MitiRisk Security White Paper

Enterprise-Grade "Stateless" Orchestration & Data Sovereignty

Executive Summary

MitiRisk provides a modern alternative to traditional legal document management by utilizing a **Stateless Architecture**. Unlike legacy software that stores sensitive client data on third-party servers indefinitely, MitiRisk orchestrates data in real-time and immediately vaults it into the firm’s own secure Google Cloud. Our system is built exclusively on top of platforms that maintain the gold standard of security: **SOC 2 Type II Compliance.**

---

1. The SOC 2 Type II Standard

A **SOC 2 Type II** rating is an independent audit that verifies a company’s security controls over an extended period (typically 6–12 months). It confirms that a provider doesn't just *have* security policies on paper (Type I), but that they **actively and consistently follow them** in practice.

The MitiRisk system leverages the following SOC 2 Type II certified pillars:

Component	Provider	Compliance Status (2026)	Role in MitiRisk
Foundation	**Google Enterprise Plus**	SOC 2 Type II, SOC 3, HIPAA, GDPR	Document storage, encryption, and e-signatures.
Database	**Airtable Business**	SOC 2 Type II, ISO 27001	Real-time CRM and matter-state tracking.
Payments	**Stripe**	SOC 2 Type II, PCI DSS Level 1	Secure PCI-compliant fee collection.
App Layer	**MitiRisk**	**SOC 2 Type I (Targeted Type II)**	The stateless "Engine" orchestrating the flow.

2. Architectural Security: The "Stateless" Advantage

Traditional CRMs and drafting tools create "data persistence"—they hold your client's Social Security numbers, family details, and asset lists on their servers forever. This creates a massive target for hackers.

MitiRisk eliminates this risk through Statelessness:

- **Transient Memory:** Data is processed in an encrypted "transient" state.
- **Instant Purge:** Once the document is assembled and pushed to your Google Vault, MitiRisk "forgets" the data.
- **No Honeypot:** By not storing a master database of client secrets, MitiRisk is not a target for large-scale data breaches.

---

3. The Google Enterprise Plus "Fortress"

MitiRisk specifically requires the **Enterprise Plus** tier of Google Workspace to unlock these critical legal security features:

- **Client-Side Encryption (CSE):** The firm holds the encryption keys. Google cannot read your documents. MitiRisk cannot read your documents. Only you can.
- **Data Loss Prevention (DLP):** AI-powered rules automatically identify sensitive legal instruments (e.g., Wills) and prevent them from being shared outside the firm's domain.
- **Zero-Trust Access:** Context-aware access ensures that your MitiRisk dashboard is only accessible from firm-approved devices in specific geographic locations.

4. Data Sovereignty & Ethical Compliance

Under the **ABA Model Rules of Professional Conduct (Rule 1.6)**, attorneys have a duty to make "reasonable efforts" to prevent the unauthorized disclosure of client information.

MitiRisk facilitates this by ensuring **Data Sovereignty**:

1. **Ownership:** You never lose control of your templates or client files. They stay in **your** Google Drive.
2. **Audit Trails:** Every movement of a document—from intake to final vaulting—is logged within your Google and Airtable audit logs, providing a clear "Chain of Custody" for every instrument.
3. **Encrypted Payments:** No credit card data ever touches MitiRisk or your firm's servers; it is handled entirely by Stripe's SOC 2 certified infrastructure.

Conclusion

MitiRisk is built for the 2026 threat landscape. By combining the stateless orchestration of MitiRisk with the SOC 2 Type II certified power of Google Enterprise Plus and Airtable, we provide transactional law firms with a system that is as secure as it is efficient.

> **"We don't just secure your data; we ensure you never have to store it where you don't own it."Client**

Privacy & Security FAQ

1. What is "Stateless" Technology, and why is it safer?

Most law firm software acts like a "storage locker" that holds your social security numbers, asset lists, and family details indefinitely. This creates a risk if that software company is ever hacked.

MitiRisk is different. It is "stateless," meaning it works like a high-speed conveyor belt. It processes your information to create your legal documents and then instantly "forgets" the data once the job is done. Your sensitive details are never stored on MitiRisk’s servers long-term.

2. Where is my data actually kept?

Your final legal instruments (Wills, Trusts, Contracts) are stored directly in our firm’s private, encrypted Google Cloud vault. Unlike other firms that store your data on various third-party websites, your information stays within our firm’s direct control at all times.

3. Who has the "Keys" to my files?

We use Client-Side Encryption (CSE). In plain English, this means we have a "digital deadbolt" on your files.

- Google cannot read your documents.
- MitiRisk cannot read your documents.
- Only our legal team has the keys to unlock and view your files.

4. How do I know these systems are trustworthy?

The tools we use (Google, Airtable, and Stripe) are all SOC 2 Type II Certified. This is the "gold standard" of security in 2026. It means independent auditors have verified—over a period of many months—that these companies consistently follow the strictest security and privacy rules in the world.

5. Is my payment information secure?

Yes. We use Stripe to process all payments. Stripe is a world leader in secure payments and is certified to the highest industry standards (PCI Level 1). Our firm never sees or stores your credit card number; it is handled entirely by Stripe's encrypted systems.

Security is our focus.

We have invested in MitiRisk because it allows us to focus on what we do best - a **stateless system** providing expert legal advice while ensuring your data is protected by the **most advanced security architecture available today**.

Component	Provider	Compliance Status (2026)	Role in MitiRisk
Foundation	**Google Enterprise Plus**	SOC 2 Type II, SOC 3, HIPAA, GDPR	Document storage, encryption, and e-signatures.
Database	**Airtable Business**	SOC 2 Type II, ISO 27001	Real-time CRM and matter-state tracking.
Payments	**Stripe**	SOC 2 Type II, PCI DSS Level 1	Secure PCI-compliant fee collection.
App Layer	**MitiRisk**	SOC 2 Type I (Targeted Type II)	The stateless "Engine" orchestrating the flow.

> *"Your legacy is safe with us. We use the most advanced technology so you never have to worry about your privacy."*

IMPORTANT/CONFIDENTIAL: *This document is intended for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential, and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone or reply email and destroy the original message. Thank you.*