AI Tooling Needs Assessment

Survey + scoring sheets to select AI tools safely and efficiently.

Client: [Your company name]	**Date:** [DD MMM YYYY]
Owner: [Name / role]	**Review cadence:** [Quarterly]

Purpose: capture business use cases, non-negotiable requirements, and a consistent scoring method so teams can compare options.

Outputs: 1) a requirements baseline, 2) a use-case inventory, 3) a weighted scorecard for tool comparison.

How to use this assessment

• Run a 45-60 minute workshop with business leads, IT/security, and a representative user group.

• List 5-10 priority use cases and tag the data sensitivity (public/internal/confidential/regulated).

• Mark requirements as **Must** vs **Should**. Musts are hard gates (fail = no-go).

• Shortlist 2-4 tools, then score them using the same rubric. Capture evidence for each score.

• Pilot the top 1-2 tools with a clear success metric and guardrails before organisation-wide rollout.

Key terms (plain English)

• **SSO (single sign-on):** users log in with your company identity provider.

• **SCIM:** automatic user provisioning/deprovisioning (critical for joiners/leavers).

• **Data residency:** where customer data is stored/processed (region/country controls).

• **Audit logs:** records of access and key actions for investigation and compliance.

• **RAG (retrieval-augmented generation):** the assistant searches approved internal sources and uses them to answer (reduces guesswork).

Decision hygiene

• Treat marketing claims as hypotheses until verified with documentation or a pilot.

• Prefer tools that can enforce policy (data controls, logging, admin settings) over 'trust the user'.

• Design for the exit: data export, portability, and avoiding lock-in where possible.

Must-have requirements checklist

Mark Priority as Must/Should/Could. Mark Result as Pass/Fail/NA. Attach evidence (policy link, contract clause, screenshot).

Category	Requirement	Priority	Result	Evidence / notes
Security	SSO (SAML/OIDC) supported for all users	Must		
Security	Role-based access control (RBAC) + admin console	Must		
Security	SCIM or equivalent automated provisioning	Should		
Security	Audit logs (admin actions + user access) exportable	Must		
Security	Encryption in transit and at rest	Must		
Security	Tenant isolation / customer data segregation	Must		
Privacy	Clear data retention controls (set retention period)	Must		
Privacy	Inputs/outputs not used to train shared models by default (opt-out available)	Must		
Privacy	Supports redaction or data loss prevention (DLP) integrations	Should		
Compliance	SOC 2 Type II and/or ISO 27001 (or equivalent assurance)	Should		
Compliance	DPA available; supports GDPR obligations (incl. sub-processors list)	Must		
Compliance	Data residency options that match our constraints	Must		
Governance	Usage analytics + ability to set policies/guardrails	Must		
Governance	Content filters + configurable safety settings	Should		
Governance	Human approval workflows for automation actions (where relevant)	Should		
Integration	API access for integration/automation	Must		
Integration	Connectors to key systems (email/docs/CRM/ticketing) or webhook support	Should		
Quality	Grounding/citations when using internal sources (RAG)	Should		
Quality	Evaluation tooling: test sets, prompt/version control, rollback	Should		
Legal/IP	Clear IP terms: who owns outputs; indemnities (where possible)	Should		
Operations	Support SLAs, incident reporting, and status transparency	Should		

Non-negotiables (examples): define your red lines here (e.g., no regulated data; no tool without SSO; no unknown sub-processors).

Use case inventory (by team)

Capture the top workflows where AI could help. This prevents buying a tool that is powerful but irrelevant - or relevant but unsafe.

Team	Use case	Inputs (sources)	Outputs	Data class	Volume	Success metric
				Public / Internal / Confidential / Regulated		
				Public / Internal / Confidential / Regulated		
				Public / Internal / Confidential / Regulated		
				Public / Internal / Confidential / Regulated		
				Public / Internal / Confidential / Regulated		
				Public / Internal / Confidential / Regulated		
				Public / Internal / Confidential / Regulated		
				Public / Internal / Confidential / Regulated		

Data sensitivity notes

Public: safe to share externally. Internal: non-public but low risk. Confidential: customer/company secrets. Regulated: personal data, health data, financial data, legal privilege, or sector-regulated content.

Integration and deployment needs

Tick what matters. These answers heavily influence tool choice and implementation effort.

Identity & access	Data & knowledge	Workflow automation
[ ] SSO required [ ] SCIM required [ ] MFA enforced [ ] Separate admin roles	[ ] Internal docs search [ ] Approved knowledge base [ ] File upload controls [ ] Citation/grounding required	[ ] API required [ ] Webhooks [ ] Human approval steps [ ] Action execution (e.g., create ticket)
Integrations (tick)	**Where users work**	**Deployment constraints**
[ ] Email [ ] Chat [ ] Ticketing [ ] CRM [ ] HRIS [ ] Data warehouse [ ] Custom app	[ ] Browser [ ] Desktop app [ ] Mobile [ ] Inside existing tools (e.g., chat/email)	[ ] EU/UK data residency [ ] On-prem / private cloud [ ] Bring your own keys (BYOK) [ ] Network restrictions

Architecture hint

If you need reliable answers from internal policy/process docs, plan for an approved knowledge layer (e.g., curated documents + permissions + citations) rather than relying on generic responses.

Weighted scorecard (compare tools)

1 = poor, 3 = acceptable, 5 = excellent. Multiply by weight and total. Add evidence for each score.

Category	Weight
Security & compliance	30%
Privacy & data controls	20%
Capability fit for use cases	20%
Integrations & extensibility	15%
Admin, analytics, governance	10%
Cost & vendor viability	5%

Tool	Sec/Comp (30)	Privacy (20)	Fit (20)	Integrations (15)	Admin (10)	Cost (5)	Total	Notes / evidence
Tool A								
Tool B								
Tool C								
Tool D								

Pilot checklist: define 2-3 success KPIs; run with a controlled user group; measure quality and time saved; review incidents and policy compliance; decide scale/stop.