# Integrated versus Federated Records Management Solutions (RMS)

## Integrated versus Federated Records Management Solutions (RMS)

This is a topic that should be of great interest to all records managers as it refers to the basic architecture of an RMS and to the particular and very different RM controls that need to be in place to accommodate either the integrated or federated design. The core issues are database integrity and document security. If the records manager gets it wrong he/she will certainly not have a compliant RMS no matter how many certifications the actual software product has.

This last point is critical and in my experience is either misunderstood or ignored by many records managers. That is, using a software product that is 'certified' does not mean your practices and procedures are certified, it is just one of the measures required. Your organization can still be non-compliant (and many are) even if you use a compliant RM product. RM compliance is not about software, it is about practice and procedures and this is particularly important to any organization subject to e-Discovery legislation.

Because of the vagaries of our industry and the inconsistent use of acronyms and terminology by different vendors and industry groups, everything I say about this topic from this point on is a generalization.

Let's begin by saying that there are integrated RMS and federated RMS offerings on the market. There are also solutions that include both architectures generally by incorporating what has been know for a very long time as a 'Federated Search'. That is, the ability to search foreign repositories as well as the local or 'proprietary' repository.

An integrated solution takes a record of Metadata and 'copies' of electronic documents (including emails) and stores everything in its own proprietary database. This database then includes records of all information for an organization including file folders, archive boxes, paper documents, electronic documents and emails as well as all transactional information. Ideally, everything is kept in a secure and inviolate state and managed according to best practice records management principles as espoused by ISO 15489. Everything will be backed up every night and religiously transferred to new media on a periodic basis to avoid media obsolescence.

The integrated RMS application controls and manages all data and protects it from outside interference using a security system; the application knows with absolute confidence where every item of information is because it is stored in its own database.

A federated RMS basically connects to and indexes information in any number of 'foreign' repositories, for example, the databases of other applications and URLs on the Internet. It does this using a federated search technique and a number of other tools that allow it to connect to the databases of other applications and access the information stored in them.

A federated search by its very nature (i.e., accessing the databases of other vendor's applications) has a few security problems of its own. You can't for example; access information in a foreign database without first knowing the database password and this is usually kept secret by the DBA. In order to surmount this formidable challenge most federated solutions use something called the Kerberos Network Authentication Service, http://www.kerberos.info/.

Kerberos provides an industry standard way for federated solutions to access foreign databases in a secure and fully authenticated manner. Anything else is called hacking.

However, being able to access a foreign information source is just the beginning of the problem. The real issue is that a federated RMS does not own or manage the information it indexes. It cannot for example, ever guarantee that the information it has just indexed will actually exist in a minute, a day or a week because it is not the application that actually manages and controls that information. Nor can the federated RMS guarantee that the foreign application is backing up and securing its database or moving its precious electronic documents to new media on a periodic basis. The foreign application could delete the information, move the information, archive the information or even rename it so it is no longer 'findable' under the same search.

This is the fundamental problem with a federated RMS; you have absolutely no guarantee of data integrity. You cannot guarantee to your compliance authority that you can produce the

information or electronic document you have previously indexed because you do not have a copy of the information, you just have a tenuous reference or link to it and you do not manage or control that information, someone else does.

This doesn't mean that federated RMS are inferior to integrated RMS, it just means they work in a very different way and that you need to ensure that your RM practices and procedures are cognizant of this and allow for this.

If you have information stored in your database you can guarantee its integrity, if all you have is a link to information stored in another application's database then you cannot guarantee the integrity of the information.

Email management is a good way to illustrate this difference between integrated and federated RMS.

In an integrated RMS copies of all corporate emails would be saved in the database of the RMS where they are secure and searchable and 'deliverable' at any time in the future. In a federated RMS the emails would be maintained within the email server (e.g., Exchange, GroupWise or Notes) where they can be deleted or archived by the IT person responsible for email. Once an email is either deleted or archived the link is broken and you will no longer be able to locate or produce that email in response to an e-Discovery request.

On the other hand, the oft-mentioned downside of the integrated approach is that you have to take copies and then use up a lot of disk storage. But, this is 2009 not 1980 and disk storage is cheap so I wouldn't expect anyone other than a troglodyte to make this an issue.

Obviously, makers of federated RMS products (e.g., IBM, Microsoft, and EMC) are smart people and are well aware of all the data integrity issues and provide functionality to address them. It is up to the records manager to ensure that the particular federated solution they choose both addresses and solves all of the data integrity issues arising out of the use of a federated architecture approach. In particular, the records manager needs to ensure that the federated RMS can deliver the electronic documents required under any future e-Discovery request.

Going back to my initial point, compliance isn't about software, it is about practice and procedures and it is the legal responsibility of the records manager to ensure that any RMS he/she buys, regardless of architecture, will allow the organization to meet any expected future discovery request. The fact that the software you bought is 'compliant' will be irrelevant if you can't produce the required documents in a discovery process.

My recommendation would be to select a hybrid system, one that incorporates both architectures to provide all options and the best of both worlds. Software architecture should never drive business solutions; business processes and requirements should drive business solutions.