WHITE PAPER: The Zero-Data Retention Standard

Architecting Digital Sovereignty for the 2026 Legal Landscape

Prepared By: MitiRisk Engineering Group

Subject: Stateless Orchestration vs. Persistent Storage

Compliance Standard: Inherited SOC 2 Type II / HIPAA / GDPR Sovereign-Native

---

I. Executive Summary

In 2026, the primary liability for a law firm is **"Data Persistence."** Traditional legal SaaS providers operate on a "Stateful" model, where sensitive client data and proprietary legal instruments are stored on third-party servers. This creates a fragmented security perimeter and a "Compliance Tax" that costs the average firm over $50,000 annually in audit overhead.

MitiRisk introduces the **Zero-Data Retention Standard**. By utilizing stateless orchestration, MitiRisk facilitates the creation of complex legal instruments without ever permanently storing the underlying data. The firm retains 100% sovereignty within its own Google Enterprise environment.

II. The Stateless Architecture

Unlike traditional software that acts as a **reservoir** (storing data), MitiRisk acts as a **conduit** (processing data).

The "Ghost" Workflow

1. **Transient Intake:** Client data is received via an encrypted TLS 1.3 connection.
2. **Volatile Memory Processing:** Data is held in **Non-Persistent RAM**. It is never written to a physical disk (SSD/HDD) within the MitiRisk environment.
3. **Sovereign Handshake:** MitiRisk authenticates with the firm's **Google Workspace Enterprise** via OAuth 2.0.
4. **Native Assembly:** The document is assembled using the firm's Google Doc templates.
5. **The Final Purge:** Upon confirmation of the "File Save" to the firm's Google Drive, MitiRisk executes a **Cryptographic Wipe** of the RAM buffer.

Technical Result: Within seconds of document generation, MitiRisk possesses **Zero Knowledge** of the client's identity, assets, or legal instructions.

III. Inherited SOC 2 Compliance

By adopting a stateless, Google-native posture, MitiRisk allows firms to leverage **Inherited Security Controls**.

- **Data at Rest:** All sensitive documents live in the firm's Google Vault, protected by Google's multi-billion dollar security infrastructure.

- **Encryption Sovereignty:** Firms utilize **Google Client-Side Encryption (CSE)**. MitiRisk processes the "logic," but the firm holds the keys. Even under subpoena, MitiRisk cannot produce client documents because it does not possess them.
- **Audit Transparency:** Every action taken by MitiRisk is logged directly into the firm's **Google Cloud Audit Logs**, providing the firm with a central "Source of Truth" for compliance officers.

IV. Security vs. Savings: The Economic Impact

Risk Factor	Traditional Legal SaaS	MitiRisk Sovereign Model
Data Ownership	Third-party managed	**Firm-Owned (Sovereign)**
Storage Risk	Centralized "Honey Pot"	**Distributed/Stateless**
Audit Cost	High (Multi-vendor verification)	**Low (Inherited from Google)**
Exit Strategy	Difficult (Data Migration)	**Instant (Delete MitiRisk API access)**

V. Formal Zero-Data Guarantee

MitiRisk legally and technically guarantees the following:

1. **No Persistent Databases:** MitiRisk does not maintain a database of Client PII.
2. **No Data Mining:** MitiRisk does not analyze, sell, or "train AI" on firm proprietary instruments.
3. **Immediate Deletion:** All session data is purged automatically upon task completion or session timeout (maximum 30 minutes).

Conclusion

The MitiRisk **Zero-Data Retention Standard** is the only logical choice for the modern, risk-averse law firm. It provides the speed of a digital factory with the security of an air-gapped vault plus saving around $50K/yr in audits. By turning the firm’s existing Google infrastructure into a high-speed engine, MitiRisk eliminates the "Compliance Tax" and restores absolute digital sovereignty to the practitioner.
