interactions

SECURITY CREDENTIALS CHECKLIST

When evaluating technology vendors, security should never be an afterthought. The growing complexity of AI systems, and the sensitive data they touch, means every organization must be confident their partners meet the highest standards of protection and compliance.

This checklist gives you a practical framework for evaluating a vendor's security practices and confirming they meet essential standards. Check off what's confirmed, flag what's missing, and choose a vendor who can demonstrate real security.

General Security Framework

Strong foundational security practices demonstrate a vendor's commitment to protecting customer data and maintaining operational integrity. These measures ensure that risk management, compliance, and continuous monitoring are built into the organization's DNA, not treated as a checkbox exercise.

- **AICPA SOC 2 type II:** Independent audit verifying the design and effectiveness of security, availability, and confidentiality controls
- **PCI Compliance certification:** Secure storage and handling of credit card data
- **ISO 27001-Aligned Practices (not certified, but stated alignment):** Risk management and asset protection policies consistent with ISO best practices

Technical & Platform Controls

A secure infrastructure requires more than certifications. It demands proactive defense. Vendors should demonstrate mature technical controls that prevent, detect, and respond to threats across systems, applications, and APIs. Continuous testing and automated safeguards ensure vulnerabilities are identified and remediated before they can be exploited.

- **Data Encryption:** At rest and in transit using industry-standard encryption protocols (AES256 / RSA 1024)
- **Role-Based Access Control (RBAC):** Least-privilege access model; Centralized policy enforcement
- **Audit Logging:** Full traceability of user and system actions; Audit logs available for compliance reviews
- **Multi-Factor Authentication (MFA):** Enforced for all access
- **API Security & Rate Limiting:** Authentication via OAuth 2.0; IP whitelisting and request throttling supported

Process & Monitoring

Even the strongest technical defenses need disciplined processes to back them up. Vendors should demonstrate a mature security lifecycle that includes continuous monitoring, prompt incident response, and accountability for every change. Regular assessments and real-time visibility into system health are key indicators of operational resilience and readiness.

- **Annual Security Assessments:** Internal control assessments reviewed at least annually; Covers system integrity, access, and operational safeguards
- **Internal & External Network Penetration Testing:** Regular third-party penetration tests; Findings remediated as part of the security lifecycle
- **Automated system scanning for susceptibility to exploit:** Continuous scanning of both internal and external systems for outdated software, yielding vulnerability to known exploits
- **Automated Software Code Scanning during development:** Continuous scans against OWASP Top 10 and other benchmarks to ensure common vulnerabilities have not been introduced into newly developed code

Data Privacy & Compliance

A trusted vendor should treat data privacy as a core obligation, not an add-on. Look for clear frameworks governing how personal and sensitive information is collected, stored, processed, and deleted. Strong compliance programs demonstrate a commitment to both legal obligations and ethical data stewardship, ensuring transparency and respect for customer rights across every geography.

- **GDPR Compliant:** Comprehensive privacy and data use program facilitating, data subject rights, data processing addendums, technical & operational measures
- **Data Residency Options:** EU-hosted and region-specific data processing available

Documentation & Transparency

Security only builds trust when it's visible. Vendors should provide clear, accessible documentation that demonstrates their security posture, compliance status, and operational safeguards. A transparent partner openly shares certifications, whitepapers, and testing summaries, making it easy for your team to verify claims and assess risk with confidence.

- **Public Trust Center:** Lists certifications, policies, and detailed technical controls
- **Security Whitepapers & Certificates Available on Request:** SOC 2 and PCI reports downloadable or available upon request