

# General AI Integration and Adoption Strategy Paper

*From use-case catalogs to measurable business transformation*

A practical framework for turning current processes, events, actions, and decisions into governed, valuable, and sustainable AI capabilities

Date: July 2026

## Central thesis

Almost any existing business process, event, action, decision, document, transaction, conversation, or workflow can be described as an AI use case. That does not mean every activity should become an AI project. A successful AI integration strategy must distinguish AI-worthy opportunities from ordinary automation, data cleanup, reporting, and process discipline. The goal is not to maximize the number of AI use cases; the goal is to redesign work so AI improves outcomes, evidence, productivity, quality, speed, control, and decision confidence.

*Prepared as a general companion paper to AI use-case catalog and AI strategy work.*

## Table of Contents

- 1. Executive Summary
- 2. Why Everything Can Look Like an AI Use Case
- 3. AI Integration Adoption Model
- 4. Taxonomy of AI Use Cases Across Business Processes
- 5. What Must Be True for a Successful AI Use Case
- 6. Data, Resource, Environment, and Process Requirements
- 7. Governance, Risk, and Control Requirements
- 8. Step-by-Step AI Use-Case Lifecycle
- 9. Metrics, Expected Outcomes, and Value Realization
- 10. Recommended Actions for Leaders
- 11. Conclusion
- Appendix A. AI-Worthiness Scoring Model
- Appendix B. Reusable Use-Case Patterns
- Appendix C. Source Notes

# 1. Executive Summary

Artificial intelligence has reached the stage where organizations can plausibly apply it to almost every business function: drafting, summarizing, searching, classifying, forecasting, reconciling, monitoring, detecting anomalies, recommending actions, generating code, testing controls, supporting decisions, and orchestrating multi-step workflows. This broad applicability is both the opportunity and the danger. If everything is labeled an AI use case, leadership loses the ability to prioritize, fund, control, and measure what matters.

The strategic issue is therefore not whether an activity can use AI. The strategic issue is whether AI materially improves the work when compared with existing automation, better data governance, process redesign, standard operating procedures, or ordinary analytics. A business process becomes an AI-worthy use case when the work contains enough information complexity, judgment, repeated pattern recognition, language/document burden, exception handling, or decision volume that AI can improve measurable outcomes under acceptable risk and governance.

Recent research and public guidance point in the same direction: AI adoption is broad, but enterprise impact depends on workflow redesign, leadership ownership, data and technology foundations, human validation, governance, and adoption discipline. McKinsey reported that 88 percent of surveyed organizations regularly use AI in at least one business function, but only about one-third report that they have begun scaling AI programs. It also found that high performers are more likely to redesign workflows, define human validation processes, and build practices across strategy, talent, operating model, technology, data, and scaling. [4]

This paper proposes a practical adoption model: classify use cases, score their AI-worthiness, build reusable platforms and governance, pilot only where data and process owners are ready, integrate AI into operational workflows, and measure impact through business outcomes rather than demo activity. Successful AI integration requires more than a model. It requires data access, data quality, secure environments, responsible governance, trained users, operating procedures, funding, system integration, workflow redesign, human accountability, and continuous monitoring.

## Core recommendation

Move from a “use-case list” mindset to an “AI capability portfolio” mindset. A use case should not be approved because it sounds innovative. It should be approved because it has a clear process owner, trusted data, a measurable baseline, a controlled target environment, a defined human-in-the-loop decision point, risk controls, and a path to production adoption.

Strategic question	Recommended answer
Can any process become an AI use case?	Yes. Any process with documents, transactions, decisions, events, knowledge, patterns, exceptions, conversations, or data can be described as an AI use case.
Should every process become an AI project?	No. Many problems are better solved by process cleanup, rules automation, master-data fixes, system integration, training, or standard reporting.
What makes AI integration successful?	A clear business problem, trustworthy data, workflow redesign, secure technical environment, human accountability, governance, adoption support, and measurable outcomes.
What is the highest-value adoption approach?	Start with repeatable, high-volume, evidence-rich workflows where AI can reduce cycle time, improve quality, detect risk, or support decisions without replacing accountable humans.

Table 1. Executive summary of AI integration strategy positions.

## 2. Why Everything Can Look Like an AI Use Case

AI is flexible because modern systems can work with structured data, unstructured text, documents, images, audio, code, workflow logs, and human instructions. That means a meeting can become a summarization use case, a spreadsheet can become an anomaly detection use case, an email inbox can become a triage use case, a policy can become a question-answering use case, and a monthly report can become a narrative-generation use case.

This flexibility creates a catalog explosion. The same process can generate many candidate AI use cases: summarizing the process, extracting data from process documents, predicting the next process event, detecting exceptions, recommending action, drafting correspondence, monitoring controls, creating training material, or producing management dashboards. Without a governance framework, organizations may count these as separate AI wins even when they do not materially improve the work.

### 2.1 A practical definition of an AI use case

For management purposes, an AI use case should be defined as: a repeatable business capability that uses AI to transform specific inputs into useful outputs, embedded in a workflow, controlled by accountable humans, and measured against a baseline outcome.

Element	Definition	Example
Inputs	The data, documents, events, transactions, conversations, images, logs, or instructions the AI uses.	Invoices, contracts, policies, emails, GL transactions, service tickets, meeting transcripts.
AI transformation	The AI task performed on the inputs.	Summarize, classify, extract, match, predict, detect, recommend, generate, translate, code, plan.
Workflow insertion point	Where AI output affects the process.	Before review, during triage, after transaction posting, during audit response, at customer contact.
Human accountability	Who accepts, rejects, edits, overrides, or acts on the output.	Process owner, analyst, manager, auditor, case worker, service representative.
Control and evidence	How the use case is logged, reviewed, validated, secured, and auditable.	Prompt log, output version, data lineage, model version, reviewer approval, exception queue.
Outcome metric	How success is measured.	Cycle time, error rate, backlog, cost, quality, customer experience, risk reduction, revenue.

Table 2. Minimum definition of a governed AI use case.

#### Important distinction

A chatbot demo is not a business capability. A model output is not a business outcome. A pilot is not adoption. AI integration becomes real only when the tool is embedded in a governed workflow and changes how work is performed, measured, and improved.

### 3. AI Integration Adoption Model

AI adoption should be treated as a staged operating model. Organizations move from individual experimentation to managed pilots, then to production workflow integration, and eventually to portfolio-level AI transformation. Each stage requires different controls and leadership actions.

Maturity stage	Typical behavior	Main risk	Leadership action
Stage 0: No AI discipline	Employees use public tools informally or avoid AI entirely.	Data leakage, inconsistent quality, shadow AI.	Publish acceptable-use guidance and approved tools.
Stage 1: Experimentation	Teams test copilots, summarization, drafting, coding, and analytics.	Many pilots, little business value.	Create intake, inventory, risk tiering, and pilot standards.
Stage 2: Managed pilots	Selected use cases have process owners, data sources, success metrics, and risk controls.	Pilots do not scale.	Fund reusable platforms and demand adoption plans.
Stage 3: Production integration	AI is embedded in workflows, systems, approvals, reporting, and exception management.	Operational dependency without sufficient monitoring.	Add model monitoring, SOPs, continuity plans, and audit logs.
Stage 4: AI-enabled operating model	Work is redesigned around human-AI teaming, digital labor, analytics, and continuous improvement.	Governance fragmentation and skill gaps.	Operate AI as a business capability portfolio with executive ownership.

*Table 3. AI integration maturity model.*

Public research supports this staged view. Microsoft’s 2026 Work Trend Index emphasizes that organizations with stronger AI work practices are more likely to have managers who openly use AI, set quality standards for AI work, create space for experimentation, and encourage work redesign. [5] BCG’s 2026 AI Radar similarly describes AI as a CEO-level transformation issue, with corporate AI investment expected to rise and leaders focused on ROI. [6]

## 4. Taxonomy of AI Use Cases Across Business Processes

A practical AI catalog should categorize use cases by the kind of work being changed. This prevents organizations from treating every use case as unique and helps build reusable patterns, platforms, and controls.

Use-case family	AI capability	Business examples
Knowledge and research	Search, summarize, explain, compare, cite.	Policy assistant, legal/regulatory Q&A, technical research, knowledge-base support.
Document intelligence	Extract, classify, validate, transform documents.	Invoice extraction, contract clause review, claims packets, audit evidence indexing.
Workflow triage	Prioritize, route, cluster, recommend next action.	Service tickets, fraud alerts, procurement exceptions, customer complaints.
Anomaly and risk detection	Detect unusual patterns and score risk.	Journal-entry anomalies, payment fraud, cyber alerts, inventory discrepancies.
Prediction and forecasting	Estimate future outcomes or demand.	Cash forecasting, staffing demand, sales forecast, maintenance prediction.
Decision support	Recommend options and explain tradeoffs.	Budget allocation, vendor risk, loan underwriting support, case prioritization.
Content generation	Draft structured outputs from data and context.	Reports, memos, emails, audit narratives, variance explanations.
Code and application support	Generate, review, test, refactor, document code.	Legacy modernization, SQL generation, test case creation, data pipeline support.
Robotic and agentic automation	Plan and execute multi-step tasks across systems.	Close assistant, procurement agent, customer onboarding agent, audit evidence agent.
Monitoring and controls	Continuously monitor processes and produce alerts.	Access reviews, control compliance, exception aging, policy violation monitoring.

Table 4. Reusable AI use-case families.

### 4.1 From business event to AI use case

Every business event can produce several AI candidates. For example, a customer complaint can generate an intake-classification use case, a sentiment-analysis use case, a response-drafting use case, a root-cause clustering use case, a policy-recommendation use case, and a management trend report. A purchase order can generate supplier-risk scoring, price anomaly detection, contract-term extraction, approval-path monitoring, and payment-matching use cases.

Business object or event	Possible AI use cases
Meeting	Agenda generation, live notes, action-item extraction, decision log, follow-up email, risk summary.
Email	Triage, prioritization, sentiment, response draft, attachment extraction, policy matching, escalation.
Invoice	Data extraction, duplicate detection, PO/receipt match, fraud score, payment-term optimization.
Contract	Clause extraction, obligation tracking, risk scoring, price/cost analysis, renewal alert.
Transaction	Classification, anomaly detection, reconciliation, exception queue, root-cause analysis.
Report	Narrative generation, variance explanation, source tie-out, disclosure check, executive summary.
Customer interaction	Intent detection, response guidance, case routing, next-best action, quality review.
System log	Access anomaly, workflow bottleneck, control violation, cyber threat, performance issue.

Table 5. Examples of converting ordinary business events into AI use-case candidates.

## 5. What Must Be True for a Successful AI Use Case

A successful AI use case is not defined by model sophistication. It is defined by sustained business adoption and measurable improvement. In many organizations, the most valuable AI solutions are relatively simple: document extraction, reconciliation, search, summarization, anomaly detection, classification, or drafting. The hard part is making them trusted, governed, integrated, and used.

Success condition	What it requires	Failure signal
Clear problem statement	Specific pain point, process owner, baseline, target outcome.	The use case is described only as “use AI for X.”
Trusted data	Known sources, lineage, quality checks, access rights, update cadence.	Users argue about the data more than the AI output.
Workflow fit	AI output appears at the right decision point in the process.	AI produces interesting results that no one uses.
Human validation	Defined reviewer, threshold, exception process, override policy.	Users copy outputs blindly or ignore them completely.
Technical environment	Secure hosting, integration, monitoring, logging, role-based access.	Pilot runs on ad hoc files, personal accounts, or unmanaged tools.
Governance and risk controls	Risk tier, policy compliance, model validation, security review, audit logs.	Legal, compliance, security, or audit blocks deployment late.
Change management	Training, champions, SOPs, incentives, communication.	Users see AI as extra work or a threat.
Measurement discipline	Baseline, KPIs, ROI method, adoption metrics, quality metrics.	The team reports demos instead of outcomes.

*Table 6. Conditions that distinguish real adoption from experimentation.*

### Adoption insight

The same AI tool can succeed in one organization and fail in another because the difference is usually not the model. The difference is data readiness, workflow design, leadership ownership, user trust, control environment, and whether the organization measures outcomes.

## 6. Data, Resource, Environment, and Process Requirements

AI integration requires a full operating environment. The model is only one component. The organization must prepare the data foundation, resource model, technical environment, process architecture, and workforce support needed to move from idea to production.

### 6.1 Data requirements

- **Authoritative sources:** Identify the system of record and avoid building AI on unofficial spreadsheets when authoritative sources exist.
- **Data lineage:** Track where data originated, how it was transformed, and who approved the transformation.
- **Data quality:** Define accuracy, completeness, timeliness, consistency, validity, uniqueness, and exception thresholds.
- **Metadata and context:** Capture definitions, business rules, owner, sensitivity, update frequency, and retention requirements.
- **Access control:** Apply role-based access, least privilege, need-to-know, privacy controls, and secure handling of sensitive data.
- **Ground truth and labels:** For supervised learning, define reliable historical labels and avoid encoding past bias as future automation.
- **Feedback data:** Capture user overrides, reviewer decisions, corrected outputs, and incident reports so the system improves.

### 6.2 Resource requirements

Resource category	Required capability
Executive sponsor	Owns value, risk appetite, funding priority, and cross-functional alignment.
Business/process owner	Defines the workflow, accepts operational change, and owns final decisions.
Product owner	Manages backlog, user feedback, release plan, adoption, and metrics.
Data owner/steward	Approves data use, data definitions, data quality rules, and access controls.
AI/ML engineer or AI platform team	Builds models, integrations, evaluations, orchestration, and monitoring.
Data engineer	Builds ingestion, transformation, lineage, quality checks, and pipelines.
Cybersecurity and privacy	Approves architecture, identity/access, sensitive data handling, and incident response.
Legal/compliance/risk/audit	Reviews obligations, risk tiering, evidence, controls, and auditability.
Change-management lead	Drives training, communications, adoption, and frontline feedback.

Table 7. Resource model for successful AI use cases.

### 6.3 Environment requirements

The AI environment must be secure, scalable, observable, and integrated. A pilot can run in a sandbox, but production requires identity management, secrets management, API gateways, data-loss controls, model monitoring, version control, logging, and approved deployment pipelines. Federal and regulated organizations should align AI environments with existing cybersecurity, privacy, records, and risk-management requirements. OMB M-24-10 directs federal agencies to advance AI governance and innovation while managing risks, including specific minimum risk-management practices for uses affecting rights and safety. [3]

Environment layer	Minimum requirement
Experiment sandbox	Approved low-risk environment for testing with non-sensitive or synthetic data.
Data platform	Governed access to authoritative datasets, vector stores, metadata, and lineage.
Model layer	Approved models with documented purpose, limits, evaluation results, and usage rules.
Application layer	User interface, workflow integration, APIs, and role-based functions.
Logging and evidence layer	Prompt/input logs, model version, output, reviewer action, timestamp, and audit trail.
Monitoring layer	Quality, drift, latency, hallucination/accuracy checks, security events, and usage/adoption metrics.

Table 8. AI environment layers.

## 7. Governance, Risk, and Control Requirements

AI governance should enable innovation while preventing irresponsible deployment. NIST AI RMF 1.0 organizes AI risk management through Govern, Map, Measure, and Manage functions. NIST’s Generative AI Profile is a companion resource for generative AI risk management and trustworthiness considerations across the AI lifecycle. [1][2] ISO/IEC 42001 provides a management-system approach for organizations developing or using AI systems. [9]

Control domain	Required practice
Inventory	Maintain an AI use-case inventory with owner, purpose, data, model, risk tier, status, and approvals.
Risk tiering	Classify use cases by potential impact on rights, safety, money, mission, legal obligations, reporting, and reputation.
Model evaluation	Test accuracy, robustness, limitations, bias, hallucination, explainability, security, and fit for purpose.
Human oversight	Define human review, approval thresholds, escalation, override, and segregation of duties.
Security	Protect against prompt injection, data exfiltration, model misuse, credential exposure, and unauthorized tool execution.
Privacy and data rights	Minimize data, protect sensitive information, control retention, and disclose appropriate AI use.
Vendor/third-party risk	Review provider terms, data use, subcontractors, model updates, exit strategy, and service dependencies.
Auditability	Preserve logs, evidence, model versions, inputs, outputs, and reviewer actions.
Incident response	Define issue detection, user reporting, containment, rollback, communication, and remediation.
Continuous monitoring	Track drift, quality degradation, user overrides, adoption, errors, and unintended consequences.

Table 9. Governance and control requirements for AI integration.

### Governance principle

AI outputs do not remove human accountability. The business remains accountable for the decision, the process, the customer or stakeholder impact, the evidence, and the consequences of using the AI system.

### 7.1 Special considerations for generative and agentic AI

Generative AI and agentic AI require additional controls because they can produce persuasive but incorrect content, combine data sources in unexpected ways, call tools, and execute multi-step tasks. Agentic workflows should begin with constrained actions, read-only access, limited tools, strong identity controls, approvals before irreversible action, and complete logs. BCG reported that agents already accounted for an estimated share of AI value in 2025 and are expected to represent a larger share by 2028, while McKinsey reported that organizations are already experimenting with AI agents. [7][4]

- Require tool-use permissions by role and by use case.
- Separate “recommend” mode from “execute” mode.
- Use approvals for payments, contract actions, access changes, public communications, and high-impact decisions.
- Keep a complete execution trace: instruction, context, tool call, data used, output, decision, and approval.
- Red-team high-risk agents for prompt injection, unauthorized action, data leakage, and task misinterpretation.
- Create a kill switch and rollback procedure for production agents.

## 8. Step-by-Step AI Use-Case Lifecycle

The following lifecycle converts a broad idea into a controlled AI capability. It is designed to stop weak ideas early and accelerate strong ideas into production.

1. 1. Intake: Capture the proposed use case, business owner, target process, current pain point, expected outcome, affected users, data sources, and risk concerns.
2. 2. AI-worthiness screen: Determine whether the problem truly needs AI or can be solved better by process redesign, rules automation, data cleanup, system integration, or training.
3. 3. Baseline and value case: Measure current cycle time, cost, error rate, backlog, control failure, customer impact, or decision quality before AI.
4. 4. Data readiness assessment: Validate data availability, lineage, quality, access, sensitivity, labels, retention, and update frequency.
5. 5. Risk tiering and governance review: Classify the use case by impact and define required legal, privacy, cyber, model-risk, and audit controls.
6. 6. Solution design: Choose the AI pattern: retrieval assistant, classifier, extractor, prediction model, anomaly detector, recommender, agent, or automation workflow.
7. 7. Prototype with real users: Test with sample data and users, evaluate accuracy, usability, workflow fit, and edge cases.
8. 8. Evaluation and validation: Perform quantitative and qualitative testing, compare against baseline, document limitations, and confirm human-review rules.
9. 9. Pilot in controlled operations: Run the use case in a limited live environment with logs, feedback, and business-owner acceptance.
10. 10. Production deployment: Integrate into systems, SOPs, dashboards, help desk, monitoring, access controls, and training materials.
11. 11. Adoption and change management: Train users, assign champions, update performance expectations, and collect feedback.
12. 12. Continuous monitoring and improvement: Track quality, drift, usage, ROI, incidents, feedback, and future enhancement opportunities.

Gate	Approval question	Exit requirement
Gate 1: Idea to candidate	Is this AI-worthy?	Clear problem, owner, baseline, and expected value.
Gate 2: Candidate to prototype	Are data and risk conditions acceptable?	Data readiness and risk-tier plan approved.
Gate 3: Prototype to pilot	Does the solution work well enough with users?	Validation results, workflow fit, and control design approved.
Gate 4: Pilot to production	Is it safe, adopted, and valuable?	Operational support, monitoring, SOPs, training, and KPI dashboard ready.
Gate 5: Continue, scale, or retire	Does the use case still deliver value?	Periodic review of adoption, quality, cost, risk, and user trust.

Table 10. AI use-case governance gates.

## 9. Metrics, Expected Outcomes, and Value Realization

AI programs often fail to prove value because they track activity instead of outcomes. Counting prompts, pilots, demos, licenses, or models is not enough. Leaders need a value-realization model that connects AI to the organization’s mission and operating results.

Metric type	Examples	Why it matters
Adoption	Active users, repeat usage, workflow completion rate, percent of target users trained.	Shows whether AI is actually used.
Productivity	Cycle time reduction, cases processed per analyst, hours saved, backlog reduction.	Shows efficiency and capacity impact.
Quality	Error rate, rework rate, output acceptance rate, reviewer correction rate.	Shows whether AI improves work quality.
Risk/control	Control exceptions detected, false positives/negatives, audit findings, policy violations.	Shows whether AI strengthens or weakens controls.
Financial value	Cost avoidance, revenue lift, cash acceleration, working-capital improvement, fraud loss prevented.	Shows economic value.
Experience	Customer satisfaction, employee satisfaction, time to answer, first-contact resolution.	Shows human impact.
Model/system health	Latency, uptime, drift, hallucination rate, security events, incident count.	Shows operational reliability.

Table 11. Metrics for AI value realization.

### 9.1 Expected outcomes of successful AI integration

- Faster cycle times for knowledge work, document review, service response, reconciliation, coding, and reporting.
- Higher-quality outputs through consistent review, better evidence, reduced manual error, and stronger exception detection.
- Improved decision confidence through better data synthesis, risk scoring, and scenario analysis.
- Reduced backlog and manual burden in high-volume processes such as case management, audit response, procurement, finance, HR, IT support, and compliance.
- Stronger control environment through continuous monitoring, anomaly detection, and traceable review actions.
- Greater workforce leverage by shifting employees from low-value repetitive tasks to judgment, stakeholder engagement, and remediation work.
- More scalable institutional knowledge through AI-enabled search, training, policy interpretation, and knowledge retrieval.

## 10. Recommended Actions for Leaders

Leadership should treat AI as a business transformation capability, not as an IT experiment. The actions below create the conditions for sustainable adoption.

13. 1. Establish an AI portfolio board: Create a cross-functional board with business, data, IT, cyber, privacy, legal, compliance, risk, audit, and change-management representation.
14. 2. Build a use-case intake and scoring process: Require each proposed use case to pass AI-worthiness, data-readiness, risk, value, and adoption screens.
15. 3. Fund reusable platforms, not one-off demos: Invest in shared data pipelines, approved models, vector stores, logging, evaluation tools, monitoring, and deployment patterns.
16. 4. Prioritize high-value workflow redesign: Focus on workflows where AI can reduce cycle time, improve quality, detect risk, or increase decision confidence.
17. 5. Set human-in-the-loop standards: Define when AI can draft, recommend, triage, decide, or execute; preserve human accountability for consequential actions.
18. 6. Create an AI data readiness program: Treat data quality, lineage, metadata, access, and ownership as adoption prerequisites, not technical afterthoughts.
19. 7. Build AI literacy and role-based training: Train leaders, managers, analysts, auditors, developers, and frontline users differently based on their role and risk responsibilities.
20. 8. Measure impact through business KPIs: Track adoption, productivity, quality, risk, cost, experience, and control outcomes from baseline to production.
21. 9. Create feedback loops: Collect corrections, overrides, user trust signals, incidents, and quality results to improve both AI systems and business processes.
22. 10. Retire weak use cases: Stop pilots that lack data, ownership, measurable value, or adoption. Reallocate resources to stronger use cases.

### Leadership message

The organization should reward responsible work redesign, not just AI usage. The best AI programs ask: What work should humans stop doing? What work should AI assist? What work must humans still own? What new controls are needed? What outcome improved?

## 11. Conclusion

AI adoption has entered a new phase. The question is no longer whether organizations can identify AI use cases. They can identify hundreds or thousands. The harder question is whether those use cases are worthy of investment, integrated into real work, controlled responsibly, trusted by users, and measured against outcomes that matter.

The most important insight is that AI integration is not mainly a technology problem. It is a business design problem. A business process becomes a strong AI use case when the organization understands the process, owns the data, defines the decision point, manages the risk, trains the users, integrates the tool, and measures the result. Without those conditions, AI creates more dashboards, more pilots, more demos, and more unmanaged risk. With those conditions, AI becomes a force multiplier for productivity, quality, control, customer service, decision support, and mission performance.

Therefore, the recommended strategy is disciplined ambition. Be ambitious in recognizing that AI can help almost every process. Be disciplined in approving only those use cases that have clear business value, data readiness, governance, adoption ownership, and measurable outcomes. The goal is not to make every action an AI use case. The goal is to redesign work so people, data, systems, and AI operate together in a safer, faster, smarter, and more accountable enterprise.

## Appendix A. AI-Worthiness Scoring Model

The following model can be used to score and prioritize candidate AI use cases. Each item can be scored from 1 to 5. A use case with low scores in data readiness, ownership, or risk control should not proceed to production even if expected value is high.

Criterion	Score 1	Score 5
Business value	Nice-to-have or unclear benefit.	Directly improves mission, cost, quality, speed, revenue, risk, or customer outcomes.
Process repeatability	One-time task or unclear workflow.	High-volume or recurring workflow with stable steps.
Information complexity	Simple rule-based task.	Requires synthesis of many documents, data sources, patterns, or exceptions.
Data readiness	Data unavailable, poor quality, or uncontrolled.	Authoritative, accessible, well-defined, and quality-controlled data.
Workflow integration	Output has no clear user or decision point.	Output fits directly into an operational decision or action.
Human accountability	No clear reviewer or decision owner.	Named owner accepts/rejects outputs and owns outcomes.
Risk manageability	High-impact use with unclear controls.	Risks are known, tiered, mitigated, and monitorable.
Scalability	One team or one dataset only.	Reusable pattern across units, functions, or processes.

Table 12. AI-worthiness scoring criteria.

## Appendix B. Reusable Use-Case Patterns

Pattern	Description
Policy assistant	Use RAG to answer questions from approved policy, guidance, SOPs, manuals, and regulations.
Document extractor	Extract structured fields from contracts, invoices, claims, forms, applications, and evidence packages.
Exception triage engine	Rank exceptions, alerts, or cases by severity, aging, impact, confidence, and recommended next action.
Anomaly detector	Identify unusual transactions, behaviors, access patterns, payments, journal entries, or system events.
Narrative generator	Draft management summaries, variance explanations, audit narratives, customer responses, or case notes from structured evidence.
Reconciliation assistant	Match records across systems, explain breaks, propose correcting actions, and preserve evidence.
Forecasting model	Predict demand, cost, cash, workload, risk, backlog, supply, inventory, or staffing need.
Quality review assistant	Check completeness, consistency, formatting, policy compliance, and missing evidence before submission.
Workflow agent	Execute constrained multi-step actions such as gathering documents, checking status, drafting correspondence, and routing approvals.
Continuous controls monitor	Watch process logs, data feeds, and system activity for control violations and emerging risk.

*Table 13. Common reusable AI patterns.*

## Appendix C. Source Notes

This paper relies on public guidance and research on AI adoption, governance, and enterprise value realization. References are included for traceability and further review.

- [1] NIST AI Risk Management Framework 1.0. National Institute of Standards and Technology. 2023. <https://www.nist.gov/itl/ai-risk-management-framework>
- [2] NIST AI RMF: Generative AI Profile (NIST AI 600-1). National Institute of Standards and Technology. 2024. <https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence>
- [3] OMB M-24-10: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence. Office of Management and Budget. 2024. <https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf>
- [4] The State of AI: Global Survey 2025. McKinsey & Company / QuantumBlack. 2025. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai>
- [5] 2026 Work Trend Index: Agents, Human Agency, and the Opportunity for Every Organization. Microsoft WorkLab. 2026. <https://www.microsoft.com/en-us/worklab/work-trend-index/agents-human-agency-and-the-opportunity-for-every-organization>
- [6] As AI Investments Surge, CEOs Take the Lead. Boston Consulting Group. 2026. <https://www.bcg.com/publications/2026/as-ai-investments-surge-ceos-take-the-lead>
- [7] Are You Generating Value from AI? The Widening Gap. Boston Consulting Group. 2025. <https://www.bcg.com/publications/2025/are-you-generating-value-from-ai-the-widening-gap>
- [8] AI in Action: Beyond Experimentation to Transform Industry. World Economic Forum. 2025. [https://reports.weforum.org/docs/WEF\\_AI\\_in\\_Action\\_Beyond\\_Experimentation\\_to\\_Transform\\_Industry\\_2025.pdf](https://reports.weforum.org/docs/WEF_AI_in_Action_Beyond_Experimentation_to_Transform_Industry_2025.pdf)
- [9] ISO/IEC 42001:2023 Artificial Intelligence Management System. International Organization for Standardization. 2023. <https://www.iso.org/standard/42001>
- [10] EU Artificial Intelligence Act implementation overview. European Commission. 2024-2026. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>