GOVERNANCE TEMPLATE

Intent Document Template

v1.0 May 2026 Sougata Roy, sougataroy.com

A minimum Tier 2 Intent Document structure for documenting agent purpose, authorized scope, explicit prohibitions, accountability, review cadence, and escalation path before deployment.

HOW TO USE THIS TEMPLATE

Complete every field before the agent enters production. The Explicit Prohibitions field cannot be blank. A scope document without explicit prohibitions is incomplete. It defines permissions but not the boundary from the outside, which is what an examiner will ask for. Tier 1 agents may use an abbreviated version covering Purpose Statement, Authorized Scope, and Consequence Owner only. Tier 3 agents require additional fields covering delegation scope, sub-agent authorization, and board reporting obligations.

SECTION 1: AGENT IDENTITY

Agent Name

Display name as it appears in the agent registry. Not the technical identifier.

Deployment Environment

Microsoft 365 tenant name, Copilot Studio environment, or platform where the agent is deployed.

Risk Tier

Tier 1 (Low Risk), Tier 2 (Medium Risk), or Tier 3 (High Risk). Determined before this document is written.

Deployment Date

The date the agent first entered production operation. This document must be signed before this date.

SECTION 2: INTENT, THE PURPOSE (LAYER 2)

LAYER 2 REQUIREMENT

All three components below must be present. A purpose statement without an explicit scope is incomplete. An authorized scope without explicit prohibitions is incomplete. Expected outputs without human review triggers are incomplete. If any component is missing, the Intent Document does not exist for this agent.

Purpose Statement

What this agent is supposed to accomplish, in plain language that a compliance officer can evaluate without technical context. If this sentence could have been written by reading the configuration file, it is a capabilities description, not a purpose statement.

Authorized Actions

Specific actions this agent may take, tied to named systems. Use "The agent may:" for each permitted action. Be specific enough that a new compliance officer could determine whether a specific observed action was authorized.

The agent may:
The agent may:
The agent may:
The agent may:

EXPLICIT PROHIBITIONS — THIS FIELD CANNOT BE BLANK

Use "The agent may NOT:" for each prohibition. Authorization boundaries without explicit prohibitions are incomplete. This field defines the boundary from the outside.

The agent may NOT:
The agent may NOT:
The agent may NOT:
The agent may NOT:

Data Access Scope

Named systems with read/write designation. If the agent can access it, list it. If it is not listed, the agent is not authorized to access it.

System Name	Access Type	Scope Notes
	Read / Write / Read-Write	
	Read / Write / Read-Write	
	Read / Write / Read-Write	
	Read / Write / Read-Write	

Expected Outputs and Human Review Triggers

Describe what correct behavior looks like and what constitutes an anomalous output requiring human review. This is the standard against which production behavior is measured.

Correct Behavior	Triggers Human Review

SECTION 3: GOVERNANCE, THE ACCOUNTABILITY (LAYER 3)

Consequence Owner

Full name, title, and organizational unit. This is the named individual accountable for board-level accountability and incident escalation decisions. Not a team. Not a role. A specific person who knows they own this agent.

Consequence Owner Contact

Work phone and email. Reachable during an incident.

Technical Owner

Full name and title. Responsible for agent configuration, credentials, monitoring, and day-to-day control enforcement. Must be a different individual from the Consequence Owner.

Review Cadence

Scheduled interval (e.g., quarterly) plus named event triggers: any Microsoft product release that modifies agent capabilities, any change to system integrations, any incident involving this agent, any change to the Consequence Owner or Technical Owner.

Escalation Path

Named contacts in sequence when the agent triggers an anomaly. Include trigger conditions for immediate action versus scheduled review. This path must be written before the first incident. Not assembled during it.

SECTION 4: AUTHORIZATION SIGNOFF

Signatory	Title and Authority	Date Signed
Business Owner (Consequence	*Authorized to grant the scope*	

Owner)	*described in Section 2*	
Compliance Review	*Completed pre-deployment compliance review*	
Legal Review	*Completed pre-deployment legal review*	
Technical Owner	*Confirms configuration matches documented intent*	

SIGNING REQUIREMENT

The authorization signoff must predate the agent's first production action. A document signed after deployment is retroactive documentation, not pre-deployment governance. The date on this document is the governance evidence.

SECTION 5: DOCUMENT VERSION HISTORY

Version	Date	Change Description	Approved By
v1.0		*Initial authorization*	

This template is provided as an organizational design aid. It is not legal advice. Organizations should obtain qualified legal and regulatory counsel before treating any field or requirement here as compliance guidance. Intent Document requirements vary by industry, jurisdiction, regulatory regime, and agent risk profile.