AI safety checklist for finance professionals

AI is shifting from “nice to have” to “must-have” in modern finance. From faster board packs to automated reconciliations and scenario forecasting, AI can materially shrink period end and surface value that was previously buried in spreadsheets.

But the same capabilities that make AI powerful also expose finance teams to new risks. Bias in training data can skew outcomes, fabricated/false results can undermine accuracy, and weak security can expose sensitive financial information.

Use this checklist to evaluate AI tools with confidence — ensuring your data stays secure, compliant, and audit-ready.

1. Security

	✓
Verify that the provider follows enterprise-grade encryption standards (for data in transit & at rest).	
Look out for a solution that offers access to AI tools through role-based permissions and multi-factor authentication.	
Regularly audit usage logs to track who is using AI systems and what data is accessed.	
Ensure models are continuously updated with security patches.	

2. Privacy & Data Protection

	✓
Where possible, mask sensitive fields before sending them to any model. Use tokenisation for supplier IDs, account numbers and personal identifiers.	
Look for a solution where your data remains private and never leaves your control.Many AI vendors feed prompts and outputs into external training sets.	
Confirm your AI vendor supports data residency requirements (e.g., DPA, GDPR, CCPA, regional banking laws).	
Validate that the AI provider does not retain or train on your financial data without explicit consent.	
Agree precise retention windows for inputs, outputs and logs. Ensure deletion requests are supported and can be validated.	

3. Compliance & Risk

Conduct a compliance review to align AI usage with the UK Data Protection Act, GDPR, CSRDor other local financial regulations.	
Check that AI outputs can be traced back to their data sources (essential for audit trails and compliance).	
Document everything. If an AI assistant suggests an adjustment, the decision to accept or reject it should be recorded alongside rationale — creating a verifiable audit trail.	
Ensure governance tools allow sensitivity labels to be set to enforce Information security rights management	

4. Proofing & Accuracy

Always verify AI outputs against trusted financial sources before acting.	
Use a tool (like 5Y) that can cleanse inconsistencies, remove duplicate entries, and transform data into a standardised format before analysis	
Train staff to cover responsible prompt engineering, and red flags to watch for in outputs	
Establish policies that require human review for decisions involving external reporting, compliance submissions, or material financial disclosures	

The 5Y Business Transformation Platform centralises your data, embeds governance from day one, and delivers AI-ready insights you can trust.

Request a proof of concept