DOCUMENT WORKBENCH™ INFORMATION SHEET

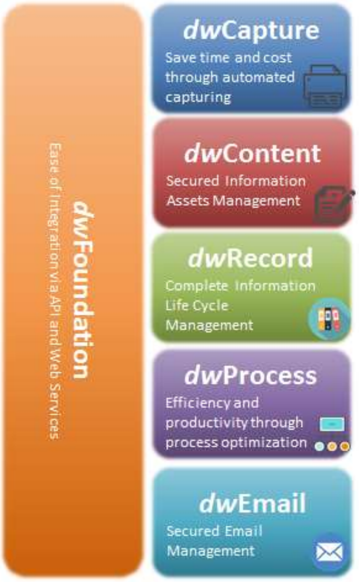
Document WorkBench™ for Simplified Content Security Administration

Simplified and Efficient Information Assets (Content) Administration resolves System Administration Pains, improve Work Efficiency, Productivity and save Costs

Document WorkBench™

Highlights

- Highly Secured.
- High Performance.
- Features Rich
- Highly Scalable
- Yet, easy to operate and manage.


dwFoundation
Ease of Integration via API and Web Services
dwCapture
Save time and cost through automated capturing
dwContent
Secured Information Assets Management
dwRecord
Complete Information Life Cycle Management
dwProcess
Efficiency and productivity through process optimization
dwEmail
Secured Email Management

Content Security Administration Woes

A typical Content Management System houses all of the Information Assets of the organization concerned. Information Assets, in most cases, are given classifications such as, unclassified – for everyone to access, confidential, restricted, secret, top secret etc. so access to the Content is controlled to ensure it is accessed on a need-to-know basis based on a person's job role and responsibilities.

There is a need for a security scheme to administer such access control. Most Enterprise Content Management Systems relies on an access control scheme known as Discretionary Access Control (DAC). According to the definition in DoD (US Department of Defense) Standard 5200.28-STD, Discretionary Access Control is a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. This mechanism allows users (the owners) to grant or revoke access to any object under their control. The common implementation of Discretionary Access Control security model is known as Access Control List (ACL).

Issues with ACL

Based on ACL requirements, when a user indexes a document into the Content System, he/she has to specify a list of other users who will be allowed to access this document. Subsequently, when there is a user trying to access this document, the Content Management System first checks the Access Control List to find if there is a matching entry. In theory, this sounds perfectly fine but in practice, it suffers in two key aspects of any good Content Management System:

i. Ease of Content Security Administration; and,
ii. Performance with Visibility Control.

In the first aspect, the administration becomes overwhelming when there are constant changes in either Content or in personnel movement, particularly if the Content and/or the user groups are large. For every such change, the Content Administrator has to revise the ACL List entries to ensure security practice remain relevant. But this usually gets to a point where it becomes not practicable to execute and many would just leave it unmanaged, leading to heightened incidents of information or data exposure or theft.

In the second aspect, Visibility Control means preventing documents from being visible to requestors who have no access to them; meaning, for each request, the Content Management System has to check against the Access Control List to determine if the resulting documents should be visible to the requestor. For a single request, it is a non issue but in real life usage, most users would query the Content for information which may result in tens or hundreds or thousands of document matches, this is when the Access Control List will grind the system to a halt when there are multiple such search requests carried out about the same time.

Negative Visibility Control Approach

Visibility Control implemented by Access Control List is termed Negative Visibility Control Approach and it has a huge performance downside as content, user base and activities grow.

Document WorkBench™ Simplified and Improved Content Security Administration

Document WorkBench™ addresses the issues faced by the Access Control List implementation with a Positive Approach to Visibility Control, and it is also in compliance with 3 widely known good security principles:

i. Principle of Least Privilege;
ii. Separation of Duties; and,
iii. Data Abstraction.

Principle of Least Privilege requires that a user be given no more privilege than necessary to perform a job; this is important to meet integrity objectives.

Separation of Duties deters fraud since fraud tends to occur if an opportunity exists for collaboration between different job capabilities.

Data Abstraction enforces a clear separation of the abstract properties of a data type from the concrete details of its implementation. This means, for example, in Document WorkBench™ Content Security context, permissions are not given to any user directly, but through another abstract entity like Role. This ensures robustness in managing changes without the burden of updating the mass access controls of the underlying Content Management System.

Dynamic Role Based Access Control - Achieving Positive Approach

Document WorkBench™ implementation of Dynamic Role Based Access Control is the key to achieving the positive approach in content visibility control.

Many of the claimed Role Based Access Control System focus on user aspect of role – a group based security approach that does not address the meaning of role permissions with respect to the document permissions. Document WorkBench™Dynamic Role Based Access Control System adds dynamic object permission and effective permission to offer document-centric control versus user-centric control of the originating standard of Role Based Access Control.

With document-centric control implementation, Document WorkBench™ achieves the positive approach in content visibility control. The complicated and time consuming task of Content Security Administration as experienced with ACL implementation is simplified and reduced to minimal effort in Document WorkBench™ Enterprise Content Management System. Managing content changes and personnel movement is a matter of updating the affected roles and mapping or remapping of role(s) to the persons concerned, such jobs could be performed in minutes instead of hours or days. This means drastic work efficiency and productivity improvement, efforts and costs saving; and, protection of investment is assured in deploying a Document WorkBench™ Enterprise Content Management System.

Positive Content Visibility Control Brings Positive Performance

The retrieval checks enforced by ACL have a large performance downside when content, user base and content activities grow. On the other hand, with a Positive Content Visibility Control Approach, Document WorkBench™ achieved high performance and is able to sustain such high performance even when content size, user base and activities grow; this is possible simply because it does not rely on filtering for visibility control.

For enquiries, contact

1. Sales Enquiry: sales@i-maginationgroup.com
2. Partner Program Enquiry: sales@i-maginationgroup.com
3. Tel: (65) 6490 9588
   Fax: (65) 6490 9599