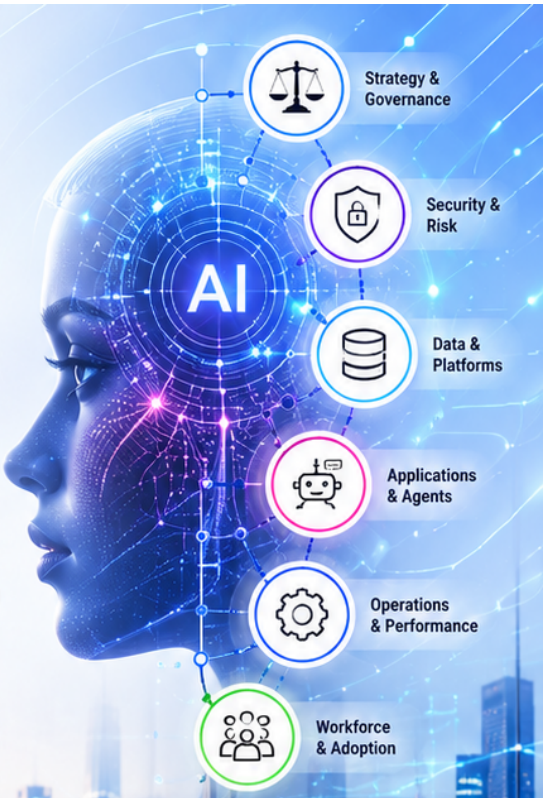
MODERN AI
smart. secure. transformative

# AI READINESS EXECUTIVE ASSESSMENT REPORT

Enterprise maturity, risk, governance, platform, security, applications, operations and workforce readiness




| 71.0% | 3.55 / 5 | Established | 56 |
|---|---|---|---|
| Overall Maturity | Overall Score | Maturity Level | Critical / High Items |

TOP GAP DOMAIN:
**Applications & Agents**

Prepared from
Modern_AI_AI_Readiness_Assessment_Professional_Workbook(5).xlsx

Prepared by
MODERN AI
smart. secure. transformative

Table of Contents



# 1. Executive Summary

**Overall assessment.** The workbook reports an overall AI readiness score of 3.55 out of 5, equivalent to 71.0% and an "Established" maturity level. This indicates that the organization has meaningful foundations in place, but key controls, operating disciplines, and delivery practices are not yet consistently institutionalized across the enterprise.

**Executive interpretation.** The organization appears strongest in Strategy & Leadership and Operations & Scale. The most material readiness gap is Applications & Agents, followed by Security, Risk & Privacy and Talent & Change. Governance, data, and security contain the largest concentration of critical and high-priority assessment items, which means scaling AI without remediation could increase privacy, cyber, regulatory, operational, and reputational exposure.

## Key Executive Findings

| Finding | Business Meaning | Executive Response |
|---|---|---|
| Leadership is comparatively mature | There is a platform to sponsor and fund change, but the supporting data suggests inconsistent execution beneath the headline score. | Confirm ownership, portfolio governance, funding, and board reporting. |
| Applications & Agents is the largest gap | The enterprise may identify AI opportunities faster than it can safely move pilots into production. | Adopt a gated use-case lifecycle with testing, human oversight, permissions, and production criteria. |
| 56 critical/high items are reported | Risk concentration is greatest in strategy, governance, data, and security. | Create a 90-day remediation portfolio with named control owners. |
| Use-case inventory is empty | There is no evidence in the workbook of a prioritized, measurable AI investment portfolio. | Populate and rank the top 10–20 use cases using value, risk, readiness, complexity, and time-to-value. |
| Risk register is empty | Material AI risks are not yet documented, scored, assigned, and tracked in the workbook. | Establish the initial AI risk register before approving new high-impact pilots. |

Recommended executive action: prioritize high-value pilots only after closing material governance, data, security, and operating-model gaps.

# 2. Assessment Scope and Scoring Integrity

The workbook covers seven readiness domains with 15 questions per domain, plus an executive dashboard, gap analysis, AI roadmap, use-case inventory, risk register, and executive report tab. The assessment is therefore broad enough to support executive planning across strategy, governance, data, cyber risk, delivery, operations, and change enablement.

> **Important scoring caveat:** multiple Answer Dropdown cells contain labels such as “6 - Developing”, “10 - Developing”, and “16 - Initial”, although the intended maturity scale appears to be 1–5. The score formulas then extract only the first character, causing values such as 10, 11, or 16 to be interpreted as 1. As a result, the reported 71.0% maturity should be treated as a provisional directional indicator until the response validation and formulas are corrected and the assessment is re-certified.

## Recommended Scoring Remediation

- Restrict all assessment responses to a controlled 1–5 list with one approved description per score.
- Validate that every question has evidence, an accountable owner, and a recommendation before final scoring.
- Recalculate domain scores after invalid response values are corrected.
- Separate priority severity from maturity scoring so that high-priority questions do not distort the maturity scale.
- Obtain executive and control-owner sign-off on the final baseline.

# 3. Enterprise Maturity Dashboard

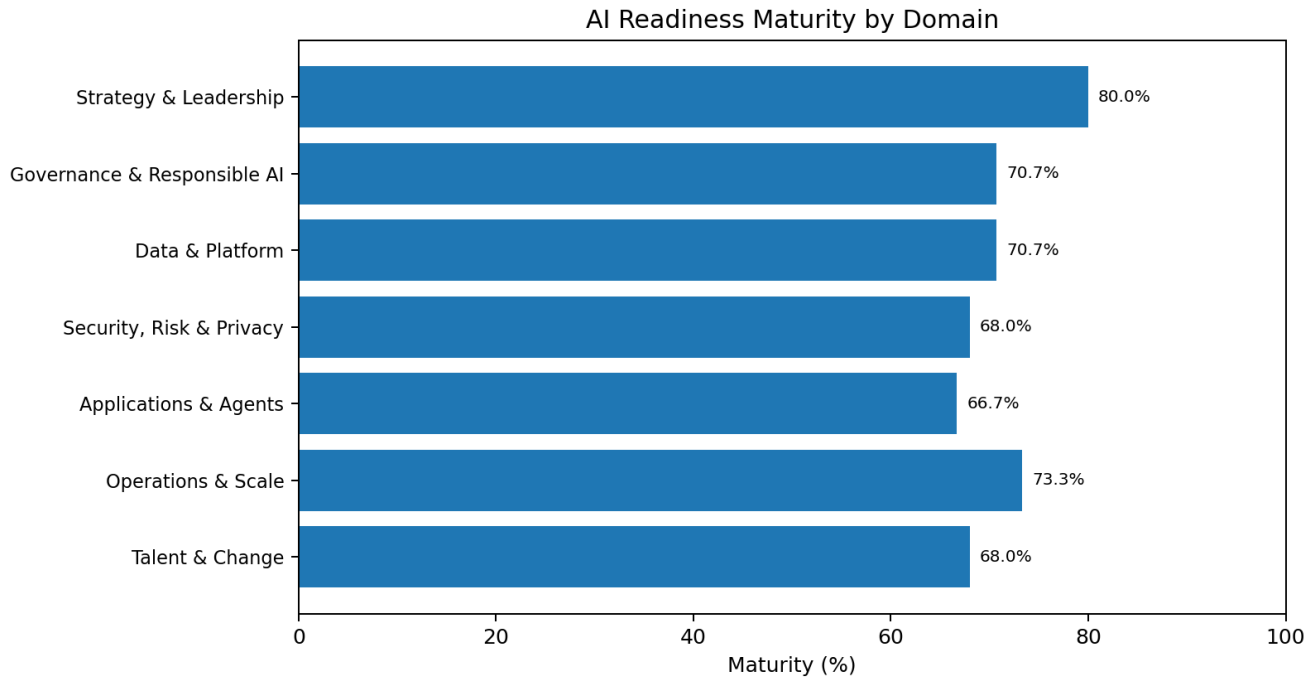



*Figure 1. Reported maturity by assessment domain.*

| Domain | Score | Maturity | Level | Gap | Critical/High |
|---|---|---|---|---|---|
| Strategy & Leadership | 4.00 | 80.0% | Optimized | 0.00 | 15 |
| Governance & Responsible AI | 3.53 | 70.7% | Established | 0.47 | 15 |
| Data & Platform | 3.53 | 70.7% | Established | 0.47 | 11 |
| Security, Risk & Privacy | 3.40 | 68.0% | Established | 0.60 | 15 |
| Applications & Agents | 3.33 | 66.7% | Established | 0.67 | 0 |
| Operations & Scale | 3.67 | 73.3% | Established | 0.33 | 0 |
| Talent & Change | 3.40 | 68.0% | Established | 0.60 | 0 |

The score distribution is relatively narrow, ranging from 66.7% to 80.0%. This suggests broad but uneven readiness rather than a single isolated weakness. Because the underlying response validation is inconsistent, the relative ordering of domains is more useful than the absolute percentages.

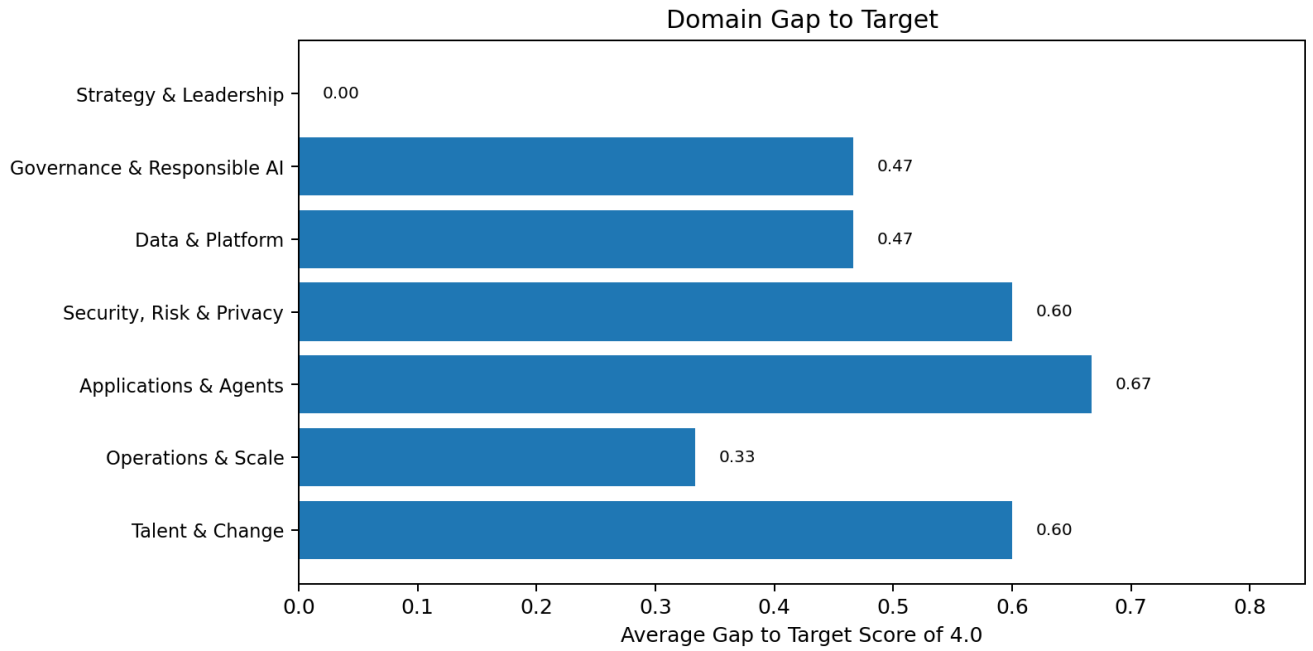



*Figure 2. Average gap to the target score of 4.0.*

# 4. Domain Findings and Business Context

## Strategy & Leadership

**Reported maturity: 80.0% | Reported strength.** The domain reports 80.0% maturity and no average gap to the target. Executive sponsorship, use-case portfolio thinking, value realization, and strategic alignment are therefore positioned as relative strengths.

**Key gap interpretation.** The detailed responses include several invalid values above the 1–5 scale and also show material gaps in enterprise KPIs, innovation pipeline, partner strategy, benchmarking, board reporting, and transformation planning. The headline score may therefore overstate maturity.

**Recommended focus:**

- Confirm a single accountable executive sponsor and AI steering forum.
- Define an enterprise AI portfolio with value, risk, cost, and status reporting.
- Establish board-level AI progress and risk reporting.
- Approve a phased transformation plan and investment model.

## Governance & Responsible AI

**Reported maturity: 70.7% | Established but incomplete.** The domain reports 70.7% maturity with 15 critical/high items. This means governance foundations may exist, but the control environment remains a major enterprise risk concentration.

**Key gap interpretation.** Priority gaps include governance committee effectiveness, policy and acceptable use, risk ownership, model/use-case approval, human oversight, transparency, fairness, regulatory mapping, third-party governance, audit trail, exception management, data-governance alignment, and lifecycle governance.

**Recommended focus:**

- Approve an enterprise AI policy and responsible AI principles.
- Create risk-tiered approval gates for use cases, models, applications, and agents.
- Define human oversight requirements for high-impact decisions.
- Map controls to ISO/IEC 42001 and NIST AI RMF.
- Establish auditability for approvals, exceptions, incidents, and model changes.

## Data & Platform

**Reported maturity: 70.7% | Foundation requires control and architecture.** The domain reports 70.7% maturity and 11 critical/high items. Data availability alone is not sufficient; AI value depends on quality, ownership, classification, access, lineage, integration, and scalable platform patterns.

**Key gap interpretation.** The workbook highlights data inventory, ownership, quality, classification, access, unstructured data, RAG readiness, metadata and lineage, pipelines, vector databases, cloud/hybrid architecture, integration APIs, residency, retention, and scalability.

**Recommended focus:**

- Create an AI data inventory linked to approved use cases.
- Assign data owners and define quality thresholds for AI-critical datasets.
- Implement classification, access, retention, residency, and lineage controls.
- Define the approved RAG, vector-store, API, and integration architecture.
- Assess whether pilot data pipelines can support production scale.

## Security, Risk & Privacy

**Reported maturity: 68.0% | Material control exposure.** The domain reports 68.0% maturity and 15 high-priority items. This is one of the most consequential gaps because AI expands the attack surface across prompts, models, data, APIs, tools, agents, third parties, and human users.

**Key gap interpretation.** The workbook calls for an AI security strategy, threat modeling, prompt-injection defenses, DLP, identity, agent identity, API security, vendor risk, privacy reviews, prompt/action logging, incident response, behavioral monitoring, secure SDLC, encryption, and red teaming.

**Recommended focus:**

- Publish an AI security baseline and reference architecture.
- Threat-model every material AI application and agent.
- Enforce identity, least privilege, tool permissions, API controls, and DLP.
- Log prompts, outputs, actions, approvals, and security events appropriately.
- Extend incident response and red-team testing to AI-specific scenarios.

## Applications & Agents

**Reported maturity: 66.7% | Largest readiness gap.** At 66.7% maturity and a 0.67 gap to target, this is the weakest reported domain. The business risk is a growing portfolio of pilots that cannot be safely operationalized or scaled.

**Key gap interpretation.** Key capabilities include use-case discovery, pilot selection, copilot strategy, agentic readiness, human approvals, workflow integration, testing, user experience, process redesign, knowledge management, permissions, output validation, adoption metrics, reusable components, and a production path.

**Recommended focus:**

- Prioritize use cases with a transparent value-risk-readiness score.
- Use stage gates from idea to pilot, production, scale, and retirement.
- Require human approval for consequential agent actions.
- Validate outputs and test accuracy, safety, security, and user experience.
- Create reusable prompt, connector, API, and agent-control patterns.

## Operations & Scale

**Reported maturity: 73.3% | Promising operating foundation.** The domain reports 73.3% maturity and the smallest non-zero gap. It is a relative strength, but it must be converted into reliable production operations rather than isolated technical practices.

**Key gap interpretation.** Focus areas include MLOps/LLMOps, lifecycle management, deployment standards, observability, drift, cost management, SLAs, change and release management, recovery, performance testing, knowledge transfer, sourcing decisions, continuous improvement, and enterprise scaling.

**Recommended focus:**

- Define a common MLOps/LLMOps operating model.
- Implement monitoring for quality, drift, abuse, reliability, latency, and cost.
- Create release, rollback, support, and incident standards.

- Track token, model, infrastructure, and vendor consumption.
- Develop a repeatable pilot-to-enterprise scaling playbook.

# Talent & Change

**Reported maturity: 68.0% | Adoption risk remains.** The domain reports 68.0% maturity. Without role-based enablement and structured change management, even well-designed AI solutions can underperform because of low trust, misuse, poor process integration, or workforce resistance.

**Key gap interpretation.** The workbook covers AI literacy, role-based training, executive education, skills inventory, change strategy, communications, champions, job impact, feedback, training metrics, responsible use, security awareness, innovation culture, leadership alignment, and sustained enablement.

**Recommended focus:**

- Launch mandatory baseline AI literacy and responsible-use training.
- Provide role-based training for business, technology, security, risk, legal, and executives.
- Assess job and process impacts before scaling deployments.
- Create an AI champion network and user-feedback loop.
- Measure adoption, confidence, productivity, and training effectiveness.

# 5. Cross-Cutting Risks and Gaps

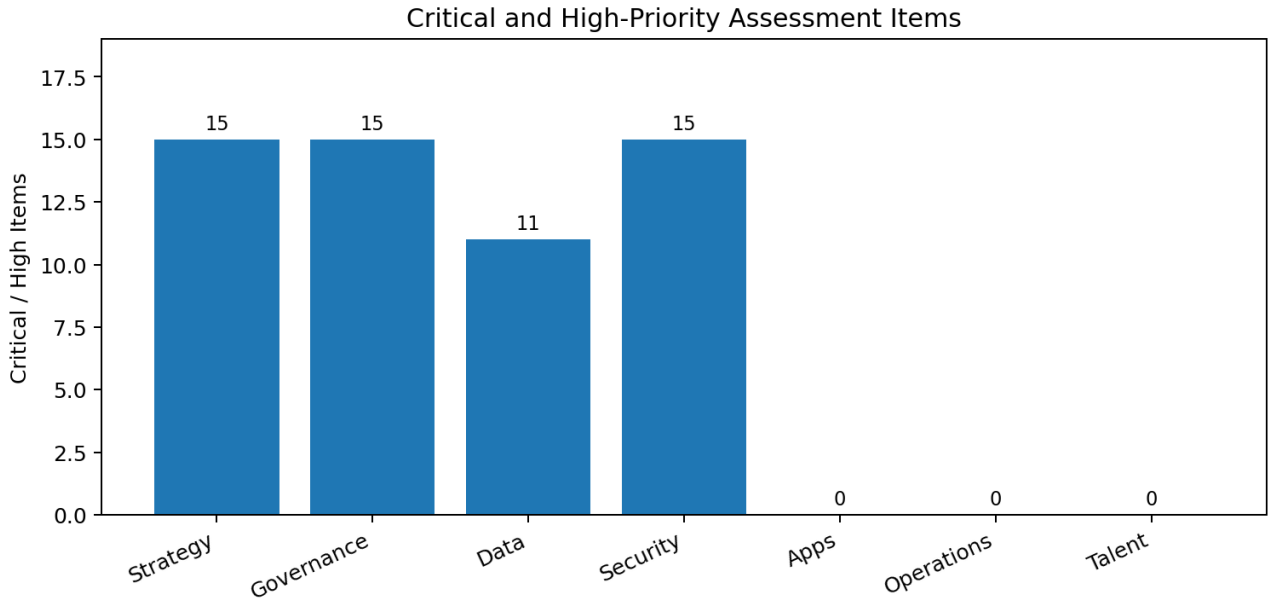



*Figure 3. Concentration of critical and high-priority assessment items.*

| Cross-Cutting Issue | Business Impact |
|---|---|
| **Governance before scale** | Governance, data, and security are the control backbone for safe AI. These disciplines must mature at least as quickly as applications and agent deployment. |
| **Pilot-to-production gap** | Applications & Agents is the largest reported gap, while the use-case inventory is empty. The organization needs a measurable pipeline, not disconnected experiments. |
| **Control ownership gap** | Many owner and recommendation fields are blank. Unassigned gaps are unlikely to close predictably. |
| **Evidence gap** | Evidence/client-notes fields are largely blank. Scores without evidence are difficult to audit, defend, or reproduce. |
| **Risk-management gap** | The risk register contains identifiers but no populated risks. High-impact AI should not proceed without documented inherent risk, controls, residual risk, owner, and status. |
| **Scoring integrity gap** | Invalid answer values undermine confidence in the maturity baseline. Remediation is a prerequisite for executive scorecard use. |

# 6. Use Case and Risk Management Readiness

## Use Case Portfolio

The workbook includes capacity for 40 AI use cases, but the portfolio is currently unpopulated. This prevents the organization from demonstrating where AI investment is concentrated, which initiatives have accountable owners, and how value, complexity, risk, data readiness, security readiness, estimated impact, priority, status, and next steps compare.

Minimum portfolio fields for every proposed use case:

- Business problem, user group, process owner, and expected outcome.
- Quantified value hypothesis: revenue, cost, productivity, quality, experience, or risk reduction.
- Risk tier based on data sensitivity, decision impact, autonomy, external exposure, and regulatory relevance.
- Data and security readiness, architecture pattern, model/vendor choice, and integration dependencies.
- Stage, decision gate, funding, owner, target dates, success measures, and retirement criteria.

## AI Risk Register

The workbook provides 50 risk-register rows but no populated risks. The initial register should include at least privacy and data leakage, prompt injection, insecure tool use, excessive agent permissions, hallucination, bias and unfair impact, explainability limitations, model or vendor dependency, third-party risk, intellectual-property exposure, cyber abuse, weak monitoring, regulatory non-compliance, workforce impact, operational resilience, and uncontrolled cost.

| Risk Theme | Example Scenario | Core Controls | Executive Metric |
|---|---|---|---|
| Sensitive data exposure | Employees submit confidential data to unauthorized AI services. | Approved-tool policy, DLP, classification, access controls, logging. | Unauthorized AI data events |
| Agent overreach | An agent executes a consequential action beyond intended authority. | Unique identity, least privilege, tool allowlists, human approval, transaction limits. | High-risk actions requiring approval |
| Hallucination / error | AI output drives an incorrect customer, operational, or compliance decision. | Grounding, validation, confidence thresholds, human review, monitoring. | Material error rate |
| Adversarial misuse | Prompt injection or malicious content manipulates the model or tools. | Threat modeling, input/output controls, segmentation, testing, red teaming. | AI security incidents |
| Third-party dependency | Vendor model, data practice, outage, or contract change creates exposure. | Due diligence, contract controls, portability, monitoring, exit plans. | Critical vendor exceptions |

# 7. Prioritized Recommendations

| Priority | Recommendation | Primary Owner | Timing | Success Measure |
|---|---|---|---|---|
| 1 | Correct scoring logic and re-baseline the assessment | AI Program / PMO | 0–30 days | Validated 1–5 scoring; executive sign-off |
| 2 | Establish AI governance forum, policy, and risk-tiered intake | Executive Sponsor / Risk / Legal | 0–30 days | Forum active; policy and intake approved |
| 3 | Populate the top AI use cases and select 3–5 priority pilots | Business and Technology Leaders | 0–60 days | Ranked portfolio with owners and value cases |
| 4 | Create the initial AI risk register and remediation plan | CISO / CRO / Privacy | 0–60 days | Material risks scored, owned, and tracked |
| 5 | Approve AI security baseline and reference architecture | CISO / Enterprise Architecture | 0–90 days | Baseline adopted for all new pilots |
| 6 | Implement data and RAG readiness controls | CDO / Data Platform | 30–120 days | Priority data domains meet quality and access thresholds |
| 7 | Adopt application and agent lifecycle stage gates | Product / Engineering / Risk | 30–120 days | All pilots pass design, test, approval, and production gates |
| 8 | Launch role-based AI literacy and change program | HR / Change / Business Leaders | 30–180 days | Training completion, adoption, and confidence targets met |
| 9 | Implement AI monitoring, observability, and cost controls | Operations / Platform | 90–270 days | Quality, drift, risk, latency, and cost dashboards live |
| 10 | Scale only proven use cases with measured outcomes | Executive Portfolio Board | 6–12 months | Benefits realized and risk within tolerance |

# 8. 12-Month Transformation Roadmap

## 0–30 Days: Foundation

- Validate the assessment and correct the scoring model.
- Confirm executive sponsor and AI governance forum.
- Approve acceptable-use policy and AI risk-intake process.
- Inventory AI tools, data sources, active pilots, and vendors.
- Define baseline AI security and data-control requirements.

## 31–90 Days: Prioritize

- Rank the top 5–10 use cases by value, risk, readiness, complexity, and time-to-value.
- Populate the AI risk register and assign mitigation owners.
- Define application and agent lifecycle stage gates.
- Approve target architecture for copilots, RAG, APIs, agents, and monitoring.
- Launch executive, role-based, and responsible-use training.

## 91–180 Days: Build and Prove

- Launch controlled pilots with governance, security, data, and measurement embedded.
- Implement data-quality and RAG-readiness improvements.
- Introduce threat modeling, testing, human oversight, and output validation.
- Establish production support, release, rollback, and incident procedures.
- Measure adoption, productivity, quality, risk, cost, and user experience.

## 6–12 Months: Scale

- Implement enterprise MLOps/LLMOps monitoring and cost management.
- Scale only use cases that meet value and risk thresholds.
- Expand reusable prompts, connectors, APIs, controls, and reference patterns.
- Operate quarterly AI governance, portfolio, risk, and value reporting.
- Refresh the readiness assessment and compare progress against the baseline.

# 9. Executive Decisions and Success Measures

## Decisions Required

- Who is the accountable executive sponsor for enterprise AI?
- What AI risk appetite and prohibited-use boundaries will the organization adopt?
- Which 3–5 use cases receive funding and executive sponsorship first?
- Which enterprise platform, model, integration, and security patterns are approved?
- What evidence is required before a pilot can enter production?
- Which metrics will determine whether an AI investment is scaled, changed, or stopped?

## Recommended Enterprise Scorecard

| Dimension | Illustrative Measures |
|---|---|
| **Value** | Realized savings, revenue, productivity, cycle-time improvement, risk reduction |
| **Portfolio** | Use cases by stage, funded value, time-to-value, stopped initiatives |
| **Adoption** | Active users, frequency, satisfaction, process penetration, training completion |
| **Quality** | Accuracy, groundedness, exception rate, human override, customer impact |
| **Risk** | Open high risks, control exceptions, privacy events, policy violations, residual risk |
| **Security** | Prompt attacks, data-loss events, excessive permissions, vendor findings, incidents |
| **Operations** | Availability, latency, drift, failure rate, support volumes, recovery time |
| **Cost** | Token and model spend, infrastructure, vendor consumption, unit economics |

# Appendix A. Domain Scorecard

| Domain | Score | Maturity % | Reported Level | Target | Gap | Priority Interpretation |
|---|---|---|---|---|---|---|
| Strategy & Leadership | 4.00 | 80.0% | Optimized | 4.00 | 0.00 | Maintain and validate |
| Governance & Responsible AI | 3.53 | 70.7% | Established | 4.00 | 0.47 | Targeted optimization |
| Data & Platform | 3.53 | 70.7% | Established | 4.00 | 0.47 | Targeted optimization |
| Security, Risk & Privacy | 3.40 | 68.0% | Established | 4.00 | 0.60 | Priority remediation |
| Applications & Agents | 3.33 | 66.7% | Established | 4.00 | 0.67 | Priority remediation |
| Operations & Scale | 3.67 | 73.3% | Established | 4.00 | 0.33 | Targeted optimization |
| Talent & Change | 3.40 | 68.0% | Established | 4.00 | 0.60 | Priority remediation |

## Assessment Limitations

This report is based solely on the uploaded workbook. Evidence fields, owners, recommendations, use-case records, and risk-register records are largely unpopulated. Several dropdown values do not conform to the intended 1–5 maturity scale. The report therefore provides an executive interpretation of the workbook's reported outputs and a remediation-oriented action plan; it is not a substitute for evidence-based control testing, stakeholder interviews, architecture review, or legal and regulatory advice.

### Prepared by Modern AI

AI Strategy | Governance | Security | Data | Applications | Operations | Enablement