Synthetic Users Business Impact Analysis (BIA)

Version: 1.0

Effective Date: 15 February 2026

Owner: Kwame Ferreira, CEO

Approved by: Kwame Ferreira, CEO

1. Purpose

This Business Impact Analysis identifies and evaluates the potential effects of disruptions to Synthetic Users' critical business functions, establishes recovery priorities, and informs the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).

2. Scope

This BIA covers all business functions operated by Synthetic Users, including the SaaS platform, customer support, IT infrastructure, finance, and human resources.

3. Methodology

The BIA was conducted through:

- Interviews with department owners (CEO, CTO, CFO)
- Review of system dependencies and data flows
- Analysis of cloud infrastructure architecture (AWS, Render, Vercel, Cloudflare)
- Review of contractual obligations (SLAs, DPAs) with clients

4. Critical Business Functions

4.1 Impact Assessment

Function	Description	Impact of Disruption	Financial Impact	Reputational Impact	Regulat Impact
SaaS Platform Operations	Core product — AI-powered user research	Clients unable to run studies; direct revenue impact	High	High	Mediun (SLA breach)
IT Infrastructure & Security	Data protection, encryption, access systems	Security exposure; potential data breach	High	Critical	High (GDPR, SOC 2)
Customer Support	Client communication and issue resolution	Degraded client experience; delayed issue resolution	Medium	High	Low
Finance & Billing	Payments, payroll, vendor management	Delayed billing and payroll; cash flow disruption	Medium	Low	Mediun
Human Resources	Staff communication and administration	Employee management disruption	Low	Low	Low

4.2 Recovery Objectives

Function	Priority	RTO	RPO	MTD
SaaS Platform Operations	1	2 hours	15 minutes	8 hours
IT Infrastructure & Security	1	2 hours	15 minutes	8 hours
Customer Support	2	4 hours	1 hour	24 hours
Finance & Billing	3	12 hours	4 hours	48 hours
Human Resources	4	24 hours	12 hours	72 hours

---

5. Critical Dependencies

5.1 Technology Dependencies

Dependency	Function Supported	Failover Strategy	Impact if Unavailable
Render	Application hosting	Failover to AWS direct hosting (RTO: 4 hours)	Platform unavailable
AWS (S3, EC2, RDS)	Data storage, compute, backups	Multi-AZ replication; regional redundancy	Data inaccessible
OpenAI / Anthropic / Google / Meta / Mistral	AI model processing	Multi-provider failover (RTO: 2 hours)	Studies cannot be generated
Google Firebase	User authentication	SSO provider redundancy	Users unable to log in
Cloudflare	CDN, WAF, DNS	DNS failover configuration	Service unreachable

Postmark	Transactional email	Alternative email provider	Notification delays

5.2 Data Dependencies

Data Type	Storage Location	Backup Frequency	RPO	Immutability
Customer study data	AWS S3 (regional)	Continuous	15 minutes	S3 Object Lock (compliance mode)
Database (PostgreSQL)	AWS RDS	Continuous with PITR	15 minutes	Provider-managed
Application configuration	Render	Version-controlled	N/A (IaC)	Git history
Logs	Axiom, PaperTrail	Real-time streaming	Near-zero	Provider-managed

5.3 Personnel Dependencies

- **CTO (Artur Ventura):** Primary owner of disaster recovery execution and infrastructure decisions. Cross-trained backup: senior engineering team.
- **CEO (Kwame Ferreira):** BCP activation authority and external communication. Backup: CFO.
- **CFO (Zumbi Ferreira):** Financial continuity and insurance claims. Backup: CEO.

---

6. Impact Scenarios

6.1 Cloud Platform Outage (Render)

- **Likelihood:** Low
- **Impact:** Platform unavailable to all users

- **Maximum tolerable downtime:** 8 hours
- **Recovery strategy:** Pre-configured AWS failover environment (RTO: 4 hours)
- **Data loss risk:** Minimal — data stored on AWS, not Render

6.2 AI Provider Outage (OpenAI)

- **Likelihood:** Medium
- **Impact:** Study generation unavailable
- **Maximum tolerable downtime:** 6 hours
- **Recovery strategy:** Failover to Anthropic or other configured providers (RTO: 2 hours)
- **Data loss risk:** None — stateless processing

6.3 Cybersecurity Incident (Ransomware / Data Breach)

- **Likelihood:** Low
- **Impact:** Data exposure, service disruption, regulatory notification obligations
- **Maximum tolerable downtime:** 8 hours
- **Recovery strategy:** Incident response plan activation, immutable backup restoration
- **Data loss risk:** Bounded by RPO (15 minutes) and S3 Object Lock compliance mode

6.4 Loss of Key Personnel

- **Likelihood:** Low
- **Impact:** Delayed recovery, knowledge gap
- **Maximum tolerable downtime:** N/A (degraded operations, not outage)
- **Recovery strategy:** Cross-training, documented procedures, infrastructure-as-code

---

7. Findings and Recommendations

1. **Primary risk** is concentrated in cloud provider availability (Render, AWS). Mitigation is in place via multi-provider failover.

2. **AI provider risk** is mitigated by multi-model support across OpenAI, Anthropic, Google, Meta, and Mistral.
3. **Data loss risk** is minimal due to continuous backups, immutable S3 storage, and multi-AZ replication.
4. **Regulatory risk** (GDPR, SOC 2) is managed through documented incident response with 72-hour breach notification.
5. **Personnel risk** is managed through cross-training and documented procedures, though the small team size means key-person risk remains elevated.

---

8. Review

This BIA is reviewed annually, following any significant incident, or when material changes occur to the business or technology environment. Results feed directly into the BCP and DRP.