

Building the Trust Layer

Article 3: The Business Case for Document Ownership

Ask most organisations why they collect documents and the answer is usually the same.

"We need evidence."

- Evidence that someone is qualified.
- Evidence that a supplier meets regulatory requirements.
- Evidence that an employee has completed mandatory training.
- Evidence that a contractor is insured.
- Evidence that a customer has been verified.

Documents have become the currency of trust. The problem is that every organisation collects, stores and manages its own copy of the same information.

The result is an endless cycle of requests, uploads, downloads, emails, reminders, renewals and duplicate records.

The costs are rarely measured because they are spread across every department.

- Recruitment teams chase CVs.
- Procurement teams chase supplier certificates.
- Compliance teams chase policies.
- HR teams chase qualifications.
- Auditors request evidence that already exists somewhere else.
- Individuals repeatedly upload documents they have already shared dozens of times.

Everyone is working hard. Yet everyone is repeating the same process.

But what if we have been focused on solving the wrong problem? For years, organisations have invested in making document management more efficient.

- Better document repositories.
- Faster workflows.
- Smarter search.
- Artificial intelligence to classify files.

These are worthwhile improvements. But they all assume the same thing - that every organisation needs its own copy of every document.

What if that assumption is wrong?

Let's imagine a different model.

Instead of collecting copies, organisations are granted secure, permission-based access to trusted information owned by the individual or organisation responsible for maintaining it. Here are a few examples:

- A recruiter views a candidate's CV without creating another uncontrolled copy.
- A supplier updates an insurance certificate once, with every authorised customer immediately seeing the current version.
- A regulated professional renews a licence once rather than sending updated copies to multiple employers or clients.
- An auditor is given access to verified evidence instead of requesting documents by email.

The information remains where it belongs. The owner remains in control and everyone else consumes the trusted information rather than managing duplicate copies.

This changes more than efficiency. It changes accountability.

When information exists in one trusted location, organisations spend less time wondering whether they are looking at the latest version.

Audit trails become clearer.

Regulatory evidence becomes easier to demonstrate.

The administrative burden of chasing documents begins to disappear.

Most importantly, trust becomes continuous rather than periodic.

Today, many compliance activities rely on snapshots in time.

A certificate is valid on the day it is submitted.

A qualification is verified during recruitment.

A supplier passes an annual review.

Tomorrow, trusted information could be continuously available, continuously current and continuously auditable.

That represents a very different way of thinking. It is no longer about document management. It is about trust management and the business case is therefore much broader than reducing administration costs. It includes:

- Stronger governance.
- Better cybersecurity.
- Greater operational resilience.
- Improved regulatory compliance.
- Reduced third-party risk.
- Higher-quality data.
- Faster onboarding.
- Simpler audits.

And perhaps most importantly, greater confidence in the information organisations rely upon every day.

Over the past three decades I have watched organisations invest in systems designed to manage information. Perhaps the next generation of enterprise technology will focus less on managing documents and more on managing trust.

That thinking became the foundation for Resolut. Not because organisations need another repository for documents but because the future may depend upon something much more valuable.

Trusted access to trusted information.

A Question to Consider

If ten organisations each store a copy of the same document, which one should be trusted when the information changes tomorrow?

References

- UK General Data Protection Regulation (UK GDPR).
- Information Commissioner's Office (ICO): Guidance on accountability, accuracy and information governance.
- National Cyber Security Centre (NCSC): Guidance on supply chain security and cyber resilience.

Question: If your organisation never needed to store another copy of a document, what would change?