1. Executive Summary

Standard Notes is a privacy-first, end-to-end encrypted note-taking service. All user data is encrypted on the client before it ever reaches Standard Notes' servers, and the encryption keys are derived from a password known only to the user. The company publishes a detailed privacy policy that limits data collection to the minimum required for account provisioning, billing, and optional analytics, and it discloses the handful of subprocessors it uses (AWS, Cloudflare, Stripe, PayPal, Coinbase, GitHub, ProtonMail).

Four independent security audits have been completed (most recent in 2022) covering server-side penetration testing, cryptographic review, and overall architecture. However, Standard Notes does **not** publicly claim SOC 2, ISO 27001/27017, or other formal compliance certifications on its website.

Overall, the service demonstrates strong technical safeguards (zero-knowledge encryption, open-source code, regular backups, limited data retention) but lacks formal attestations that many enterprise buyers require. The draft scorecard below reflects this mix of robust security controls and missing compliance evidence.

---

2. Scope & Methodology

Item	Description
Target	Standard Notes SaaS platform (web, desktop, iOS, Android) and supporting cloud infrastructure.
Framework Used	*NIST Cybersecurity Framework (CSF)* mapped to *ISO 27001 Annex A* controls – a widely recognized baseline for SaaS security assessments.
Data Sources	Public website (privacy policy, security-audit pages), blog posts, and disclosed third-party audit reports.
Approach	1□ Identify data flows & assets → 2□ Map to regulatory requirements (GDPR, CCPA, HIPAA-relevant controls) → 3□ Align each requirement with NIST/ISO controls → 4□ Evaluate evidence from public disclosures → 5□ Score & recommend remediation.

---

3. Data Handled & Regulatory Landscape

Data Category	What Standard Notes Collects	Legal Basis / Regulation
User-generated content (notes, attachments)	Encrypted on-device; stored ciphertext only.	GDPR Art. 32 (integrity & confidentiality); CCPA §1798.150 (encryption as safeguard).
Account identifiers (email, username)	Required for registration & billing.	GDPR Art. 6(1)(b) (contract); CCPA (personal information).
Payment data	Processed by Stripe/PayPal; not stored by Standard Notes.	PCI-DSS (via subprocessors).

Data Category	What Standard Notes Collects	Legal Basis / Regulation
Analytics	Self-hosted Plausible (IP-anonymised).	GDPR “legitimate interest” – minimal profiling.
Backups (14-day)	Retained for recovery, then deleted.	GDPR storage limitation principle.

Because all note content remains encrypted with a key only the user possesses, Standard Notes is **out-of-scope** for many data-privacy mandates that focus on plaintext processing (e.g., HIPAA). Nevertheless, the collection of email addresses and payment information brings GDPR, CCPA, and PCI-DSS considerations.

---

4. Control Mapping (NIST CSF → ISO 27001 → Observed Evidence)

NIST CSF Function	Sub-Control (example)	ISO 27001 Annex A Ref.	Observed Implementation	Evidence
Identify	Asset Management – inventory of hardware/software	A.8.1.1	Public repo & open-source client binaries listed on GitHub.	—
Protect	Access Control – least privilege	A.9.1.2	Password-derived keys; no server-side decryption.	Privacy policy description of zero-knowledge encryption
	Data Encryption – at rest & in transit	A.10.1.1	End-to-end AES-256 encryption; TLS for transport.	Same as above
	Secure Configuration – hardening of servers	A.12.1.2	Regular server-side penetration tests (2022 audit).	Security-audit page
Detect	Continuous Monitoring – log analysis	A.12.4.1	Limited logging; error reporting only.	Privacy policy notes “no usage analytics”.
Respond	Incident Response – documented plan	A.16.1.1	No public IR plan; but audit reports include “response recommendations”.	Audit summary (2022)
Recover	Backup – periodic & tested	A.12.3.1	14-day encrypted backups, then purge.	Privacy policy statement

---

5. Scorecard (0-5 scale per domain)

Domain	Score	Rationale
Governance & Policies	3	Clear privacy policy & open-source stance, but no published governance framework or SOC/ISO attestations.
Risk Management	3	External audits performed, yet risk register not public.
Data Protection	5	Zero-knowledge encryption, minimal data collection, strong backup deletion.

Domain	Score	Rationale
Identity & Access Management	4	Client-side key derivation; no MFA for account login (optional “private username” mode).
Security Testing	4	Four independent audits (incl. penetration & cryptography) – latest 2022.
Compliance Evidence	2	No explicit SOC 2, ISO 27001, or PCI-DSS certification disclosed.
Incident Response	2	No public IR plan; reliance on third-party audit recommendations.
Overall Maturity	**3.3 / 5**	Strong technical controls, but enterprise-grade compliance attestations are missing.

---

6. Sample Audit Findings & Recommendations

Finding	Severity	Recommendation
Missing formal compliance attestations (SOC 2, ISO 27001)	Medium	Initiate a SOC 2 Type II audit (security & privacy principles) and pursue ISO 27001 certification to satisfy enterprise procurement requirements.
Limited multi-factor authentication (only password-derived key)	Medium	Offer optional TOTP or WebAuthn as second factor for account login; document in security policy.
Incident-Response documentation not public	Low	Publish an IR plan (roles, escalation, communication) and conduct tabletop exercises annually.
Backup retention period (14 days) may be insufficient for some regulated workloads	Low	Provide configurable backup retention (e.g., 30 days) for business customers, with encrypted snapshots.
Sub-processor transparency – list of vendors present but no SOC reports from them	Low	Obtain SOC 2 reports from key subprocessors (AWS, Stripe) and link them in the compliance page.

---

7. Conclusion

Standard Notes delivers a technically solid, privacy-centric SaaS offering with end-to-end encryption, open-source code, and a track record of independent security audits. From a pure security-control perspective the product scores highly, especially in data protection and encryption. The primary gap for corporate adopters is the lack of **formal compliance certifications** (SOC 2, ISO 27001/27017) and a publicly documented governance/incident-response framework.

Addressing these gaps would elevate Standard Notes from a “privacy-focused niche tool” to a **full-stack, audit-ready enterprise solution**, making it attractive to organizations that must demonstrate compliance with GDPR, CCPA, PCI-DSS, and internal security policies.
