

ECM Technical Integration Guide

**What Document Automation Actually Delivers—and
How to Evaluate Whether a Vendor Can Execute**

*For IT Directors, CIOs,
and Software Architects
at credit unions*

Table of Contents

Introduction	3
What Document Automation Requires	4
1. How Your Core System Keeps Documents Findable	4
How Data Flows Work	4
What Your Vendor Should Know	4
If You Work Through an Intermediary Host	5
2. What Gets Deployed to Staff Workstations	6
A Quick Module Deployment Guide	6
Infrastructure Requirements	6
Module Details	7
3. How Performance Gets Prioritized	8
4. Security Structured for Examination	9
Access Control Structure	9
What Examiners Request	10
5. When APIs Extend Automation	11
How to Evaluate a Vendor	12
Core Compatibility	12
Implementation Model & Resources	12
Performance & Optimization	12
Security & Compliance	12
Support Structure & Response	12
What You Can Expect from Identifi	13
Banking-First Platform Design	13
SaaS Infrastructure Management	13
White Glove Implementation	13
Direct Core Vendor Relationships	13
Support Structure	13
About Identifi	14
Enterprise Content Management (ECM)	14
Workflow Platform	14
Schedule a Discovery Call	14

Introduction

Most credit unions have document management software that isn't delivering what they expected. Staff still print documents because retrieval is too slow to rely on. Compliance teams spend hours pulling files for examiners instead of running queries that return results in minutes. The platform stores everything but changes nothing.

The difference comes down to execution. Platforms work when data flows keep documents findable, when tools deploy where staff actually capture and process documents, when performance matches operational reality, and when security turns exam prep into querying instead of scrambling.

This guide walks through what that execution looks like. You'll learn how to configure overnight data imports so staff can find documents immediately, how to deploy workstation modules to stop paper capture, how to validate performance before training begins, and how to structure security so compliance runs queries rather than manually gathering files.

What Document Automation Requires

ECM platforms fail when institutions treat capabilities as independent features. Fast document retrieval doesn't eliminate paper if staff don't have scanning tools at their workstations. Overnight data imports don't help if retrieval is so slow that staff maintain shadow files. Security controls don't matter if staff can't find documents in the first place.

Document automation requires five capabilities working together: data flows that keep documents findable, workstation tools that eliminate paper at the point of capture, performance fast enough for staff to actually use, security that turns exam prep into querying, and APIs that extend automation when needed.

1. How Your Core System Keeps Documents Findable

Loan officers spend time hunting for documents instead of meeting with members. They search through network folders organized by someone else's logic, ask operations where files are stored, and request rescans of documents that already exist. This happens when document indexes in your ECM don't reflect current account data in your core system.

When loans close, account numbers change. When loans transfer to different officers, ownership changes. If your ECM doesn't know about these changes, staff can't find what they need, even though the documents exist.

Keeping documents findable requires your ECM to stay synchronized with your core through overnight data imports that update indexes before branches open. When this works, staff pull up member accounts and immediately see loan documents, signature cards, and account history.

How Data Flows Work

File formats are standardized by core provider. All Jack Henry Symitar customers use the same format, all Fiserv DNA customers use the same format, all COCC customers use the same format. Vendors with actual core experience already know your format and shouldn't need to figure it out during implementation.

Here's what you actually configure during setup:

TRANSFER FREQUENCY

Daily batch files work for most institutions—overnight imports update indexes before branches open the next morning. Hourly updates make sense when operations require same-day availability for loan closings or account openings during business hours.

FIELD MAPPING

Your core has standard fields (account number, loan type, customer name) and custom fields you've added over time. Map custom fields to your ECM's metadata structure during setup so they populate automatically.

INTERMEDIARY COORDINATION

If your core infrastructure is managed by CGI, Jack Henry, or another intermediary host, coordinate SFTP permissions, IP addresses, and firewall rules across all parties before implementation begins. Multi-vendor coordination causes most implementation delays.

What Your Vendor Should Know

Jack Henry (Symitar and Episys)

- Permission structures vary between installations
- Batch job coordination requires understanding overnight processing schedules
- Direct relationships require separate SFTP setup and permission configuration
- Intermediary hosting arrangements affect connectivity timelines and security requirements

Fiserv (DNA, Signature, Premier)

- DNA provides pre-built reports through Fiserv that feed document indexing and retrieval
- Signature requires hybrid approaches based on operational requirements
- Custom field mapping requires coordination across teams

FIS, Temenos, Core10, Corelation

Data transfer happens through batch files. Identifi maintains direct relationships with Corelation and COCC, streamlining connectivity setup through established processes.

If You Work Through an Intermediary Host

Core hosts like CGI or Jack Henry that manage infrastructure for multiple institutions introduce additional coordination layers. IP address conflicts require multi-party resolution. SFTP permission changes affect multiple vendors. Firewall updates involve three parties instead of two.

Identifi handles these coordination requirements, even when resolution involves working with multiple vendors.

Validate Before Staff Training

Before training begins, check that the data imports are configured correctly by testing these workflows:

- **New loan workflow:** Close a test loan in your core system and make sure the loan documents appear in ECM the next morning, with correct account linkage and metadata populated.
- **Account update workflow:** Transfer a loan to a different officer in your core system and verify document ownership updates in ECM overnight.
- **Search accuracy:** Have staff search for accounts by account number, member name, and loan type, then confirm that the results match what's currently in your core.

If these tests fail, data imports aren't configured correctly and need adjustment before staff training begins.

Red Flags in Vendor Responses

Vendors who claim they'll figure out your core's format during implementation.

File formats are already standardized by the core provider, which indicates limited experience.

Vendors who can't provide references from institutions for your specific core product.

If they say they support Jack Henry but can't name Symitar customers, they don't work with your platform regularly.

Vendors who describe every institution as unique when formats demonstrably aren't.

This means they may treat your implementation as custom, which would increase costs and delay deployment.

2. What Gets Deployed to Staff Workstations

Staff continue to print documents even after ECM implementation because scanning tools are located in the back office rather than where documents originate. Tellers capture signatures during account opening, then print them for batch scanning later. Loan officers collect documents at closings and route them to operations for processing. Paper persists because using ECM creates more friction than printing.

Stopping paper capture requires deploying client modules directly to workstations where signatures are captured, loan documents are scanned during closings, and receipts are processed. When scanning tools, signature capture, and receipt processing sit where staff work, documents are routed to ECM immediately instead of flowing through paper.

A Quick Module Deployment Guide

Staff Activity	Deploy	How It Eliminates Paper
Capturing signatures during account opening	eSign	Routes signed documents directly to ECM, eliminating printed signature cards
Scan loan documents during closings	eSign + Scan	Routes documents to member files immediately during appointments
Processing core-generated receipts	eReceipt	Routes receipts to member accounts automatically, no manual filing needed
Handling mail and back-office documents	Uplink + MFP access	Enables batch scanning without disrupting frontline operations

Infrastructure Requirements

Before purchasing an ECM, make sure your environment supports:

- Windows 64-bit across all workstations where staff will scan or sign documents
- Microsoft .NET Framework and Visual Studio C++ Redistributable
- Ability to configure antivirus exclusions before installation
- Network bandwidth to support branch locations (modules cannot be installed via RDP or Citrix)

If you use VDI, client modules require golden image updates for version changes, not auto-upgrade functionality. Plan your deployment accordingly.

Module Details

eSIGN

Captures electronic signatures using tablets, signature pads, or touchscreens and routes signed documents directly to ECM. IWorkstation clients don't support USB tablets. Administrators use Form Designer to create signature templates that include barcodes for automatic document type indexing.

eRECEIPT

Processes core-generated receipts in Nexus VMD and DNA WMF formats and routes them to member accounts. Administrators use Receipt Designer to modify templates.

SCAN CLIENT

Enables document capture from desktop scanners and multifunction devices with TWAIN drivers. 300 DPI recommended for optimal quality and OCR performance.

UPLINK

Provides network folder access for MFPs and document import processes. Runs on a standalone PC or server with minimal resources. Network folder paths must avoid spaces—use underscores instead. 32GB RAM recommended if hosting local file shares.

Validate Deployment

Before organization-wide deployment, test these workflows at actual workstations to check that modules work correctly:

- **Signature capture:** Process a test account opening with an electronic signature and verify the signed document appears in the member's file immediately.
- **Document scanning:** Scan a test loan document using a loan officer's desk scanner, and validate it routes to the correct account with the correct metadata.
- **Receipt processing:** Generate a test receipt in your core system and confirm it routes to the correct member's account.

Run these tests at your weakest network location, not just branch headquarters. Performance at a low-bandwidth branch can uncover issues that central testing would otherwise miss.

Red Flags

Vendors who require you to purchase specific hardware brands instead of working with what you already have.

This increases costs and forces you to replace equipment when the vendor should support standard hardware.

Vendors who can't provide clear deployment documentation showing actual system requirements.

Without clear requirements, you can't validate compatibility, which could lead to extra fees and delays.

Vendors who force organization-wide deployment instead of a phased rollout.

Working gradually allows you to measure paper reduction and address issues before you pull in other processes.

3. How Performance Gets Prioritized

Staff maintain shadow filing systems when ECM retrieval is too slow to rely on during member interactions. Loan officers keep printed copies at their desks. Tellers reference paper files instead of pulling up accounts on screen. Staff try the system once, wait fifteen seconds for a signature card to load, and decide never to rely on it during active member service.

Slow retrieval creates a credibility problem. The platform works well for overnight batch processing, where speed isn't critical, but fails during interactions that consume most of the staff's time.

Making retrieval fast enough that staff actually use it requires platforms that prioritize member-facing operations over background processing. When performance priorities match operational reality, staff stop maintaining shadow files because the system is faster than paper.

What Matters for Performance

1. **Real-time operations:** Document retrieval during account servicing, loan officer access during consultations, and verification review during account opening. These need sub-second response regardless of system load.
2. **Batch processing:** Statement archival from core systems, bulk document imports during migration, overnight compliance report generation. These can run when system load is low without affecting member service.
3. **Event-driven workflows:** Commercial loan exception routing when amounts exceed authority limits, BSA documentation checks when required fields are incomplete, and approval queue notifications. These trigger based on document metadata.

How Platforms Optimize

Effective platforms cache common metadata like document type lists, retention policy tables, and user permission structures. This eliminates repeated database queries that slow retrieval during peak hours. They balance batch sizing to reduce network overhead without increasing recovery time when processing fails midstream.

Operational Priorities

Staff retrieving documents during active member service need consistent performance regardless of what's running in the background. Operations during peak periods create load spikes that exceed average daily volume. Capacity planning based on average performance fails during actual operations.

Performance at headquarters doesn't reflect conditions at remote locations with limited bandwidth or older infrastructure. Testing must include at least one low-bandwidth location to reveal issues headquarters won't catch.

Validate Performance

Test document retrieval during Monday morning opening and Friday afternoon peak periods to measure response times when system load is highest. Test at your location with the worst network connection—if retrieval works there, it works everywhere.

Red Flags

Vendors who show benchmark speeds without explaining testing conditions.

Ask whether tests simulated actual peak load or measured idle system performance.

Vendors who can't demonstrate performance during simulated peak load.

If they haven't tested under realistic conditions, performance claims are meaningless.

Vendors who haven't tested at locations with limited bandwidth.

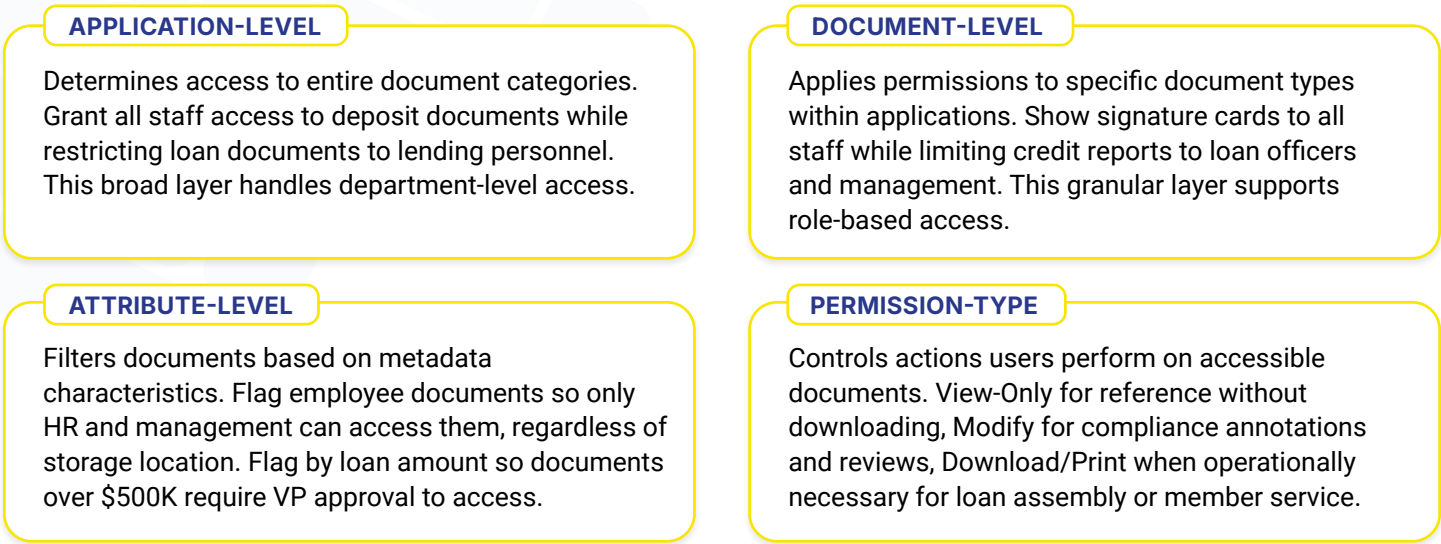
Performance at headquarters doesn't predict performance at remote locations.

4. Security Structured for Examination

Compliance teams spend the week before exams manually compiling document lists instead of doing actual compliance work. Examiners request all SARs filed in Q3, and compliance spends hours tracking them down across different document categories and storage locations. Manual compilation introduces errors—document lists may miss items stored under different naming conventions—and audit trails require IT to run database queries.

When security architecture is structured for examination, compliance runs queries instead of compiling lists. Examiners request SARs from a specific quarter, and compliance produces complete results in minutes. Audit trails show who accessed documents, when, and what actions they took without requiring IT involvement. Legal holds prevent deletion across all document types.

Access Control Structure



Permission Type	What It Allows	Use Case
View-Only	Reference without downloading or printing	Teller verification of information
Modify	Update metadata or document content	Compliance annotation of reviews
Download/Print	Full access when operationally necessary	Loan officer document assembly

When examiners request SARs filed in a specific quarter or commercial loans above specified dollar thresholds, this layered structure enables staff to retrieve them in minutes via database queries.

Consistent categorization matters, too. Loan applications, credit reports, collateral documents, BSA forms, and account-opening records all need standard naming conventions and metadata schemas that map to regulatory categories, not generic enterprise filing systems.

What Examiners Request

Examiners don't just request documents. They request evidence that your controls work.

DOCUMENT RETRIEVAL

When examiners request all SARs from Q3, compliance queries by date range and document type, preview results, and produce formatted exports in hours. The same query structure applies to commercial loans above dollar thresholds, credit reports pulled within a specific period, and any other document category organized by regulatory requirement.

ACCESS AUDIT TRAILS

When examiners ask who accessed a specific SAR and when, compliance retrieves audit trails that show every access, timestamp, and action taken. The system maintains immutable logs for every document without requiring IT to run database queries.

RETENTION COMPLIANCE

When examiners ask how you enforce retention requirements, compliance shows system-enforced retention configured by document type—TILA for certain disclosures, RESPA for settlement documents, BSA for suspicious activity reports, member business lending rules for commercial files. Documents remain accessible for required periods and become eligible for deletion only after retention expires. The system enforces this without manual tracking.

LEGAL HOLD STATUS

When examiners ask how you prevent deletion during investigations, compliance shows legal holds that prevent deletion across all document types during litigation, investigations, and regulatory actions. Legal holds apply across document categories and storage locations without manual intervention.

Red Flags

Vendors with generic document categories instead of banking-specific structures.

If document types don't align with specific requirements, exam prep can drag.

Vendors who can't demonstrate retention enforcement for specific regulatory requirements.

Ask them to show how TILA retention differs from BSA retention in their system.

Vendors whose audit trails require IT to run database queries and compile reports.

Compliance should be able to pull audit trails directly without technical support.

5. When APIs Extend Automation

Most credit unions don't need APIs. Standard ECM functionality handles document capture, storage, retrieval, retention, and compliance without custom development. APIs matter for institutions with development resources who want to automate workflows beyond what the platform provides—instantly generating documents when events occur in your core, building member-facing portals, or routing documents based on complex business rules unique to your institution.

For institutions with development resources, APIs extend automation beyond standard platform capabilities. Identifi provides REST endpoints documented in an operational context so developers understand performance requirements without consulting operations teams.

When APIs Add Value

Custom automation that connects ECM to other systems: creating documents when specific events occur in your core, pulling document data into custom dashboards or reporting tools, building member-facing portals where members upload documents directly, and automating document routing based on complex business rules specific to your institution.

This requires technical expertise, either with in-house developers or a third-party development partner who writes code against the API documentation.

Core Endpoints

DOCUMENT OPERATIONS (/documents)

Upload member signature cards during account opening, retrieve loan documents during member meetings, bulk upload nightly statement batches via SFTP, and apply retention tags to BSA documentation.

SEARCH AND QUERY (/search)

Query capabilities with filter parameters for account numbers, loan types, retention categories. Staff queries require sub-second response. Compliance reports tolerate longer processing for comprehensive results.

WORKFLOW AUTOMATION (/workflow)

Route commercial loan exceptions when amounts exceed authority limits, flag BSA documentation missing required fields, send notifications when signature cards arrive from branches.

BATCH PROCESSING (/batch)

Statement archival from core systems, bulk imports from legacy systems, and compliance report generation across millions of documents.



Complete API documentation is available via Swagger UI, including banking workflow examples and data flow patterns for core systems.

Red Flags

Vendors who push APIs as the primary implementation path.

Most credit unions don't need custom development, and vendors who lead with APIs may lack strong standard functionality.

Vendors who can't provide operational context in API documentation.

If developers need to consult operations teams to understand performance requirements, documentation is inadequate.

How to Evaluate a Vendor

Use these questions during vendor evaluation to assess capabilities beyond feature demonstrations and marketing claims. These questions reveal vendor experience, institutional knowledge, and their ability to execute independently without consuming your IT resources.

Core Compatibility

- ☐ Which cores do you support? How does your data flow approach differ between Jack Henry, Fiserv, and FIS platforms?
- ☐ If we work through an intermediary host, how does that affect your timeline and approach?
- ☐ Walk us through how data flows when a loan closes in our core. What triggers document creation? How does indexing transfer?
- ☐ How does your platform handle core system updates? What's the process for ensuring continued data flows after our core provider releases updates?

Implementation Model & Resources

- ☐ Walk us through your most recent implementation similar to ours in terms of asset size and core platform. What problems surfaced? How were they resolved? How long did the resolution take?
- ☐ What percentage of implementation work do you handle independently, and what percentage requires our team's involvement? Be specific about configuration, testing, data mapping, and training.
- ☐ How do you adapt to constraints like NCUA exams, core conversions, and seasonal volume spikes?

Performance & Optimization

- ☐ What performance benchmarks do you use for workstation retrieval? What factors affect those benchmarks?
- ☐ How do you optimize for distributed branch networks with varying bandwidth?

Security & Compliance

- ☐ Walk us through your last SOC 2 audit. What was the scope? What were the findings?
- ☐ Show us the audit trail for a document. Who accessed it? When? What actions were taken?
- ☐ If we receive an e-discovery request tomorrow, how long does it take to query documents, preview results, and produce formatted exports?

Support Structure & Response

- ☐ Do support requests route to teams who know our configuration, or to general support queues where we re-explain our setup with each request?
- ☐ If we experience a production issue during month-end close or exam preparation, what's your escalation process and response time?

What You Can Expect from Identifi

Identifi has served banks and credit unions for more than 35 years, focusing exclusively on financial institution document management in highly regulated environments.

Banking-First Platform Design

Our platform was built for financial institutions and only for financial institutions. Retention policies map to TILA, RESPA, BSA, and member business lending requirements. Workflow automation accounts for signature authority limits, exception routing based on loan amounts, and compliance review triggers specific to regulated financial services.

SaaS Infrastructure Management

Our platform operates as SaaS-only. You don't manage servers, storage, or upgrades. Infrastructure runs in hosted environments under SOC 2 oversight. Identifi handles capacity planning, security patching, and version upgrades without requiring your team's involvement.



If you're moving from an on-premise solution, this eliminates server hardware, storage arrays, database administration, and IT staff time currently consumed by infrastructure management.

White Glove Implementation

Implementation means building the platform with and for you, rather than handing you documentation and expecting you to configure it yourself. Identifi extracts documents from your current ECM, maps them to the new platform structure, loads sample documents for your review and approval, and iterates until the configuration matches your requirements.



For institutions without an existing ECM, Identifi provides guidance on configuration based on your organizational structure and operational workflows.

Direct Core Vendor Relationships

Identifi maintains direct relationships with COCC and Corelation, streamlining connectivity setup through established processes and institutional knowledge. Baseline Integration (BLI) supports these and many other core and non-core banking systems, adapting to each platform's specific data structures and workflow requirements.

We can discuss specific data flow approaches for your core during technical discovery calls, providing details about data mapping methods, permission structures, and typical implementation timelines based on actual experience with institutions running your configuration.

Support Structure

Support requests route to teams who know your configuration, not general queues where you re-explain your setup with each request. Staff you know by name handle your tickets. Escalation paths are clear. Critical issues affecting member service receive prioritized attention.

About Identifi

Identifi was built for the parts of servicing that don't show up in demos. The day-to-day document work that slows teams down, creates risk, and turns small process gaps into bigger operational problems. For more than 35 years, we've helped banks and credit unions tighten document management in highly regulated environments without adding complexity or forcing teams to change how they work just to fit the system.

Our platform consists of two integrated solutions designed to work together:

Enterprise Content Management (ECM)

Our mature ECM handles the full document lifecycle with automated workflows, version control, and compliance-driven retention. The platform manages millions of operational documents through an encrypted repository, maintaining rigorous audit trails and regulatory compliance from capture through disposition. Document management becomes a controlled process rather than a manual effort.

Workflow Platform

Our workflow platform digitizes and manages operational processes that extend beyond document storage. Teams can build digital-first automated workflows that route approvals, trigger notifications, track status, and integrate decision points across lending, onboarding, and compliance functions. Workflow logic connects directly to document actions—e-signatures, tracking, receipts—eliminating the need to switch between systems or manually coordinate handoffs.

Both platforms connect to the core systems credit unions already run, supporting workflows tied to real servicing needs like onboarding, lien releases, audit prep, retention tracking, and approvals. The goal is simple: reduce manual effort, shorten turnaround time, and keep IT, compliance, lending, and operations aligned.

If your institution is ready to streamline document workflows without unnecessary disruption, Identifi is here to help you move faster, stay compliant, and keep servicing running clean.

Schedule a Discovery Call

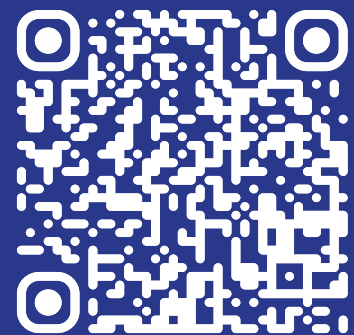
Whether you're evaluating vendors now or planning for the next fiscal year, our team can discuss your specific situation during a technical discovery call.

We'll review your core platform and data flow requirements, your institution's technical infrastructure and constraints, your implementation timeline and operational considerations, and whether ECM makes sense given your current projects and resource availability.

📞 727-725-4507

✉️ sales@identifi.net

🖱️ identifi.net/credit-union-ecm



Scan to schedule
a consultation