audit is active before Production promotion.

07

**DEFINITION OF DONE**

A release is not done until every criterion below is satisfied and evidenced. Partial completion does not qualify for production promotion - including patches.

#	Criterion	Evidence Required
1	Managed solution imports cleanly into UAT - no import errors, no manual edits to flows required	Import log screenshot
2	All environment variable values configured post-import without touching any flow action	Env var config screenshot
3	All connection references resolved to service identities - no personal maker connections in UAT or Prod	Connection reference screenshot
4	RBAC security roles and FLS profiles assigned and validated - End User cannot read ManagerDecision	Role and FLS assignment evidence
5	Environment + table auditing enabled; at least one audit record captured per lifecycle stage tested	Audit log screenshot
6	Happy path verified: ticket submitted, manager card posted once, decision written back, status resolved	Flow run history + Dataverse row state
7	NotificationSent idempotency proven: watcher re-triggered, no duplicate manager card sent	Flow run history showing flag check
8	AlreadyEscalated idempotency proven: SLA watcher re-run after escalation, no duplicate director message	Flow run history + Dataverse row state
9	Evidence pack assembled: version, env vars, connection refs, role/FLS assignments, audit log, run history	Evidence pack document

**RELEASE AUTHORISATION**

All nine criteria must be met and evidenced before any managed solution is promoted to Production. There are no emergency bypasses - including patches. This document is the evidence checklist for the IT Helpdesk Assistant solution (lai\_ITHelpdeskPortfolio).