

Proven^{DB} | Compliance Vault

ProvenDB Compliance Vault is a cost-effective software solution that provides a tamper-resistant digital store for your critical compliance information. The ownership and creation date of information stored in ProvenDB Compliance Vault can be definitively proven by stringent industry standard cryptography. With ProvenDB Compliance Vault you can be certain that your compliance data will satisfy the most rigorous compliance audit.

ProvenDB Compliance Vault is for all your critical compliance documents:

- Anti-Money Laundering and Counter-Terrorism Financing records.
- Know Your Customer (KYC) documents.
- Board minutes and resolutions.
- Receipts, invoices, and other documents supporting tax claims.
- Credit Reporting Privacy disclosures and activities.
- Contracts, applications, and all materials that form the basis of a financial credit assessment.
- Timesheets and employment records.
- Certifications.
- Personal Information Consents.
- Significant email trails.

www.provendb.com
support@provendb.com

    /provendb

L3, 20 Queen Street, Melbourne VIC 3000, Australia.

How Compliance Vault works



1. Documents are uploaded to the Vault, directly from apps, uploaded from file systems, or forwarded via emails.



2. Digital signatures of the documents are created and stored on an immutable, unhackable public Block-chain.



3. ProvenDB Compliance Vault continually monitors the integrity of the data to detect any attempts at tampering or falsification.



4. You have the proof that your compliance data will satisfy the most rigorous compliance audit.

Features and benefits



Uploads compliance documents via webforms or bulk upload.



Accepts and stores critical email threads.



Integrates with existing application frameworks.



Provides a complete history of document changes.



Proves the ownership of intellectual property.



Enables irrefutable proof of the origin date of uploaded documents.



Performs continual monitoring of data integrity.



Enforces non-repudiation of document contents.



Enables audibility and transparency of all alterations.



Delivers complete tamper detection.



Generates cryptographic certificates confirming data ownership, date of origin, and integrity.

“
The average cost for organizations that experience non-compliance problems is \$14.82 million.
”

Ponemon Institute

(based on an analysis of 53 multinational organizations)

“
The RegTech industry is on the verge of a move from ‘Know Your Customer’ to ‘Know your Data’.
”

KPMG

(RegTech there's a revolution coming.)