dAIta

The dAIta Solution

The 2026 AI Trust Playbook for SMBs

The AI Governance Toolkit

A blueprint that leaders are using to win back skeptical teams and customers

7 Templates Inside

1. Trust Framework and Scorecard
2. Vendor/ Tool Security Review
3. Internal AI Use Policy
4. AI Governance Committee Charter
5. High-Impact Use Case Matrix
6. Change Management Communication
7. Feedback Loops & Metrics

INTRODUCTION

dAIta
The dAIta Solution

7 templates to help you roll out AI without losing control

A Practical Framework for Building Trust, Control and Business Value with AI in Small and Medium-Sized Organizations

AI adoption in SMBs often starts without structure. Tools appear in teams before any policy exists, decisions are made without clear accountability, and data is shared without knowing the risks.

Without the right processes, checks and balances, organizations expose themselves to unlimited risks across technical, legal and ethical domains. Outputs may be unreliable and models malfunction, sensitive data may be exposed, results may be biased and foster discriminatory outcomes and organizations may inadvertently violate AI or privacy regulations. The cumulative impact of this is a loss of brand reputation.

This toolkit provides a series of ready-to-use templates for leaders to build governance before problems arise. Each template is lightweight, practical, and designed specifically for small and medium-sized teams in accordance with leading standards including ISO/IEC 42001, NIST AI RMF, EU AI Act, GDPR, CCPA and HIPAA. They are built from the experiences of teams deploying AI across several industries. While designed for SMBs, the tools are useful for all organizations. Followed judiciously, they build trust in your use of AI with your employees, customers and stakeholders.

Areas where this works:

Sectors

Financial Services, CPR, Energy, Manufacturing, TMT, Healthcare

Functions

Finance, Supply Chain, IT, Sales, Operations, Marketing, HR, R&D

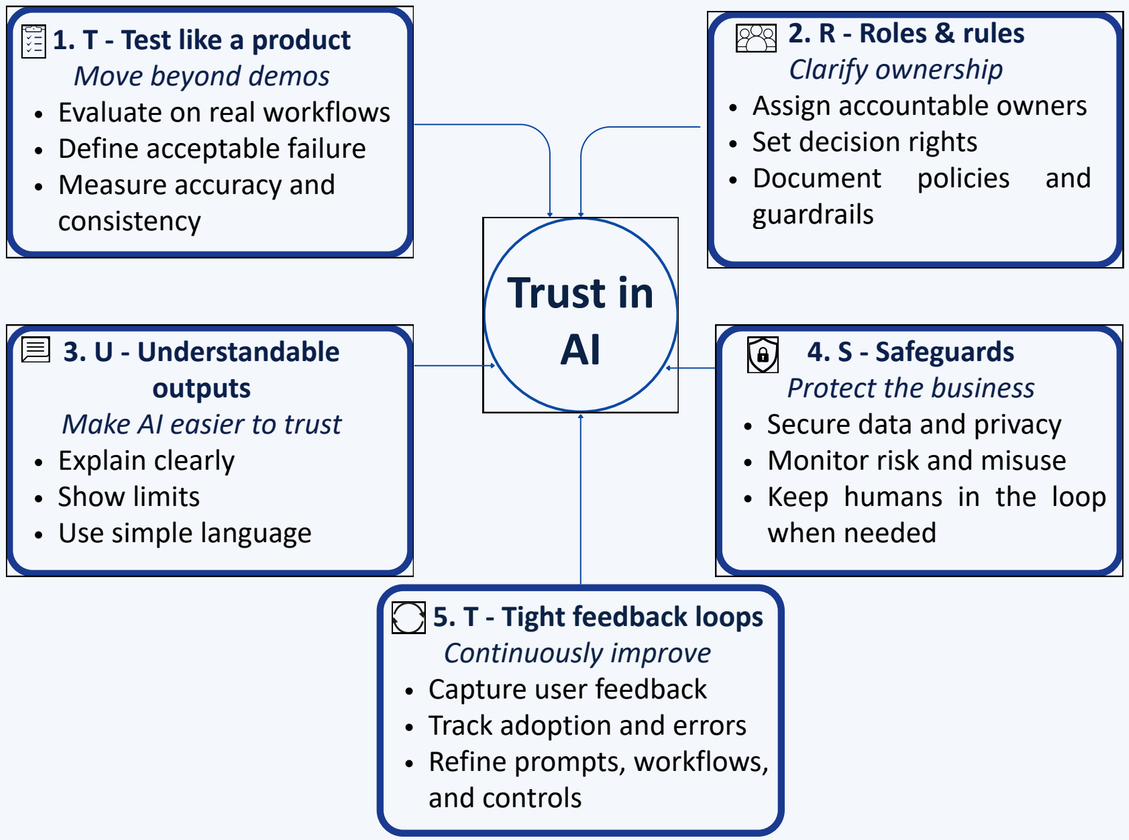
Geographies

North America, LATAM, Asia, Europe, Africa, Middle East

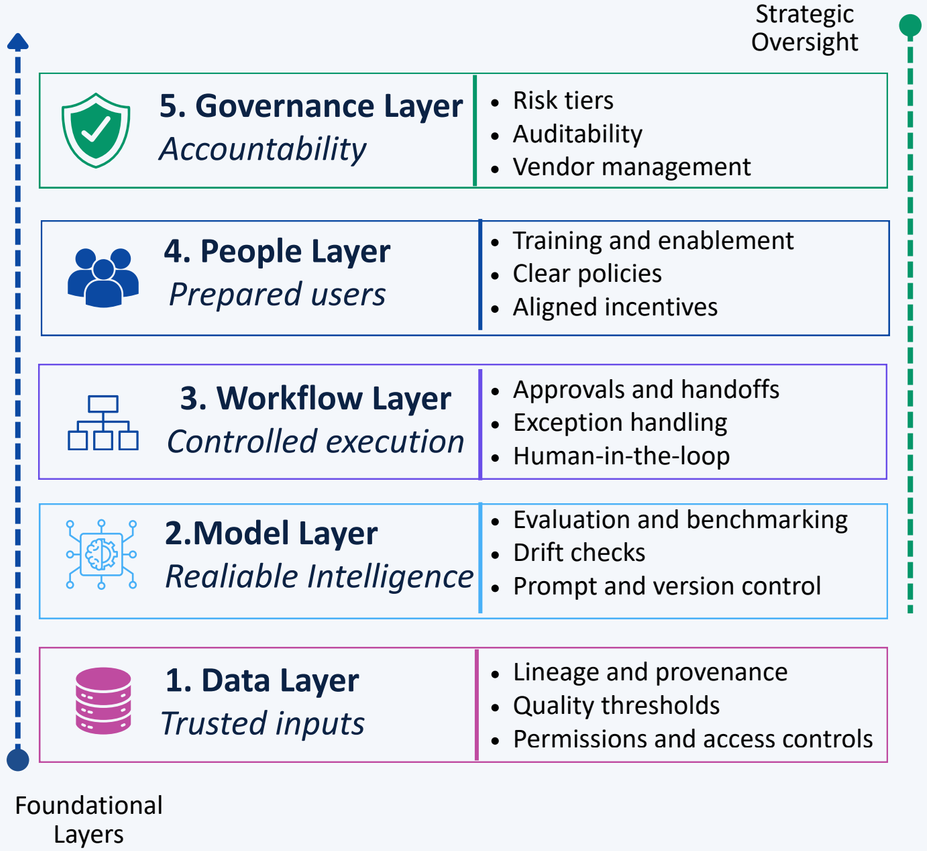
INTRODUCTION

dAIta
The dAIta Solution

The Trust Framework: Building Trust in AI



The Trust Stack for Building Trust in AI



CONTENTS

dAIta
The dAIta Solution

Inside, you'll find step-by-step templates and tools for:

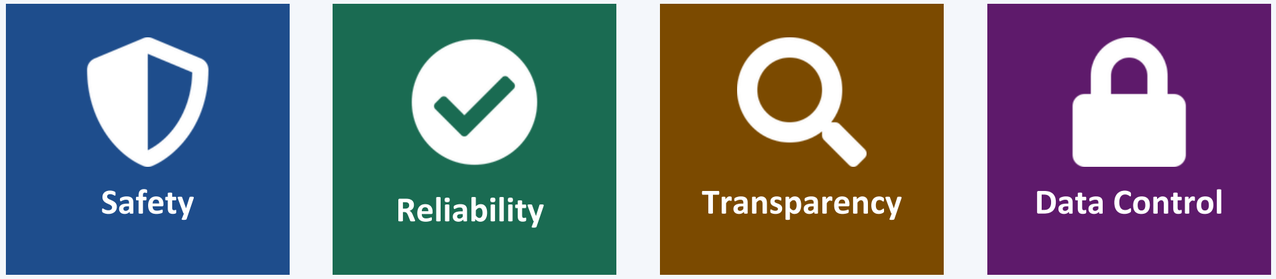
01

Trust Framework & Scorecard

dAIta
The dAIta Solution

Responsible AI starts with trust. That's why this template helps your organization define the fundamental pillars of trustworthy AI, assess your readiness before implementing any tools, identify gaps in trust, and develop an action plan to strengthen oversight, transparency, and trust throughout the organization.

PILLARS OF TRUSTED AI



Protects data, users, and business operations from AI-related risks.

Ensures AI outputs are accurate, consistent, and reviewed.

Clarifies when AI is used and who is accountable.

Defines what data can be used and where it can go.

This template covers:

- ✓ The 4 Pillars of Trusted AI
- ✓ Trusted AI Readiness Checklist
- ✓ The Trust Scorecard (self-assessment)
- ✓ Trust gap identification & next steps

Leads to the Trust Scorecard and Checklist →

TEMPLATE 01

dAIta
The dAIta Solution

Trusted AI Readiness Checklist & Trust Scorecard

READINESS CHECKLIST

- ☐ Our AI tools are inventoried and documented
- ☐ Employees know which AI tools are approved
- ☐ We have a named person accountable for AI decisions
- ☐ Clear owner for the AI workflow
- ☐ Defined purpose + out-of-scope behaviors
- ☐ Approved data sources + access controls
- ☐ Data used in AI is reviewed for sensitivity
- ☐ Security + privacy review completed
- ☐ Evaluation dataset from real work
- ☐ AI outputs are validated before use in decisions
- ☐ Training for users: “How to challenge outputs.”
- ☐ Human fallback and escalation path
- ☐ We have a process to flag AI misuse
- ☐ Monitoring for quality + drift
- ☐ Logging/audit trail
- ☐ Regular review cadence: weekly at first

TRUST SCORECARD

Safety and Security	__ / 5
Transparency	__ / 5
Reliability	__ / 5
Governance and accountability	__ / 5
Regulatory and legal compliance	__ / 5
TOTAL SCORE	**__ / 25**

ACTION STEPS

Identify the two lowest scores. ➡ Assign an owner and due date. ➡ Define one corrective action per gap. ➡ Review progress in the next governance meeting.

02

Vendor/Tool Security Review

dAIta
The dAIta Solution

Before implementing any AI tool, SMEs should understand how the provider handles security, data privacy, regulatory compliance, and user access. This analysis helps teams make informed approval decisions and avoid introducing uncontrolled AI-related risks into the company.

Bake this into your IT approval workflow to flag risks before tools enter your stack.

This template helps you check:

✓ Vendor security and privacy controls

✓ Data retention and model training practices

✓ Compliance requirements and security certifications

✓ Approval status, risk level, and follow-up actions

TEMPLATE 02

dAIta
The dAIta Solution

Data Security Review Checklist

VENDOR OVERVIEW

Vendor Name:

[Insert]

Tool Name:

[Insert]

Submitted By:

[Insert]

Submission Date:

[Insert]

SECURITY & PRIVACY

Does the tool encrypt data in transit and at rest?

Yes No

Are user inputs retained or used to train public models?

Yes No

Is multi-factor authentication (MFA) required?

Yes No

Can the vendor provide a Data Processing Agreement?

Yes No

COMPLIANCE & RISK CONSIDERATIONS

- Is the vendor certified under recognized security standards (e.g., SOC 2, ISO 27001) and compliant with applicable privacy regulations?
- Has the vendor completed a recent independent security audit, and are there any known unresolved security incidents or breaches?
- Does the vendor provide clear documentation on data retention, deletion, and model training practices, including the ability to opt out of data being used for training?
- Does the vendor support appropriate access controls (e.g., role-based access, SSO) and user activity monitoring?
- Where is customer data stored and processed, and can it be exported or deleted at the end of the contract?

APPROVAL TRACEABILITY

Reviewer: Review Date:	Risk Level: Low / Medium / High	Final Decision: Approved / Denied / Approved with Conditions / Follow-up Needed	Required Follow-up Actions: Next Review Date:

03

Internal AI Use Policy

dAIta
The dAIta Solution

AI adoption only works when employees understand what is allowed, what is restricted, and when they need approval. This policy gives SMB teams simple guardrails for using AI responsibly while protecting company data, client information, and business decisions.

✓ DO

- Use approved tools
- Validate all outputs
- Report data concerns

✕ DON'T

- Input client data into public LLMs
- Share unreviewed outputs

This template helps define:

- ✓ Approved and restricted AI activities
- ✓ What data employees can and cannot enter into AI tools
- ✓ Human review requirements for AI-generated outputs
- ✓ How to report misuse, data exposure, or risky AI behavior

TEMPLATE 03

dAIta
The dAIta Solution

Internal AI Use Policy

Policy Title:

[Insert]

Approved By:

[Insert]

Effective Date:

[Insert]

PROHIBITED USE CASES

- ✕ Upload client/proprietary data into public LLMs
- ✕ Rely solely on AI outputs without human review
- ✕ Use unapproved AI tools or browser extensions

ACCEPTABLE USE CASES

- ✓ Draft content or summaries with approved tools
- ✓ Analyze anonymized data on vetted platforms
- ✓ Automate routine internal workflows

Tool / Use Case	Department	Owner	Data Type Used	Risk Level	Approved Users	Approval Status	Last Review	Notes
[Insert]	[Insert]	[Insert]	Public / Internal / Confidential / Personal / Sensitive	Low / Medium				

This registry prevents tool sprawl and gives leadership visibility into which AI tools are being used, who owns them, what data they process, and whether they remain appropriate over time

TEMPLATE 03

dAIta
The dAIta Solution

Internal AI Use Policy

DATA CLASSIFICATION RULES FOR AI USE

Classification Level	Permitted Use	Approval Requirement	Usage Rule
Allowed with Approved Tools	Information that may be used in approved AI tools because it does not contain sensitive, confidential, personal, or proprietary data.	No additional approval required if the tool is already approved.	Employees may use this information in approved AI tools, but outputs must still be reviewed before being shared or used in business decisions.
Allowed Only with Approved and Controlled Tools	Internal business information that may be used only in approved AI tools with appropriate access controls, data protection measures, and business oversight.	Manager or business owner approval may be required depending on the use case. IT/Security review is required if the tool has not been previously approved.	Employees must confirm that the information is anonymized, does not include sensitive data, and is processed only through approved and controlled AI platforms.
Not Allowed Without Formal Approval	Sensitive, confidential, personal, regulated, or business-critical information that must not be entered into AI tools unless formally reviewed and approved.	Formal approval required from IT/Security, Legal/Compliance, and the AI Governance Committee before any use.	Employees must not enter this information into public AI tools or unapproved platforms. Any proposed use must go through a documented risk review and approval process.

TEMPLATE 03

dAIta
The dAIta Solution

Internal AI Use Policy

AI INCIDENT RESPONSE PROTOCOL

⚠ WHEN TO REPORT AN AI INCIDENT

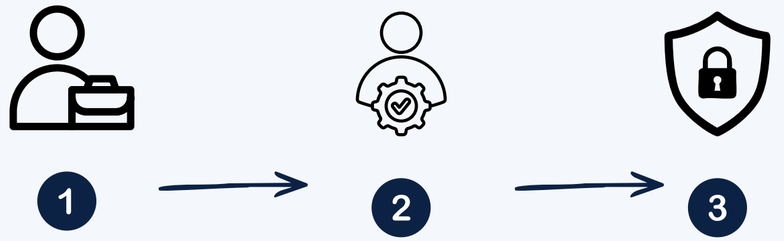
Employees must report immediately if any of the following occur:

- Sensitive data was entered into an unapproved AI tool.
- AI generated inaccurate, harmful, biased, or misleading content.
- A tool produced confidential information unexpectedly.
- A vendor or tool shows signs of unauthorized access.
- An employee discovers unapproved AI use in a business process.

INCIDENT RESPONSE STEPS

1. **Stop using the tool or workflow.**
   Immediately discontinue use of the AI tool or process involved.
2. **Notify the manager and IT/Security.**
   Report the incident as soon as possible.
3. **Capture relevant details.**
   Document the tool used, user involved, date/time, data involved, and the output generated.
4. **Assess the impact.**
   Determine whether customer, employee, or company data was exposed or could be at risk.
5. **Escalate if needed.**
   Escalate to Legal, Compliance, or the AI Governance Committee based on the severity and type of incident.
6. **Define corrective action.**
   Work with the responsible teams to contain the issue and implement corrective measures.
7. **Improve and prevent recurrence.**
   Update policy, training, or approved tool controls to prevent similar incidents in the future.

AI TOOL & USE CASE APPROVAL WORKFLOW



1. **Employee Submits Request**
   To use a new AI tool or use case, including its purpose and business need.
2. **Manager Review**
   Manager reviews the request to confirm business value, alignment with company policies, and initial risk level.
3. **IT/Security and Legal Risk Assessment**
   IT/Security and Legal assess security, privacy, compliance, and data handling risks.
4. **Governance Committee Decision**
   Reviews the assessment and approves, requests changes, or rejects the request.
5. **Use Case Added to Approved Registry**
   If approved, the use case and tool are added to the approved registry, and the requester is notified.

04

AI Governance Committee Charter

dAIta
The dAIta Solution

AI initiatives must have clear accountability; for SMBs, this does not require a large committee or heavy bureaucracy. A small, interdisciplinary team can evaluate tools, manage risks, approve use cases, and ensure that AI adoption aligns with business priorities.

Committee Chair
Strategy lead

IT/Security Lead
Risk & compliance

HR/Change Lead
Training & comms

Business Units
Dept use cases

This helps define:

✓ Who owns AI governance decisions

✓ Which roles should participate in reviews

✓ How tools and use cases are approved

✓ How risks, policies, and ROI are monitored

✓ How often the team should meet

TEMPLATE 04

dAIta
The dAIta Solution

AI Governance Committee Charter

Committee Name:

AI Governance Committee

Established On:

[MM/DD/YYYY]

Review Cadence:

◯ Monthly ◯ Quarterly

MISSION

Guide the safe, practical, and business-aligned use of AI across the organization, ensuring that tools, data, people, and risks are managed with clear accountability.

Area	Responsibility
Tools	Review and approve AI tools before use.
Use Cases	Validate business value, risk, and readiness.
Policy	Maintain AI rules, data guidance, and employee guardrails.
Risk	Monitor incidents, compliance, security, and misuse.
Value	Track adoption, productivity gains, and ROI.

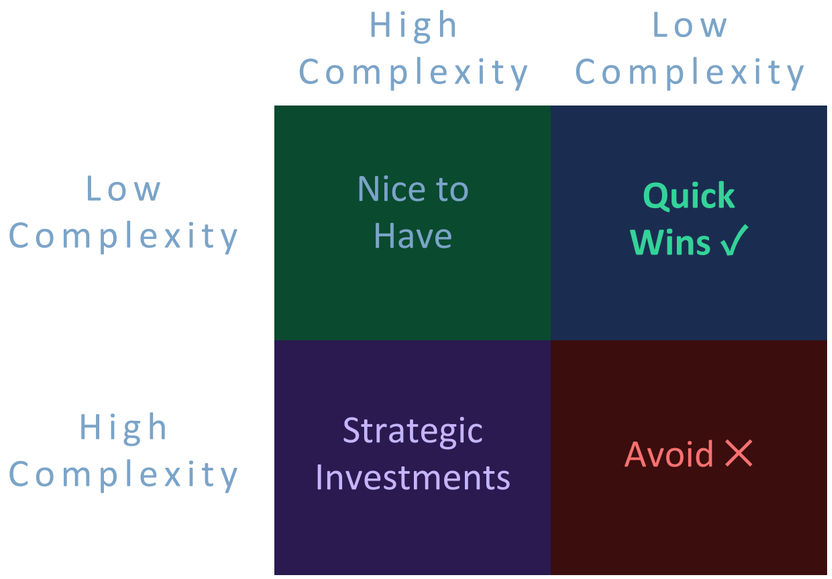
💡 Start with a 3 - 5 person team and expand only as AI adoption becomes more complex.

05

High-Impact Use Case Matrix

dAIta
The dAIta Solution

SMBs should not approve every AI idea at once; that's why this template helps teams compare use cases by business value, effort, risk, and readiness so they can select the right pilots first.



This template helps evaluate:

✓ Expected business value

✓ Implementation effort

✓ Data and technical readiness

✓ Security, privacy, and compliance risk

NEXT STEPS

Use this to align leadership around a prioritized rollout roadmap.

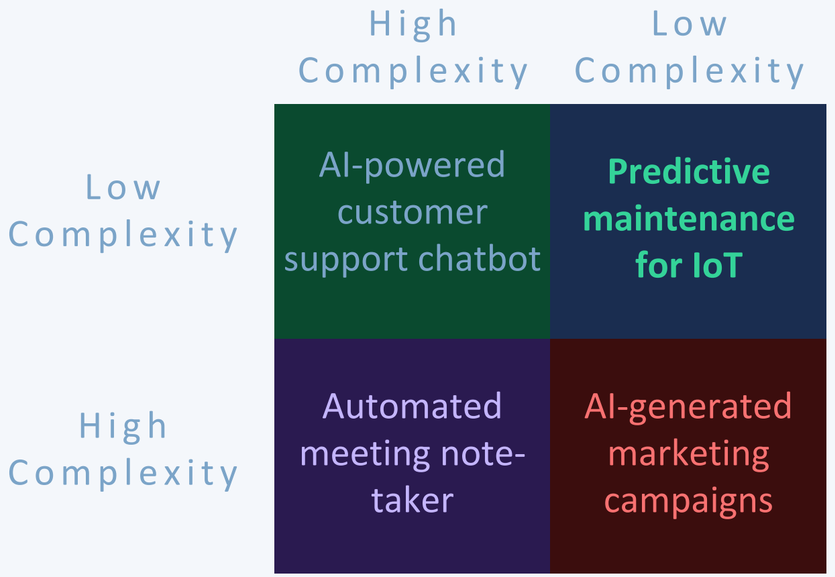
TEMPLATE 05

dAIta
The dAIta Solution

AI Use Case Prioritization Matrix

Score each use case from 1-5 on Business Impact and Implementation Complexity, then plot on the matrix below.

Use Case	Business Impact (1-5)	Complexity (1-5)
AI-powered customer support chatbot	High	Low
Predictive maintenance for IoT	High	High
Automated meeting note-taker	Low	Low
AI-generated marketing campaigns	Low	High
[Your use case here]		



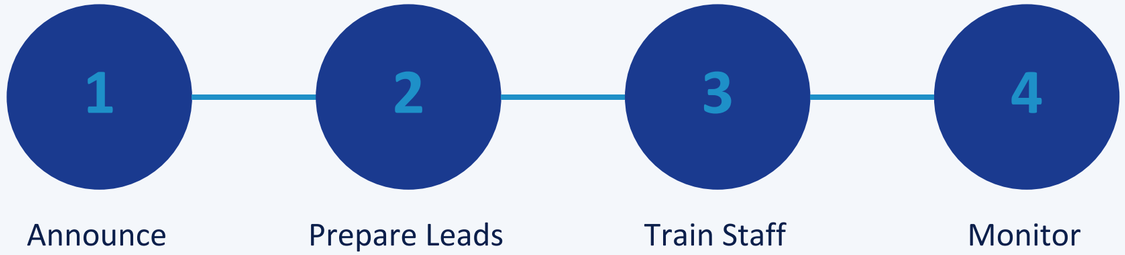
💡 Target 1- 2 low-complexity, high-impact use cases first to build momentum before tackling more ambitious projects. Later, invest in some Strategic Investments as your AI capabilities mature.

06

Change Management Communication

dAIta
The dAIta Solution

Implementing AI isn’t just about rolling out tools; employees must understand why AI is being introduced, how it will change their work, what guidelines they need to follow, and where they can get help. This template helps SMB leaders communicate clearly, reduce uncertainty, and foster confident adoption.



This template helps define:

✓ Rollout announcement email template

✓ Manager talking points guide

✓ Training & ongoing support options

✓ Monitoring adoption & flagging issues

TEMPLATE 06

dAIta
The dAIta Solution

AI Rollout Communication Worksheet

CHANGE MANAGEMENT & TRAINING PLAN

Q1 How will the AI rollout be announced?

☐ Company-wide email
☐ Slack / Teams message
☐ All-hands meeting
☐ Department meetings
☐ Manager briefing
☐ Other: _____

Q2 What should employees understand from day one?

✓ Why AI is being introduced
✓ Which tools are approved
✓ What data cannot be entered into AI tools
✓ When human review is required
✓ Where to ask questions or report concerns

SAMPLE ROLLOUT EMAIL

Subject:

[Company] is introducing AI here's what you need to know

Hi Team,
We are introducing approved AI tools to help teams save time, improve workflows, and support better decision-making.
Before using these tools, please keep three points in mind:

1. Use only approved AI tools.
2. Do not enter sensitive, client, financial, legal, or confidential data unless formally approved.
3. Review AI outputs before using them in business decisions or external communications.

Training and guidance will be provided on [date/time]. Questions can be sent to [contact/channel].

TEMPLATE 06

dAIta
The dAIta Solution

AI Rollout Communication Worksheet

CHANGE MANAGEMENT & TRAINING PLAN

Training options

☐ Quick-start guide for approved AI tools

☐ Live onboarding session

☐ Recorded training session

☐ Short how-to videos

☐ Role-specific examples by department

☐ FAQ for managers and employees

☐ New-hire onboarding module

Manager talking points

Why are we introducing AI?
“We are introducing AI to reduce repetitive work, improve decision-making, and help teams focus on higher-value activities.”

What is expected from employees?
“Use only approved tools, avoid entering sensitive data into public platforms, validate outputs before using them, and report concerns early.”

Where can employees get support?
“Employees can ask questions through [Slack/Teams channel], contact [Responsible Person], or join scheduled office hours.

07

Feedback Loops & Metrics

dAIta
The dAIta Solution

AI governance should improve as employees start using approved tools. This template helps SMBs collect feedback, monitor adoption, identify risks early, and turn real employee input into better policies, training, and tool decisions.

__ %	__ %	$___	____
Adoption Rate	Policy Compliance	ROI Realized	Issues Flagged

This template helps define:

✓ Feedback channels for employees and managers

✓ Questions to identify blockers, risks, and training gaps

✓ Metrics to track adoption, confidence, compliance, and ROI

✓ A use case tracker for new AI opportunities

✓ Action plans to improve governance over time

TEMPLATE 07

dAIta
The dAIta Solution

Feedback Loops & Metrics

01 Feedback Channels

- [ ] Anonymous survey
- [ ] Team retrospectives
- [ ] Slack/Teams channel
- [ ] Quarterly pulse surveys

02 Sample Employee Questions

Q: How comfortable are you using the approved AI tools?
Q: Has AI improved your workflow? How?
Q: What challenges or blockers have you encountered?
Q: Do you understand which AI use cases are approved?
Q: Have you seen unapproved AI tools being used?
Q: What type of AI training would help you most?
Q: Are there workflows where AI could save time but is not yet available?
Q: Do you trust the outputs generated by the approved tools?
Q: Have you found any inaccurate, biased, or confusing AI outputs?

03 Key Metrics to Track

Metric	Target	Current
AI Tool Adoption Rate	>80%	__ %
Policy Compliance Rate	100%	__ %
Reported Issues / Month	<3	___
Approved Use Cases (total)	Growing	___
Employee Confidence Score	>4/5	___

TEMPLATE 07

dAIta
The dAIta Solution

Feedback Loops & Metrics

04
Action Planning

Theme	Action	Owner	Due
Training gap	Create how-to videos	L&D Team	[Date]
Tool misuse	Send policy reminder	IT/Security	[Date]

Who reviews feedback?

AI Governance Committee
Managers and team leads
IT/Security
Legal or Compliance when needed

MANAGER USE CASE TRACKER

Department	Use Case	Description	Tool Used	Status	Notes
Marketing	Drafting content	Generates first drafts for campaigns	Approved LLM	Approved	High adoption
Customer Support	Ticket summaries	Summarizes customer conversations	AI Agent Tool	Under Review	Governance review required
Operations	Forecasting	Supports demand or inventory planning	External API	Proposed	Security vetting required

Review cadence

Weekly during initial rollout
Monthly after rollout
Quarterly for ongoing governance

A Robust Foundation for Long-Term Success

Technology alone doesn't make for a successful AI rollout. The real work happens around it: building the right structures, establishing clear communication, and committing to continuous iteration.

Do you feel confident enough to get started? The Daita Solution helps organizations implement AI and analytics solutions with built-in trust by design.

Schedule a conversation →

Visit us: www.thedaitasolution.com

NEXT STEPS →

dAIta
The dAIta Solution

01 **Use templates as a baseline**

Revisit them as your organization matures

02 **Set quarterly governance checkpoints**

Review metrics with your committee each quarter

03 **Stay aligned with frameworks**

NIST AI RMF, ISO/IEC 42001, GDPR/CCPA