



## Business AI Governance: Operational Oversight, Audit Readiness & Escalation

- 5 Hours Course
- Hands-on and Lecture

### Course Overview

As enterprise AI assistants and workflows—including Microsoft Copilot, Claude Enterprise, Agentforce, and custom GPTs—move into daily production, organizations require dedicated business oversight. This non-technical clinic prepares Business AI Owners to govern AI outputs, monitor business performance degradation, manage human reviewers, escalate technical issues to the appropriate responsible teams, and assemble audit-ready compliance documentation for three-year record retention.

### Who Should Attend

- Business AI Owners
- Process Leads
- Department Heads
- Risk Managers
- Compliance Leads

### What You'll Learn

- Define the operational responsibilities of Business AI Owners and technical platform owners.
- Establish business quality expectations for deployed AI workflows.
- Review exported AI activity logs and evaluate representative output samples.
- Detect degradation in the business quality of AI-generated outputs.
- Calculate Business Quality Scores and human-review oversight metrics.
- Identify reviewer anomalies and ineffective human-in-the-loop practices.
- Distinguish between business, content, security, compliance, and technical issues.
- Escalate AI-related incidents to the team responsible for the affected area.
- Assemble an AI evidence packet for audit and compliance review.

### Outline

#### 1. The Business AI Owner's Role and Business Quality Expectations

- Define the operational boundary between Business AI Owners and Platform or IT teams
- Business AI Owner responsibilities: business outcomes, content validity, and human processes
- Platform and technical owner responsibilities: infrastructure, APIs, and code
- Define what a correct AI-generated answer looks like
- Document business rules that must always be followed
- Identify errors that are unacceptable
- Determine when humans should intervene
- Establish how much inconsistency is tolerable in deployed AI workflows

## 2. Quality Auditing: Detecting Business Performance Degradation

- Review exported AI activity logs provided by platform administrators
- Work with sample exports using Excel, SharePoint, or ticketing tools without requiring direct system access
- Recognize degradation caused by changing inputs, vendor model updates, evolving company policies, or prompt modifications
- Hands-on exercise: evaluate a 20-response sample export from a business AI agent
- Hands-on exercise: score responses against established business guidelines
- Hands-on exercise: calculate a Business Quality Score

## 3. Human-in-the-Loop Oversight and Reviewer Quality

- Track human corrections and overrides using Excel, SharePoint, Jira, or ServiceNow
- Calculate Human Agreement Rates, Override Percentages, and Disagreement Trends
- Identify reviewers who approve AI outputs without adequate verification
- Distinguish rubber-stamping from valid human review and correction
- Hands-on exercise: analyze a simulated 30-day log of reviewer decisions
- Hands-on exercise: identify reviewer anomalies
- Hands-on exercise: draft an operational remediation plan

## 4. The Escalation Matrix: Knowing When to Hand Off

- Distinguish issues that can be resolved through business-rule updates from those requiring technical escalation
- Escalate widespread output degradation or sudden model changes to the team responsible for the AI platform
- Escalate incorrect or outdated policies, procedures, FAQs, or product information to the owner responsible for maintaining that content
- Escalate sensitive-data or PII exposure to the responsible Information Security and Legal functions
- Escalate system timeouts or error codes to the team responsible for the affected technology or vendor relationship
- Recognize that the responsible technical owner may be a SaaS administrator, platform owner, vendor support team, internal IT team, or managed service provider
- Escalate hallucinated legal, financial, or regulatory advice to the responsible Risk and Compliance functions
- Hands-on exercise: evaluate five realistic AI incident scenarios
- Hands-on exercise: map each incident to the appropriate operational escalation path
- Hands-on exercise: draft an appropriate escalation ticket

## 5. Assembling the Audit Hand-Off Packet

- Understand evidence expectations for internal audit, risk teams, and regulatory bodies
- Organize evidence for three-year record retention
- Hands-on exercise: build an audit-ready AI Evidence Packet Template
- Document the business purpose statement
- Document system instructions and baseline business rules
- Include sampled review records and Business Quality Scores
- Include a human-in-the-loop override summary and reviewer quality audit
- Include an incident and escalation history log
- Include a change-control and approval log

## Prerequisites

- None

- No coding experience required
- This course focuses on business process management and operational governance