TEC+

Generative AI Governance

Readiness Checklist

This checklist helps you quickly assess whether the core building blocks of AI governance are in place for GenAI use (e.g., copilots, chatbots, content generation, analytics assistants). It is designed for practical internal improvement and stakeholder conversations - not as legal advice.

How scoring works (0-2 per item)

Score each item using evidence you can point to (a policy, record, control, or operating practice).

0 = not in place or ad hoc

1 = partially in place / inconsistent

2 = implemented and evidenced

How to use this checklist

1) Pick your top 3 GenAI use cases and score the checklist based on how they operate today.

2) Focus first on any 0 scores in higher-risk areas (customer-facing, HR decisions, regulated contexts, sensitive data).

3) Convert gaps into a 30/60/90 day plan with clear owners and evidence targets.

Interpreting scores (per section)

Each section contains 8 items (max 16 points). As a rule of thumb:

0-6: foundational gaps - prioritise controls before scaling GenAI use.

7-12: developing - stabilise processes, strengthen evidence, and standardise.

13-16: established - maintain assurance cadence and continuous improvement.

Tip: If you want a fast, structured view, score only the items you can evidence today. Anything that is "we usually do this" but cannot be demonstrated should start at 1 at best.

Sections included

- Governance
- Risk management
- Data protection
- Model oversight
- Human oversight
- Vendor management

Ready for a quick baseline?

Book a 30-minute consultation to review your scores, prioritise the top risks, and map out a practical next-step plan for AI governance and data protection (tailored to your tools, use cases, and regulatory exposure).

Reply to the email you received with this checklist or use the booking link on the landing page.

hello@tecplus.co.uk

Governance

Set clear accountability and decision-making for GenAI use. Aim for a small, empowered group that can approve use cases, set standards, and resolve exceptions quickly.

Scoring reminder: 0 = not in place, 1 = partial, 2 = implemented & evidenced.

Checklist Item	0	1	2	Notes
Named executive sponsor for GenAI governance (role + responsibilities documented).				
RACI for AI governance (risk, legal/privacy, security, product/ops, data) agreed and communicated.				
Approved GenAI policy covering allowed tools, data handling, and prohibited uses.				
Inventory of GenAI use cases with owners, purpose, and business value.				
Process for approving new use cases (incl. risk review) is defined and used.				
Controls for shadow AI (monitoring, guidance, and an escalation path).				
Training completed for key roles (product, ops, HR, security, procurement).				
Evidence pack exists for audits/assurance (policies, records, approvals, reviews).				

Risk management

Treat GenAI as a business change with distinct risks (legal, privacy, security, safety, operational). Use lightweight risk assessments early, and deepen controls as impact increases.

Scoring reminder: 0 = not in place, 1 = partial, 2 = implemented & evidenced.

Checklist Item	0	1	2	Notes
Risk taxonomy for GenAI agreed (privacy, IP, security, bias, safety, regulatory, ops).				
Risk assessment method in place (triage for low-risk; deeper for higher-risk).				
Documented risk appetite and decision thresholds (what needs sign-off and by whom).				
Controls mapped to risks (e.g., access control, logging, evaluation, human review).				
Incident response playbook includes GenAI-specific scenarios (leakage, hallucination, harm).				
Testing/evaluation plan for deployed use cases (quality, safety, drift, monitoring).				
Record of periodic reviews (e.g., quarterly) for higher-risk use cases.				
KPIs/metrics tracked (usage, exceptions, incidents, model performance, complaints).				

Data protection

Make data handling explicit: what data goes into GenAI systems, where it goes, how long it persists, and who can access outputs. Prefer privacy-by-design defaults and strong logging.

Scoring reminder: 0 = not in place, 1 = partial, 2 = implemented & evidenced.

Checklist Item	0	1	2	Notes
Data classification rules applied to GenAI use (what can/cannot be input).				
DPIA/AI impact assessment triggers defined (when required, and who leads it).				
Lawful basis and transparency approach documented for relevant use cases.				
Retention and deletion rules defined for prompts, outputs, and logs.				
Access controls enforced (least privilege; MFA; separation of duties where needed).				
Technical controls to reduce data exposure (redaction, pseudonymisation, secure sandboxes).				
Process for handling data subject requests involving AI outputs and logs.				
Cross-border data transfer analysis completed where vendors/processors are involved.				

Model oversight

Know what model(s) you are using, what they are good at, and where they fail. Put repeatable evaluation and monitoring in place, especially for customer-facing or high-impact outputs.

Scoring reminder: 0 = not in place, 1 = partial, 2 = implemented & evidenced.

Checklist Item	0	1	2	Notes
Model register maintained (provider, version, purpose, training data notes, limitations).				
Documented selection criteria (capability, security, privacy, cost, and compliance).				
Prompting/system instructions standardised for key use cases (with version control).				
Evaluation performed before go-live (accuracy, hallucination rate, toxicity/safety checks).				
Monitoring in production (quality sampling, drift detection, incident flags).				
Change management for model updates (release notes, re-testing, approval).				

Human oversight

Define where humans must approve, review, or intervene. The higher the impact, the more explicit and auditable human oversight should be.

Scoring reminder: 0 = not in place, 1 = partial, 2 = implemented & evidenced.

Checklist Item	0	1	2	Notes
Human-in-the-loop points defined for each use case (who reviews what, and when).				
Clear guidance for reviewers (what to check: factuality, bias, privacy, tone, safety).				
Escalation routes for uncertain or high-risk outputs (legal/privacy/security).				
Records kept of reviews/approvals for higher-risk outputs (auditability).				
User experience clearly indicates AI involvement where appropriate (internal/external).				
Controls to prevent over-reliance (training, warnings, and limits on autonomous actions).				

Vendor management

Treat AI vendors like any other critical supplier - plus extra scrutiny for data use, model updates, and safety. Document assurances and align them to your risk profile.

Scoring reminder: 0 = not in place, 1 = partial, 2 = implemented & evidenced.

Checklist Item	0	1	2	Notes
Vendor due diligence questionnaire includes AI-specific topics (data use, training, retention, security).				
Contract terms cover data processing, sub-processors, retention/deletion, and confidentiality.				
Clarity on whether prompts/outputs are used for training and how to opt out.				
Security posture reviewed (SOC2/ISO evidence, pen testing, access controls, logging).				
Model update policy understood (frequency, notice period, rollback, re-evaluation).				
SLAs and support defined for incidents and urgent disable/containment actions.				
Exit plan defined (data export, deletion confirmation, replacing the service).				
Ongoing assurance cadence set (annual review or more frequent for high-risk use).				

Ready for a quick baseline?

Book a 30-minute consultation to review your scores, prioritise the top risks, and map out a practical next-step plan for AI governance and data protection (tailored to your tools, use cases, and regulatory exposure).

Reply to the email you received with this checklist or use the booking link on the landing page.

hello@tecplus.co.uk