



DoD Business Transformation

- Fully address DoD business transformation with an ECM platform that automates transactional audit.
- Retain control over records with DoD 5015.2-certified transparent records management.
- Enable content-driven collaboration with Workflow automation and SharePoint integration.
- Provide security with multi-factor access control mechanisms.
- Leverage technology to improve continuity of operations planning (COOP).

DoD Business Transformation:

Stewardship and Autonomy

A Laserfiche® Federal Focus White Paper

Contents

EXECUTIVE OVERVIEW	1
Modernizing Processes, Systems and Information Flows	1
Transparency, Accountability, Agility	2
STEWARDSHIP AND AUTONOMY	2
Transparent Records Management	3
Legal considerations	3
Records management checklist	3
Business Process Automation	4
Audit, Reporting and Accountability	5
Content-Driven Collaboration	6
Transactional content/collaborative process management (CPM)	6
Document collaboration benefits	6
Legacy System Integration	7
Back-end integration	7
Front-end integration	7
Security–Need-to-Know Access Control	8
Security Features Checklist	9
Continuity of Operations Planning (COOP)	10
Records protection across the extended enterprise	10
THE LASERFICHE RIO APPROACH: A COMPLETE ECM SOLUTION	11
Provide Continuous Access to Your Information	12
Configure flexible data storage solutions with unlimited servers	12
Extend your solution without risk	12
Manage system administration simply	12
Work Closely with SharePoint® and Other Microsoft Applications	13
Rio Web part for SharePoint	14
SharePoint records center integration within Rio services	14
ACHIEVING ENTERPRISE-LEVEL BUSINESS PROCESS AGILITY	15
Extended Enterprise Deployment	15
Processes Systems and Transparency	15
COOP	16
Reducing Operations Costs	16

Executive Overview

The Department of Defense (DoD) is undergoing a progressive transformation towards a Net-Centric enterprise, in support of data and service interoperability across various services and agencies to enhance mission-oriented decision making capabilities.

Modernizing Processes, Systems and Information Flows

In response to the National Defense Authorization Act of 2005, DoD established the Business Transformation Agency (BTA), tasked with modernizing processes, systems and information flows to deliver 21st Century enterprise-level capabilities required to support national security requirements.

Defense business operations are being streamlined so that DoD can more effectively deliver warfighting capabilities, deal with growing pressures on resources, and benefit from economies of scale. Costly and outdated systems, procedures and programs tax resources from warfighting and stifle innovation. Faster, more efficient processes reduce costs while delivering better support.

Targeted were 18 of the DOD's business programs, systems and initiatives, including: the Defense Travel System, the Standard Procurement System and the Defense Integrated Military Human Resources System. Business operations at six defense agencies have been impacted: the departments of the Army, Navy and Air Force; the defense logistics agency; defense finance and accounting service; and transportation command.

Two of DoD's strategic objectives for business transformation include reducing the cost of business operations and improving financial stewardship. A cornerstone component of this transformation is the Business Enterprise Information Services (BEIS) providing enterprise-level business intelligence capability which yields access to timely, accurate and reliable financial information across the DoD enterprise. Enterprise Systems and Services provided across agencies demand comprehensive redundancy techniques to assure continuity of operations (COOP) in response to potential operational interruptions.

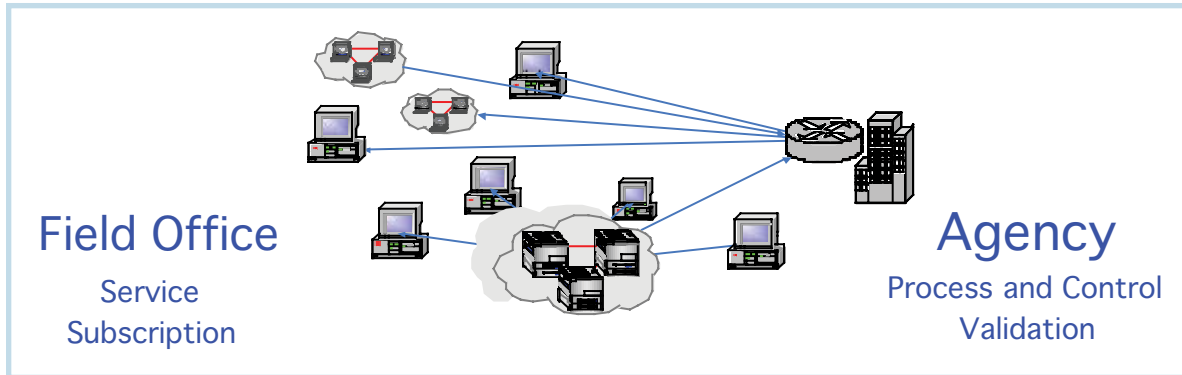
To help guide this undertaking, BTA publishes the Enterprise Transition Plan (ETP) each September, establishing the baseline against which the department measures progress during the fiscal year. The March *Congressional Report* reflects updates to the previous September ETP and provides annual status. Together, the ETP and *Congressional Report* allow leadership to evaluate gaps and overlaps between current programs and redirect efforts to minimize redundancy and provide needed business capabilities.

DoD's current efforts to reduce costs are already bearing fruit—for instance, the Defense Travel System (DTS) has reduced the processing cost of travel vouchers by millions annually on a path to savings of \$56 million per year by fiscal 2009.

Transparency, Accountability, Agility

Transparency-driven initiatives at DoD Financial Management highlight the need to improve current methods for monitoring transactional events, recording content, auditing accountability and comprehensive record keeping across the enterprise.

The modern electronic workplace offers the promise of providing both the operational metrics and transparency to fully address DoD business transformation. The combination of business process automation and transparent records management establishes a platform to monitor transactions and improve accountability.



The agile enterprise content management (ECM) solution provides transparency and accountability for the business processes so automated. Business Process Benchmarking enables development of best practices which can then be replicated and standardized throughout the extended enterprise.

Stewardship and Autonomy

Business operations at six defense agencies have been impacted: the departments of the Army, Navy and Air Force; the defense logistics agency (DLA); defense finance and accounting service (DFAS); and transportation command. The obvious decentralized nature within agencies, further complicated by inter-agency collaboration, presents unique challenges.

Stewardship for transactional content across the extended enterprise is best served providing autonomy at departmental or regional repositories when not connected, and synchronization with custodial systems at agencies when connected. Message-based ECM services offer the greatest agility where field locations experience occasional connectivity.

Extended ECM Services Securing Transactional Records

- Provide high availability repository services across the extended enterprise for protected documents and records.
- Accommodate satellite offices that need their own servers.
- Create separate servers to segregate sensitive data.

Transparent Records Management

Transparent records management allows records managers to retain control over the way information is categorized and filed outside of the view of everyday users. Once set up, users will not have to actively participate in the process, while records managers still have control over ultimate file indexing, archiving and disposition.

One of the greatest strengths of this functionality lies in the way it enables records managers to create a file plan and manage retention schedules without interfering with any department's line of business. Furthermore, the system will enable records managers to more easily apply consistent policies to records in a variety of media, from Web content to archived e-mail messages to audio and video files.

Legal considerations

Legally, records must be trustworthy, complete, accessible, admissible in court and durable for as long as the retention schedule requires. Records management applications are uniquely positioned to help records managers meet these requirements. Whereas paper files are vulnerable to fire, flood and theft, digitized files enjoy multiple layers of protection. Security features protect records from tampering or unauthorized release, while auditing functionality allows you to monitor user actions on a record.

Because Web content plays an increasingly large role in service delivery, effective management of Web records is also critical to mitigating risk. Using a records management application, you can take snapshots of your organizational Website at regular intervals and retain these files according to a specified retention schedule. These records will prove highly useful in the event of a legal challenge, or if the original Web content is compromised or lost.

A U.S. DoD 5015.2-certified records management platform is required that empowers organizations to apply records and retention policies, as well as legal discovery and holds to all relevant content across the enterprise—from content stored in file servers to physical records in a warehouse. Such a system defines, manages, and executes these records and retention policies for all enterprise content from a single server.

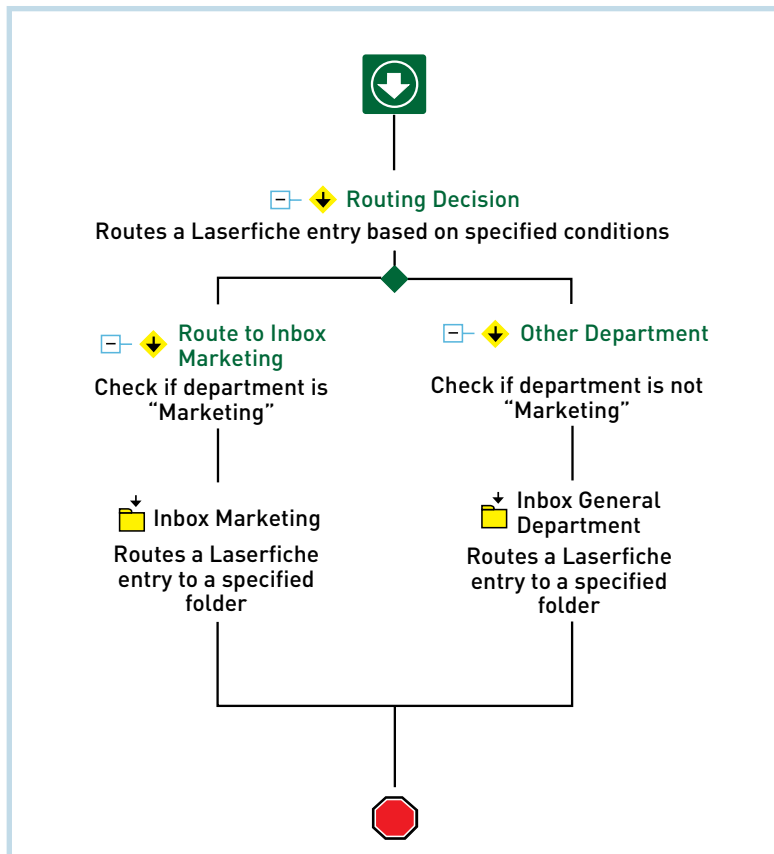
Records Management Checklist

Records management functionality requires special considerations above and beyond typical ECM functionality.

- The application should be DoD 5015.2-certified.
- The records management application should support custom searches based on record properties, retention or disposition properties, full-text content, template fields, folder location, sticky-note contents and more.
- It should be possible to save search results in a usable format, such as an Excel spreadsheet.
- The records management application should manage the full life cycle of the record, from document creation through declaration as a record to final disposition.
- The records management application should provide detailed reports of which records are eligible for transfer, accession or deletion.
- Audit trails should be in place to track system activity.

Business Process Automation

Business process automation, enabling benchmarking and improvement is one of the most effective tools available to modernize processes and information flows. This capability has particularly high impact when applied to the extended enterprise spanning agencies, departments within agencies, and front office operations.



Routing decision activities with a workflow module.

The success of any workflow system is not its ability to follow the strict routing and reporting features of a fully-automated system, but its ability to handle exceptions to the rules as they arise. An effective workflow system provides the system administrator complete access to on-the-fly routing of documents and information through the system's folder structure and security.

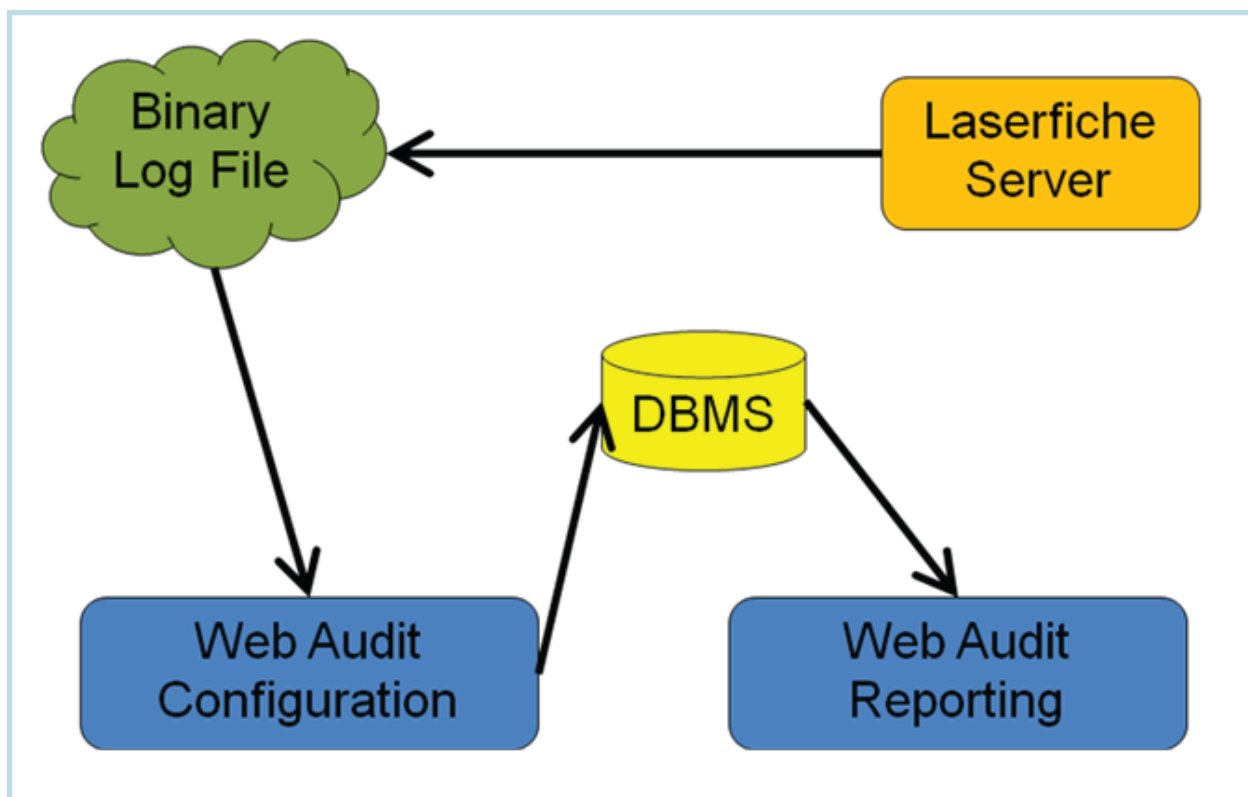
Workflow systems should offer administrators drag-and-drop simplicity, an intuitive graphical interface and an easily-understood folder structure. Workflow applications should be open data base connectivity (ODBC) compliant to facilitate integration and customized application. As a final component, workflow must provide for comprehensive security reporting through an audit trail function.

Audit, Reporting and Accountability

Transparency and accountability are words which have become the unquestioned holy grails of good governance. Audit trail capabilities are especially important when an organization seeks to automate process and control. Decision criteria and accountability can be traced to process audit trail and referenced documents of record retained within a robust ECM.

Event Tracing for Windows (ETW) forms the basis for tracing that can be enabled or disabled at any time by an administrator using standard Windows tools. Virtually every aspect of the server can be traced using ETW.

Audit trail reporting configuration.



Content-Driven Collaboration

Collaboration features within segments differ based on the objectives being served. Content usage profiles can be identified each with distinct profiles driving retention, security, capture/publish frequency, privacy and other attributes.

- **Persuasive content** such as marketing collateral typically consisting of a single document being reviewed and modified by multiple authors, then being published over a reasonably short lifecycle.
- **Business content** such as contracts with multiple exhibits or New Drug Applications composed of many subsections separately authored, then in turn reviewed by others who edit content with specific authorship of edits logged.
- **Transactional content** such as securities transactions, new account applications, mortgage origination documents, purchase orders, or documents of record validating collateral transactions in payment and securities settlement. Content management systems serving this operational model organize collections of documents sharing a common topic, goal or agenda, separately authored, then in turn reviewed by others who make comments with specific authorship of comments logged.

Transactional content/collaborative process management (CPM)

Transactional content collaboration across a multi-campus enterprise can only be served by a message based architecture enrolling content in these “managed collections” as created. This “front office” transparency combined with CPM infrastructure based on Windows Workflow Foundation (WF) enables a transaction level audit trail for the inter-enterprise business process.

Document Collaboration Benefits

This transactional content operational model and distributed capture capability offers:

- Transaction transparency to enable the DoD supply chain management goal to deliver the “right items to the right place at the right time.”
- Document collaboration enhancements for line-of-business applications.
- Business process management and workflow within document collaboration.
- Peer-to-peer tools and technologies to solve business problems that centralized systems cannot.

Legacy System Integration

The introduction of new software and databases often creates logistical challenges for an organization's computer support staff. A quality solution should provide tools to make integration easier.

Back-end integration

Back-end characteristics facilitating integration include a system designed with "open architecture," which is designed for easy integration. Hardware and software tools with open architecture enable anyone to create add-on products to connect the hardware or software to other devices.

Front-end integration

Front-end integration is especially important for organizations that utilize documents in a supporting role. These organizations want a solution that is transparent, given that staff members don't want to learn a new system just to gain access to supporting documentation. Because staff members already have a primary application they use to complete their daily tasks, the best way for them to access documents is through this familiar application. Image-enabling primary applications allow staff to quickly access the documents they need by simply clicking a button or pressing a function key.

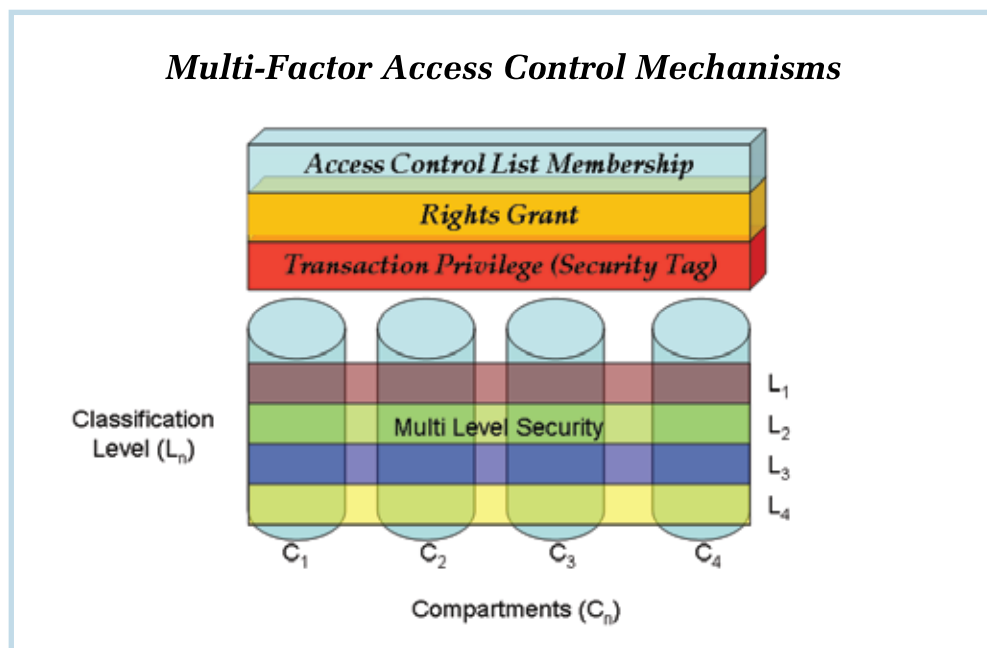
The value of front-end integration is primarily realized in training costs reduction. Because staff members already know how to locate records in their primary application, they will not need to learn how to locate documents in the document management system. They will have to learn how to request the type of document they want and, if necessary, how to work with documents in an electronic format. However, this requires less time than teaching them how to use the complete system.

Security—Need-to-Know Access Control

System security is an absolute necessity for any ECM system. A rigorous security system should permit every authorized person to perform required duties—whether from desktop, laptop, the office, a remote location or via the Web—without compromising database, system or network integrity.

Comprehensive security is critical to the successful implementation and ongoing protection of a system. While security may not be the primary concern for a single department installation, it becomes more important as the system is expanded to allow different departments, and even the public, access to files. Although a system should provide multiple levels of security, including: authentication, authorization, audit trails and disaster planning, the system's security should parallel that of the network and be simple to administer.

A full-featured ECM system gives the system administrator the tools to balance access and security through control over access and feature rights. Access rights determine who can log on to the system and which folders or files individuals can open. Feature rights determine the actions that individuals can perform on documents they have access to controlling page access, deletion, creation, and page movement. A comprehensive security system also allows high-level users to redact or black out confidential information within files.



Authentication is the level of security that requires users to present credentials, normally a user name and password, in order to access the system.

Authorization is the level of security that controls access to objects, such as files and folders. Authorization encompasses two primary areas: access and feature rights.

Rights management enables organizations to assign access rights to specific folders and documents, at the group and individual level. The use of groups with inherited or predefined rights allows system administrators to quickly assign viewing privileges, while individual-level security allows specific users, such as managers, to view documents that the rest of the group cannot. Feature rights determine a range of actions, including: adding pages, annotating, copying or deleting records.

A best-in-class ECM system will not allow users to see objects for which they do not have viewing privileges. This protective feature is especially important for organizations with systems containing confidential files and folders.

Redaction (blackout or whiteout) is a security feature applied within documents to make certain portions of the document inaccessible, except to authorized users. Blackout redactions are familiar to anyone who has seen a classified FBI file on the news, but whiteout redactions are somewhat different. Instead of a visible thick black line through the redacted text, whiteout redactions function much like an eraser. Using whiteout redaction, a viewer will not know that information has even been redacted. An ECM system should offer the ability to redact portions of a document's image and/or text.

Users' ability to view redacted text would depend on their security rights. Redaction allows you to extend security from folders and documents right down to the character level, enabling comprehensive security and maintaining the privacy of scanned images.

Security Features Checklist

- Single sign-on.
- Active directory integration.
- Permission inheritance.
- Secure documents through access control lists, security tags and privileges.
- Role-based authorization.
- Privilege delegation.
- Security watermarks.
- Mandatory watermarks for printed documents.
- Secure deletions.
- DoD 5022.22 M compatible deletion protocols.
- Secured recycle bin.
- Secure communication.
- Support for SSL for secure communication.

Continuity of Operations Planning (COOP)

COOP is simplified with clustered configuration of document repositories implementing active mirroring and failover. User data and/or applications are protected and continue to be available to the user community. High availability clusters provide protection far beyond periodic back-up by capturing byte-level changes in real time and replicating them to your alternate server, either locally or across the globe.

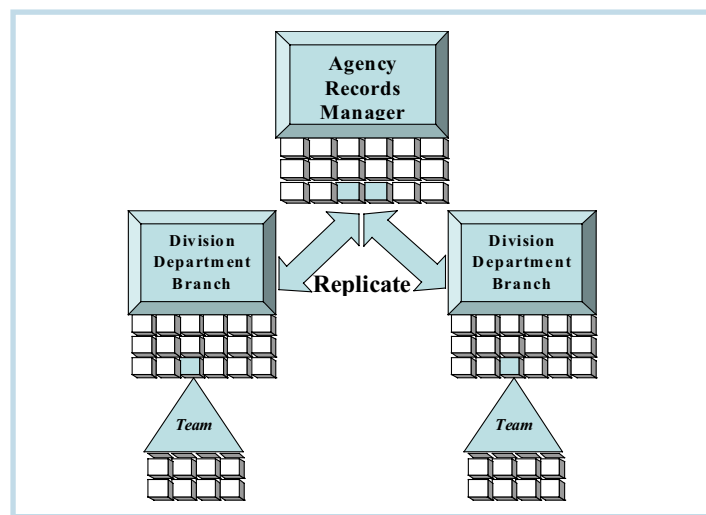
Records protection across the extended enterprise

Records protection across the extended enterprise is best provided through cluster continuous replication (CCR), a high availability capability that utilizes failover and management features provided by the cluster service that:

- Has no single point of failure.
- Has no special hardware requirements.
- Has no shared storage requirement.
- Can be deployed in one or two datacenter configurations.

Peer-peer high availability and parent-child distributed capture requirements are well served through these features in organizations distributed across a multi-campus enterprise.

To assist in disaster recovery planning, records management software enables you to copy records to disc or other unalterable media for off-site storage. If an incident occurs, you can typically restore your archives in a matter of minutes, which allows you to access the critical information you need to respond effectively and to ensure organizational continuity.



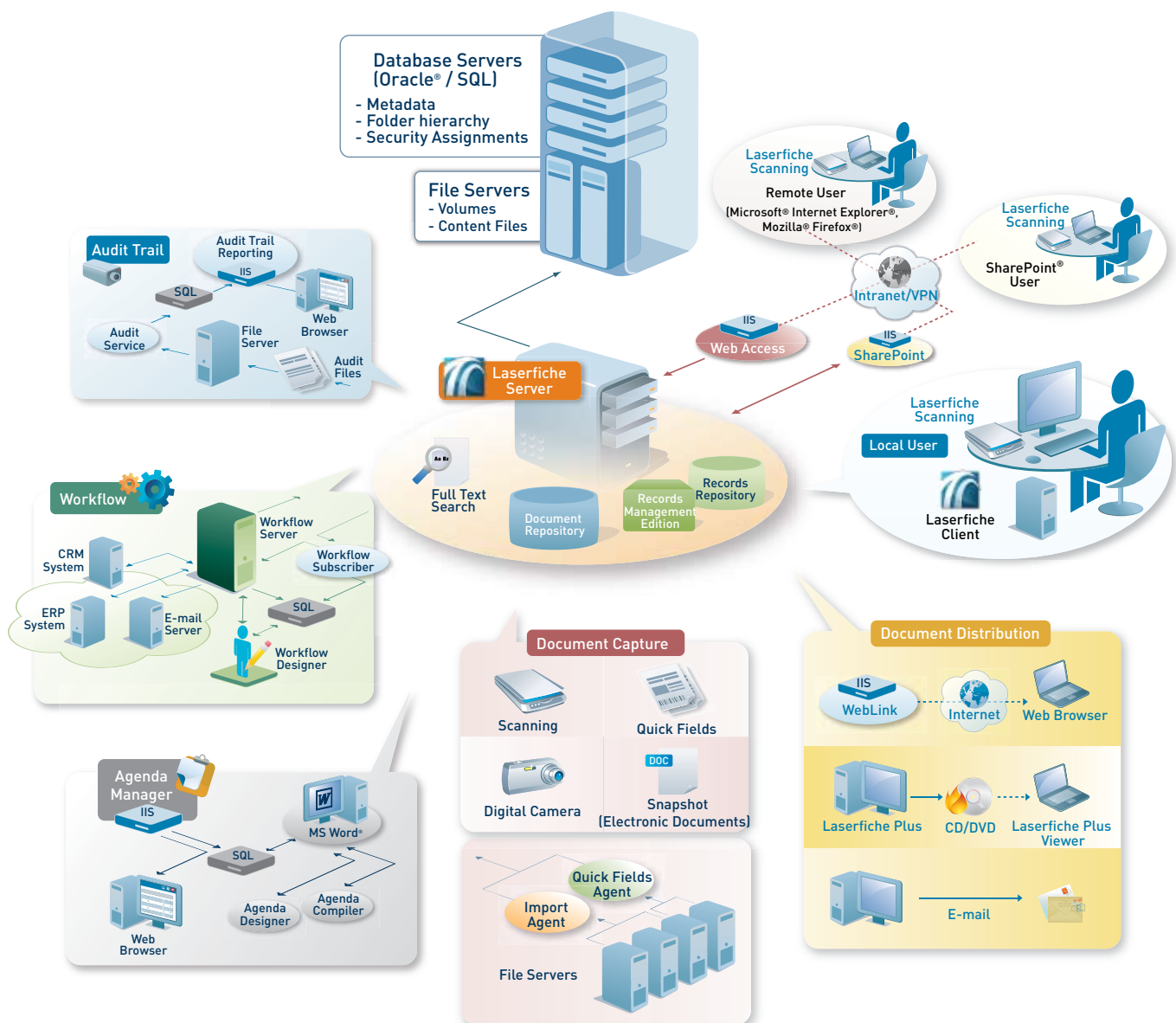
HTTP based communications, Web DAV implementation and a message based collaboration, enable remote user enrollment without installing software on multiple workstations and thin client document capture into the main document repository. Authorized users scan, index and manage documents with Web browsers just as easily as they would with the thick client installs. Field offices fully participate in business processes, contributing scanned and electronic forms for central processing.

An open systems approach extends this distributed collaboration capability through implementing seamless integration with Microsoft Office, Microsoft SharePoint, Windows WF and the Microsoft Desktop. This open systems capability provides seamless integration with Microsoft content formats.

The Laserfiche Rio Approach: A Complete ECM Solution

Laserfiche Rio ECM is a powerful, complete solution that is straightforward to purchase, deploy, extend and manage. With Rio, you have the flexibility to reconfigure your system to accommodate changing requirements, project scopes and business conditions, so your solution fits even unique situations without extensive development, programming or staff effort.

The Rio system includes information management, document imaging, DoD-certified records management, business process management, system activity monitoring and Web publishing modules in a single procurement.



Provide Continuous Access to Your Information

Rio's licensing is based on the number of people who will be using the system, so staff will never be denied access because all licenses are in use. Each connection is assigned to an individual staff member and provides access to all of the products in Rio. When you add users, you add new components to the entire system, not just to a single server or a single department's installation.

Rio's Public Portal licensing option provides unlimited read-only connections through Laserfiche WebLink, a platform-independent, Section 508-compatible Web publishing tool that integrates easily with your existing Website.

Because the amount of traffic a public information portal receives can be unpredictable, unlimited preprocessor licensing guarantees that your Web portal won't stop responding due to a lack of licenses.

Configure flexible data storage solutions with unlimited servers

The Laserfiche Rio suite includes an unlimited number of servers, so expanding your system to additional departments, satellite offices or divisions simply involves adding a new server to your existing infrastructure. Any named user can log onto any server connected to the network, delivering superior flexibility in data storage.

Extend your solution without risk

Rio organically expands throughout your organization, crossing departmental boundaries and easily integrating with your other line-of-business applications and legacy systems to eliminate data silos.

The Rio system includes Web Access, a Section 508-compatible Web-based thin client that is easily integrated into existing networked environments and enables staff to access the Laserfiche repository without installation and maintenance at the workstation level.

Manage system administration simply

Rio's Administration Console centralizes management of all the components of the server through a simple graphical interface. Administrators can easily troubleshoot Rio with ETW, supplemented by HTTP logging and real-time console mode debugging.

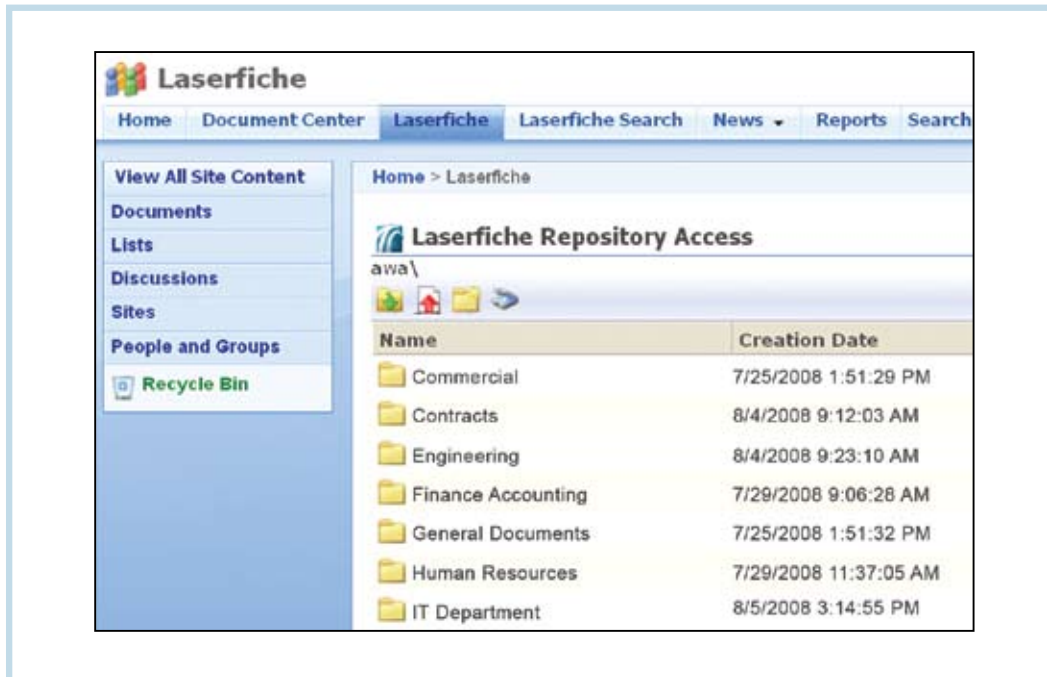
Audit Trail, Rio's built-in auditing solution for security and compliance, tracks repository changes, or administrators can create custom reports through a .NET library or Microsoft SQL reporting services.

ETW forms the basis for tracing that can be enabled or disabled at any time by an administrator using standard Windows tools. Virtually every aspect of the server can be traced using ETW. System errors and warnings are reported in the Windows event log. Administrators benefit from central control over security, content and system administration, while departments have the flexibility to customize their systems to fit different filing systems and workflow needs.

Work Closely with SharePoint® and Other Microsoft Applications

Rio is built on Microsoft technology, so it fits effortlessly into Microsoft-powered organizations.

Microsoft Office SharePoint Enrollment

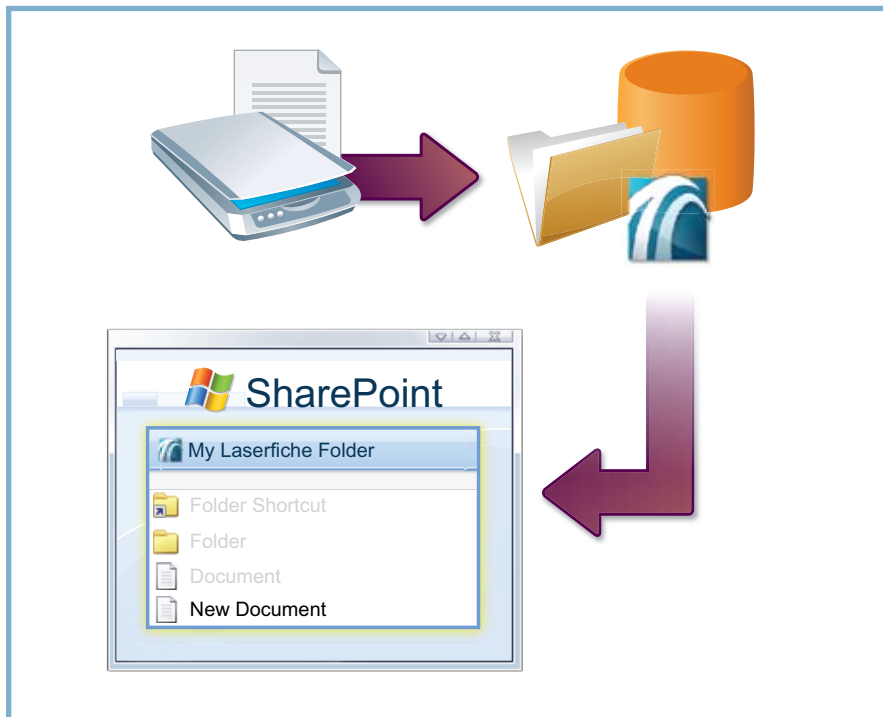


Rio and SharePoint integration maximizes the strengths of both systems to enhance the utility of your SharePoint solution. While SharePoint offers excellent collaboration and portal functionality, especially with Microsoft Office documents, Rio provides world-class document imaging, distributed capture and records management.

By combining the two, users get a complete information management system that allows users to easily and securely work with documents throughout their life cycle.

The two keys to the success of the integration are data synchronization and accessibility. With data synchronization between the two systems, a variety of tasks—such as moving documents, preserving links, limiting copies and removing deleted documents—are handled automatically, without administrative intervention. Thanks to this improved data accessibility, users do not have to know which system stores the document they need.

Rio Web Part for SharePoint



The Rio Web part for SharePoint is key to bringing imaging functionality to collaboration portals in SharePoint. Once the component is added to the SharePoint server farm, it can be added to any SharePoint portal the same way any Web part is added. It enables users to browse any part of the Rio folder structure through SharePoint. You can think of it as putting the folder browser that is part of the Rio Client in the SharePoint interface.

Every contributor throughout the organization can easily contribute content from native desktop applications, efficiently manage business content via rich library services, and securely access that content anywhere using a Web browser. All content, regardless of content type, is stored in the Web repository or database for management, reuse and access. While stored in the repository, all types of content—ranging from e-mail, discussions, documents, reports, spreadsheets and records to images, multimedia or other digital formats—receive the same set of fundamental core services.

SharePoint records center integration within Rio services

Another cornerstone of Rio and SharePoint integration is the ability to store SharePoint documents in Rio once the collaboration phase is finished. From any document library in SharePoint, a user can bring up the context menu for a document and have it sent directly to Rio. Any metadata in the content library is pulled into the document's template when it is moved to Rio, without user intervention.

To keep the system from generating a copy of a document when it is moved into Rio, the integration replaces the document with a URL pointing to the document's location in Rio. Windows Active Directory integration offers document security integrity at any step in the process. This functionality keeps the data in the two data stores synchronized.

Achieving Enterprise-Level Business Process Agility

Extended Enterprise Deployment

Often, ECM solutions are seen as departmental, rather than enterprise. An ECM solution may offer central control of information, but isn't flexible enough to accommodate the needs of the multi-campus organization and the extended enterprise presented by inter-agency collaboration.

Local autonomy

A successful ECM solution gives departmental staff and line-managers autonomy over improving business processes, centralized oversight and control over policies and direction actually increases.

Legacy system integration

ECM systems should offer packaged integration tools for simple image enabling, to minimize the burden on IT. Ensure user acceptance by empowering departments and regional business units to adapt the ECM system to their existing filing methodologies.

To minimize disruptions to business operations, it is essential that a ECM system integrate smoothly with other software applications. Packaged integrations can range from plug-ins for popular software programs, such as GIS, or additional modules supporting popular features, such as electronic signatures.

Processes Systems and Transparency

Transparent records management

Information workers may have spent years developing the way they work and the way they manage their files. It is important to remember that no ECM system will offer centralized control of content if it is not used.

Business process management

Automation for business process and audit reports of business activities of activities is key to addressing the transparency requirements of 21st century governance.

Accountability, auditing and reporting

Audit logs written to files on the file system establish an audit trail totally independent of the data management system being audited. Only when audit logs may be read offline without requiring access to the original repository can they be submitted for independent examination.

Security—Need-to-know access control

Delegating security rights should follow the principle of least privilege by granting trustees only the distinct administrative privileges they need.

Work closely with SharePoint® and other Microsoft applications

Key to creating efficiencies in departmental activities and reducing cost of government is capturing transactional events at the front office. Seamless interoperability with SharePoint® and other Microsoft applications is essential to increasing accountability and transparency.

COOP

Organizations responding to mission critical transactional management require systems offering continuous availability in the event of a site failure. High availability clusters provide protection far beyond periodic back-up by capturing byte-level changes in real time and replicating them to your alternate server, either locally or across the globe.

Reducing Operations Costs

Data management system enrollment

Capturing and indexing documents is an expensive component of implementing a document management solution, and anything that can be done to eliminate or minimize these costs will provide a nearly immediate ROI. Information that already exists in primary applications can be utilized to automatically index and file documents as they are captured.

Seek clear “cost of ownership” models

An important part of strategic planning is being able to adapt to an uncertain future. Systems that require extensive customization and development to implement “change” may result in “vendor lock-in” and significant costs responding to changing external factors. Systems that emphasize configuration of standardized solutions, and that leverage existing administration skills tend to offer lower total cost of ownership.

When evaluating solutions, seek clarity regarding costs of expanding the reach of your ECM system, and for adding to the functionality.

The Laserfiche Institute teaches staff, resellers, and current and prospective clients how to use Laserfiche most effectively. As part of this mission, the Institute conducts more than 500 Webinars each year, covering a variety of topics. The Institute also hosts an annual conference where members of the Laserfiche community attend presentations and network to share ideas and learn best practices. Additionally, the Institute conducts a number of regional training sessions and provides resellers with content for more than 100 user conferences each year.

The Institute also develops and distributes educational material through the Laserfiche Support Site. On this Website, clients can access training videos, participate in online forums and download technical papers and presentations that help them become savvier ECM users.

For more information, contact:
info@laserfiche.com

Laserfiche
3545 Long Beach Blvd.
Long Beach, CA 90807
United States

Phone: 562-988-1688
Toll-free: 800-985-8533 (within the U.S.)
Fax: 562-988-1886
Web: www.laserfiche.com

© 2008 Compulink Management Center, Inc. All rights reserved. Laserfiche is a division of Compulink Management Center, Inc. Laserfiche is a registered trademark of Compulink Management Center, Inc. All other trademarks are properties of their respective companies. Due to continuing product development, product specifications and capabilities are subject to change without notice. Printed in the U.S.A.