Cyber Security Scorecard

Tool Name	**Relevance AI**
Subscription Tier	Pro
Hosting / Deployment	AWS (US, EU, AU), MongoDB Atlas (US, EU, AU), Google Cloud (Global), Microsoft Azure (US, EU, AU)
Data Residency	US, EU or AUS

1. Security Certifications

Certification / Standard	Critical Safeguarding – Minimum	Other – Minimum	Actual / Notes
SOC 2 Type II	Required (≥1 of SOC 2 Type II or ISO 27001)	Recommended(≥1 of SOC 2 Type II or ISO 27001)	• **SOC 2 Type II certified** • Annual audits by independent external auditors • Control self-assessments performed at least annually
ISO 27001 (Information Security)			• Not explicitly mentioned in documentation • Security controls documented but no ISO 27001 certification confirmed
ISO 42001 (AI Management System)	Recommended	Optional	• Not mentioned in documentation
CSA STAR Certification	Recommended	Optional	• Not mentioned in documentation

Section Result: ☐ Meets Critical Requirements ☐ Meets Other Requirements

2. Privacy & Compliance

Control Area	Critical Safeguarding – Minimum	Other – Minimum	Actual / Notes
ISO 27701 (Privacy Information Mgmt)	Recommended	Optional	• Not explicitly mentioned in documentation
GDPR / APPs Compliance Statement	Required	Recommended	• **GDPR compliant** (confirmed) • Australian Privacy Principles (APPs) specific provisions documented • Data subject rights for Australian residents included • Right to access and correction outlined • Complaints process established
Privacy Policy & Data Handling	Public, GDPR/APPs-aligned	Public policy	• Comprehensive privacy policy

			documented • Personal information collection disclosed (contact, account, payment, communications) • Data NOT collected: credit card info, personal health info • Processing purposes clearly defined • Retention policy documented • Data encrypted in transit and at rest
Data Sharing with Third Parties	Restricted & documented	Disclosed	• **Comprehensive subprocessor list provided** (19 categories) • Includes: AWS, MongoDB Atlas, Google Cloud, Microsoft Azure • AI providers: Anthropic, OpenAI, OpenRouter, Perplexity AI, Replicate, Cohere • Third-party agreements include confidentiality and privacy commitments • Vendor management program with annual reviews • Overseas disclosures to UK, EU, US, and Australia • **Data Security Policy does NOT apply to third-party services processing outside platform**

Section Result: ☒ Meets Critical Requirements ☐ Meets Other Requirements

3. Other Compliance

Framework / Standard	Critical Safeguarding – Minimum	Other – Minimum	Actual / Notes
HIPAA (Health Data)	Required if handling health data	Not applicable	• **Personal health information NOT collected** (explicitly stated) • Services not designed for health data processing
UK Cyber Essentials Plus	Recommended	Optional	• Not mentioned in documentation
FedRAMP / IRAP / NIST 800-53	Recommended for government data	Optional	• Not mentioned in documentation • Network and system hardening standards documented based on industry best practices

Section Result: ☒ Meets Critical Requirements ☐ Meets Other Requirements

4. Core Security Controls

Control Area	Guidance	Actual / Notes
AI Model Security & Governance	Confirm controls exist to manage model integrity, bias mitigation, explainability, and governance over model training data and updates.	• **Anthropic explicitly prohibits training on customer data** (contractual) • **OpenAI DPA does NOT explicitly prohibit model training**; allows use of deidentified/aggregated data to "improve systems and services" **HOWEVER OpenAI's Public Commitment (March 2023) says they do NOT use API data to train their models** • AI model providers listed: Anthropic, OpenAI, OpenRouter, Perplexity AI, Replicate, AssemblyAI, Cohere • Customer data processed only for service provision • No model customization on customer prompts/outputs without consent • Risk assessment program includes threat identification and mitigation strategies • **Note:** OpenAI's public documentation states API data not used for training, but DPA language more permissive
API Security	Confirm that APIs are authenticated, rate-limited, encrypted, and monitored for misuse or abuse.	• **Authentication required:** unique username/password or authorized SSH keys • **Encryption:** HTTPS/TLS for all access; AES-256 encryption for data transmission • **Access control:** Role-based access controls (RBAC), least privilege principle • **Monitoring:** Intrusion detection system with continuous network monitoring • Log management tools identify security-impacting events • Remote access via approved encrypted connections only • Unique account authentication for all systems and applications
Data Segregation & Isolation	Confirm that customer or client data is logically or physically isolated to prevent cross-tenant access or leakage.	• **Network segmentation** prevents unauthorised access to customer data • Customer data logically separated by organization account with unique identifiers • Database infrastructure segregated from application servers via firewalls • Separate production and non-production environments • IaaS provider instances isolated through hypervisor layer

		• Production systems access restricted to authorized personnel only • Data classification policy ensures confidential data properly secured
Audit Logging & Monitoring	Confirm that access and system activity are logged, retained, and actively monitored for unusual activity.	• **Log management tool** utilized to identify security-impacting events • System logs aggregated for security monitoring and observability • Audit trails for all data access requests • All physical access to data centers logged and audited • Continuous network monitoring with intrusion detection • Security and privacy incidents logged, tracked, resolved, and communicated • Data center access reviewed at least annually • Periodic access audits with prompt revocation upon employee separation
Secure Development Lifecycle (SDLC)	Confirm secure coding, testing, and change management processes are followed for both AI components and supporting systems.	• **Formal SDLC methodology** governs development, acquisition, implementation, changes (including emergency changes), and maintenance • **Change management:** authorisation, formal documentation, testing, review, and approval required before production • Configuration management procedures ensure consistent deployment • **Security testing:** Penetration testing at least annually with remediation per SLAs • Vulnerability management program for prompt remediation • Code review processes implied through change management controls • System changes communicated to customers and internal users
Third-Party & Supply Chain Risk Management	Confirm that key third-party providers (e.g. cloud, API, or data suppliers) are reviewed regularly and maintain appropriate certifications.	• **Vendor management program** includes: - Critical third-party vendor inventory - Vendor security and privacy requirements - Annual review of critical third-party vendors • **Written agreements** with vendors include confidentiality and privacy commitments • Written agreements with subprocessors impose comparable data protection obligations

		• **Major infrastructure providers:** AWS, MongoDB Atlas, Google Cloud, Microsoft Azure (all with strong security profiles) • **AI providers:** Anthropic (strong data protection), OpenAI (30-day retention, SOC 2 Type II) • Third-party agreements include business need justification for data access • Subprocessor notification mechanisms in place (15-day advance notice)

Section Result: ☒ Pass ☐ Fail

Notes:

- **Key Strength: Strong infrastructure security controls with encryption, access management, and monitoring**
- **Key Concern: OpenAI DPA does not explicitly prohibit model training on deidentified customer data (unlike Anthropic's explicit prohibition) HOWEVER OpenAI's Public Commitment (March 2023) says they do NOT use API data to train their models**
- **Recommendation: If handling sensitive data, consider using only Anthropic models or negotiate additional data protection terms with Relevance AI regarding OpenAI usage**
- **Overall security posture is strong with SOC 2 Type II certification and comprehensive security controls across infrastructure, personnel, and data management**

Scorecard Completed By: James Treleaven **Date: 27/10/2025**

IA INTELLIGENCE ASSIST