

AI Automation Approval Form

The Operator's Manual for Artificial Intelligence

Template Kit — Document 6 of 6

IMPORTANT — BEFORE YOU USE THESE TEMPLATES

These templates are starting points for organizations without existing AI governance. They are not legal documents and are not a substitute for qualified legal counsel. Review and adapt them to your specific jurisdiction, industry, and situation before use. Do not implement any policy, form, or checklist from this kit without professional review. The Operator's Manual for Artificial Intelligence makes no representations as to their completeness, accuracy, or fitness for any particular purpose.

Complete this form before deploying any AI system that takes autonomous actions — sending communications, modifying records, executing transactions, or any action that affects a real system without human review of each step. Incomplete forms are not a basis for approval. Do not deploy until all items are signed off.

1. System Information

Field	Entry
System / Automation Name	
Version	
Date of Submission	
Submitted By (Name and Title)	
Team / Department	
AI Tool or Platform Used	
Vendor	
Environment (Production / Staging / Test)	
Planned Deployment Date	

2. System Description

What does this system do? Describe its inputs, what action it takes, what it affects, and under what conditions it runs.

3. Risk Assessment

Field	Entry
Risk Level (Low / Medium / High / Critical)	
Risk Ladder Category That Applies	
What is the worst plausible outcome if this system fails?	
How would a failure be detected?	
How quickly could a failure cause irreversible harm?	
Is this classified as Critical or Prohibited Without Governance?	
If Yes — what governance controls are in place?	

4. Formal Controls Checklist

This checklist is based on Sub-Module 2.3 (Before You Automate) of The Operator's Manual for Artificial Intelligence. Every item must be confirmed before deployment. Unconfirmed items are blockers.

Control	Status	Confirmed By	Date
Human-in-the-loop is documented: a named person must approve each action before it executes (or the approval criteria are explicit and logged).			
Scope is defined: the system operates only on specified data, systems, and actions. No write access beyond what is required.			
Scoped permissions are in place: the system has been granted only minimum required access. Excess access has been removed.			
A rollback procedure is documented: who executes it, what step disables or reverts the system, how confirmation is obtained.			
Logging is enabled: all AI decisions, inputs, outputs, and actions are recorded with timestamps and stored for a minimum of [enter period].			
A test run has been completed in a non-production environment. Results are documented and attached to this form.			
Drift monitoring is in place: a defined schedule exists for reviewing whether the system is still			

Control	Status	Confirmed By	Date
behaving as intended. Responsible party is named.			
Alert thresholds are defined: conditions that trigger automatic suspension or human review are documented.			
The system has been reviewed by IT security for the relevant OWASP LLM risks applicable to this deployment.			

5. Rollback Procedure

The rollback procedure must be complete before deployment. Vague or incomplete procedures are not acceptable.

Field	Entry
Who executes the rollback (Name and Title)?	
Step 1 — What action disables or suspends the automation?	
Step 2 — What action reverts any changes made by the system?	
Step 3 — How is successful rollback confirmed?	
Estimated time to complete rollback from decision to confirmation	
Has the rollback procedure been tested? (Yes / No)	
Date last tested	
Tested By (Name and Title)	

6. Test Run Documentation

Field	Entry
Test environment used	
Date of test run	
Conducted By	
Scenarios tested	
Results (Pass / Fail / Partial)	
Issues identified and resolved	

Field	Entry
Test documentation attached? (Yes / No)	

7. Review Schedule

Field	Entry
Review Frequency (e.g., monthly, quarterly)	
Responsible Reviewer (Name and Title)	
Date of First Scheduled Review	
Criteria for Suspension or Decommission	
Escalation Path if Anomaly Is Detected	

8. Approval Sign-off

All four approvals are required before deployment. Deployment without all signatures is a policy violation.

Submitted By (Engineer / Owner)	Date
Technical Review (IT Security)	Date
Risk / Compliance Review	Date
Final Approval (Policy Owner or Exec)	Date