Synthetic Users Internal Audit Report

Version: 1.0

Audit Period: January 2025 – January 2026

Report Date: 15 February 2026

Prepared by: Artur Ventura, CTO & CISO

Reviewed by: Kwame Ferreira, CEO

---

1. Executive Summary

This report presents the findings of Synthetic Users' annual internal audit, evaluating the design and operational effectiveness of security, privacy, and compliance controls across the organization. The audit was conducted in preparation for the SOC 2 Type II renewal cycle and to satisfy internal governance requirements.

Overall Assessment: Controls are operating effectively with no critical deficiencies identified. Five observations were noted, with remediation actions assigned and tracked.

---

2. Audit Scope

The audit covered the following control domains for the period January 2025 – January 2026:

Domain	Controls Reviewed
Access Control & Identity Management	SSO, MFA, RBAC, access provisioning/deprovisioning, privileged access

Data Protection & Encryption	Encryption at rest and in transit, key management, backup immutability
Network & Infrastructure Security	Firewalls, WAF, IDS/IPS, server hardening, configuration management
Application Security	SDLC, code review, vulnerability scanning, input validation
Incident Response	Detection, containment, notification, post-incident review
Business Continuity & Disaster Recovery	BCP, DRP, BIA, DR testing
Third-Party Risk Management	Vendor assessment, contractual controls, ongoing monitoring
HR & Security Awareness	Background checks, training, code of conduct
Data Management & Privacy	Retention, deletion, GDPR compliance, consent management
Change Management	Change control process, peer review, deployment procedures

3. Methodology

The audit used the following methods:

- **Inspection:** Review of policy documents, configuration screenshots, and system logs.
- **Observation:** Verification of controls in live systems (Sprinto dashboards, AWS console, Google Workspace Admin, Cloudflare, Render).
- **Testing:** Sample-based testing of control operation (access reviews, change records, incident logs, backup restoration).
- **Interviews:** Discussions with CTO, CFO, and engineering team leads to verify understanding and execution of controls.

4. Findings

4.1 Access Control & Identity Management

Control	Status	Evidence
SSO enforced for all corporate and production access	**Effective**	Google Firebase configuration, Google Workspace SSO settings
MFA mandatory for all users	**Effective**	Google Firebase MFA policy, Sprinto compliance dashboard
RBAC with least privilege	**Effective**	Permission system documentation, Render/AWS IAM policies
Access provisioned via SSO — single revocation point	**Effective**	Onboarding/offboarding logs
Semi-annual access rights review	**Effective**	Access review records (July 2025, January 2026)
Privileged access restricted to named individuals with MFA	**Effective**	AWS IAM user list, Render team settings
Access revoked within 24 hours of termination	**Effective**	Sampled 3 terminations — all revoked same day

Observation A-01: Access review documentation could be more structured. Currently maintained in Notion; recommend formalizing the review template for audit trail consistency.

4.2 Data Protection & Encryption

Control	Status	Evidence
TLS 1.2+ for all data in transit	**Effective**	SSL Labs test results (A+ rating), Cloudflare TLS settings

AES-256 encryption at rest	**Effective**	AWS S3 encryption configuration, RDS encryption settings
AWS KMS for key management	**Effective**	KMS key policies, rotation configuration
Secrets stored in encrypted vaults (Render env vars)	**Effective**	No secrets in source code (GitHub secret scanning clean)
Backups immutable via S3 Object Lock (compliance mode)	**Effective**	S3 bucket configuration, Object Lock policy

No observations.

4.3 Network & Infrastructure Security

Control	Status	Evidence
AWS Security Groups restrict traffic to required ports	**Effective**	Security group configuration review
Cloudflare WAF blocks known attack patterns	**Effective**	Cloudflare WAF event logs, rule configuration
No SSH access to production servers	**Effective**	Render service configuration, no SSH keys provisioned
Immutable container deployments	**Effective**	Render deployment logs — containers replaced, never modified
Firewall rules reviewed quarterly	**Effective**	Review records (Q1, Q2, Q3, Q4 2025)

No observations.

4.4 Application Security

Control	Status	Evidence

Documented SDLC with security gates	**Effective**	SDLC policy v1.6, Git commit history
Peer review required for all production changes	**Effective**	GitHub branch protection rules, PR merge records
Automated security scanning (SAST/DAST)	**Effective**	CI/CD pipeline configuration, scan reports
Dependency vulnerability scanning (Dependabot)	**Effective**	Dependabot alerts and resolution logs
Input/output validation via Pydantic schemas	**Effective**	Code review of API endpoints
Cache-Control headers on sensitive pages	**Effective**	HTTP response header inspection

No observations.

4.5 Incident Response

Control	Status	Evidence
Documented incident response plan	**Effective**	IRP v1.1
Severity classification defined	**Effective**	IRP Section 4.1
72-hour GDPR breach notification process	**Effective**	IRP Section 4.5, no breaches reported in audit period
Annual tabletop simulation conducted	**Effective**	Simulation records (2025)
Post-incident review within 10 business days	**Effective**	No major incidents in period; process validated via simulation

Observation A-02: No real security incidents occurred during the audit period to fully validate the incident response process under live conditions. Tabletop simulation was

conducted successfully, but a more complex scenario (e.g., simulated data breach with notification workflow) is recommended for 2026.

4.6 Business Continuity & Disaster Recovery

Control	Status	Evidence
BCP documented with RTO/RPO/MTD	**Effective**	BCP v1.1, BIA v1.0
DRP with multi-provider failover	**Effective**	DRP v1.1
Annual DR exercise conducted	**Effective**	BCP exercise records (2025)
Backup restoration tested	**Effective**	Full rebuild test (November 2025)
Exit/portability plan documented	**Effective**	BCP Section 11

No observations.

4.7 Third-Party Risk Management

Control	Status	Evidence
Third-party risk management policy documented	**Effective**	TPRM policy v1.0
Vendor risk categorization (High/Medium/Low)	**Effective**	Vendor register
DPA in place for data-processing vendors	**Effective**	DPA agreements on file
Annual review of high-risk vendors	**Effective**	Review records for AWS, Render, OpenAI, Anthropic
Subprocessor list disclosed and maintained	**Effective**	Subprocessors page on legal site

Observation A-03: Vendor risk register is maintained informally. Recommend consolidating into a structured register with review dates, risk ratings, and DPA expiry tracking.

4.8 HR & Security Awareness

Control	Status	Evidence
Background checks for new hires	**Effective**	HR onboarding records
Annual security awareness training	**Effective**	Training schedule, completion records (2025)
Employee code of conduct with mandatory acknowledgment	**Effective**	Signed acknowledgments on file
Monthly security focus communications	**Effective**	Email records (January–December 2025)

No observations.

4.9 Data Management & Privacy

Control	Status	Evidence
Data retention schedule documented	**Effective**	Data deletion and retention policy
Data deletion within 30 days of request	**Effective**	No deletion requests received in audit period; process validated
Regional data residency (US, EU, UK, CA)	**Effective**	AWS region configuration
Privacy policy published and current	**Effective**	Privacy policy (updated Feb 2025)

Consent capture via cookie banner	**Effective**	Cookie policy, banner implementation

Observation A-04: Privacy policy last updated February 2025. Should be reviewed and updated to reflect any changes from the past year, particularly around AI subprocessor updates.

4.10 Change Management

Control	Status	Evidence
Change management policy documented	**Effective**	Change management policy
All changes via Git with peer review	**Effective**	GitHub branch protection, PR history
CI/CD pipeline for automated deployment	**Effective**	Render deployment configuration
Rollback procedures documented	**Effective**	Change management policy, Render instant rollback
Emergency change process defined	**Effective**	Change management policy

No observations.

5. Summary of Observations

ID	Domain	Observation	Priority	Remediation	Owner	Target
A-01	Access Control	Access review documentation should be	Low	Create standardized access	Security Lead	Q2 2026

		formalized with structured template		review template in Notion		
A-02	Incident Response	Tabletop simulation should include more complex scenarios (e.g., full breach notification workflow)	Medium	Plan enhanced tabletop exercise for 2026	Security Lead	Q3 2026
A-03	Third-Party Risk	Vendor risk register should be consolidated into structured format	Low	Build formal vendor register with review dates and DPA tracking	Security Lead	Q2 2026
A-04	Data Management	Privacy policy due for annual review	Low	Review and update privacy policy	CEO	Q1 2026

No critical or high-priority findings. All controls audited were found to be operating effectively.

---

6. Conclusion

The internal audit confirms that Synthetic Users' security, privacy, and compliance controls are designed appropriately and operating effectively for the audit period. The organization's control environment is aligned with SOC 2 Type II requirements, GDPR obligations, and documented policies.

The five observations identified are low-to-medium priority improvements that will strengthen the control environment further. Remediation actions have been assigned and will be tracked to completion.

---

7. Approval

Name	Role	Date
Artur Ventura	CTO & CISO	15 February 2026
Kwame Ferreira	CEO	15 February 2026