CASSIA
CONTENT MANAGEMENT

PriSM

Privileges Security Management

Specific Details

Augment and Manage Permissions

- Provides the ability to augment and manage permissions of content based on category attribute values. For example, you could define a rule that would grant the Human Resource department access to any document where the Personnel File category was added.

Content Control

- Keeping control of the content within your Content Server environment is vital. When creating, moving or copying content, you never want sensitive or confidential information exposed.

Improved Taxonomy Adherence

- Your organization’s taxonomy might look fine on paper but the standard Content Server access controls do not enforce adherence to its structure.

Simplified Interface

- PriSM helps you to remove confusion for your less experienced and occasional users. By showing only those types of content that are permitted to be added, the result is cleaner, easier to use and less confusing.

CASSIA
CONTENT MANAGEMENT

PriSM

Privileges Security Management

Extend Object & Usage Privileges

Allowing granular control over what objects can be created in specific locations. A PriSM Configuration allows a taxonomy designer to restrict access to specific objects within specific areas for specific user groups. For example, the creation of folders is locked down in many organizations for Knowledge Managers who create folders. PRISM will allow users to create folders in their personal workspace but not in the enterprise area.

PriSM also allows system administrators to restrict specific file extensions that can be uploaded to Content Server. For example, you could restrict the ability to add Outlook PST files or Windows executable files.

Reduced risk of publishing confidential material

- When documents are moved or copied in Content Server, it is not obvious what access rights will be given to the document in its new location. PriSM surfaces these new rights to the user at the moment of creation. The user can then decide if these are correct and make adjustments accordingly. This avoids assuming content has the correct access rights and makes controlling permissions a part of normal Content Server activities.