The AI Compliance Buyer's Checklist

"We're compliant" is not a claim a buyer can evaluate. These are the questions that make it specific. Ask every vendor.

Compliance is now the primary bottleneck in enterprise AI procurement. Security review stalls enterprise deals at least as often as technical fit, usually after the technical evaluation has gone well, and buyers who don't pre-stage it typically lose two to three months in mid-funnel.

78%
of executives lack confidence they could pass an AI governance audit within 90 days (Grant Thornton, April 2026)

74%
of enterprises struggle to balance innovation with security when deploying generative AI (BCG)

2–3
months typically lost in mid-funnel when compliance is not pre-staged

The six questions

1. **Which certifications, and what scope?**
   Names alone aren't enough. Scope and audit dates are.
2. **When was the last audit, and who performed it?**
   Recency and independence both matter.
3. **Do you hold ISO 42001?**
   The AI-specific governance standard, not a general security cert.
4. **How is PCI handled on a live voice call?**
   Real-time redaction, audit trail, segmentation.
5. **What data residency options exist?**
   By region, with specifics.
6. **Can we run our own penetration test?**
   A yes signals confidence. A no is informative.

In 2026, compliance is the gate. The vendor that produces its certification scope and audit dates first usually wins the security review.

Proof the bar is clearable

A Fortune 500 gaming enterprise runs more than **330,000 monthly interactions** on an autonomous AI agent under regulated-industry constraints, meaning PCI compliance for in-game purchases plus AML and KYC handling. It scaled rather than stalled. Compliance depth is a gate that can be passed early when the platform is built for it: Maven holds **15 certifications and assessments**, including ISO 42001, PCI-DSS 4.0 Level 1, SOC 2, HIPAA, and GDPR.