Security Smart Buyer's Checklist

Use this checklist when investigating a potential cloud ECM vendor and when building or evaluating an in-house ECM storage system. Check all that apply.

Question 1: Was the software specifically designed as a cloud solution?

- ☐ Designed as a cloud system
- ☐ Multi-tenant software architecture

Question 2: What security features does the software provide?

- ☐ Customizable password complexity requirements
- ☐ Account lockout
- ☐ Session timeout
- ☐ Encryption of all sensitive data
- ☐ Customer information (including session IDs) is encrypted.
- ☐ Access can be limited to specific IP addresses.
- ☐ All function calls are verified for security access rights.

Question 3: How are my documents secured both during transmission and when stored?

- ☐ Secure Sockets Layer (SSL) encryption used during transmission
- ☐ 256-bit AES encryption used during storage

Question 4: How is information accessed?

- ☐ Web servers never access the secured network.
- ☐ Separate, dedicated servers (application servers) act as a go-between for the web server to access the secured network.
- ☐ Documents are not posted to a website for anyone to find. They are protected behind user passwords, and access is safeguarded by session ID encryption.

Question 5: Is the network where information is stored used for any purposes other than cloud services?

- ☐ No, it's used only for cloud services.
- ☐ The network is a separate, closed network.
- ☐ Inbound communication is reserved only for required services, and no outbound communication or traffic is allowed.

Question 6: Do you supply and manage your own security infrastructure or is it outsourced?

- ☐ No outsourcing is used. We provide and directly manage all security infrastructures.

Question 7: Is security verified on a regular basis by an independent third party?

- ☐ Yes, a third party tests network vulnerabilities and verifies system security.
- ☐ The system is tested on a daily basis, and reports are reviewed every day.

Question 8: What physical security and information reliability measures protect the data storage system?

- ☐ Physical access is restricted to required personnel with proper clearance and photo identification.
- ☐ Live monitoring of all facilities includes video recordings.
- ☐ Utility entry points are monitored.
- ☐ All networks have multiple entry points.
- ☐ On-site generators supply emergency power.
- ☐ Battery backup supports external power sources.
- ☐ Network administrator and engineer access is secured by RSA SecurID® two-factor authentication devices.
- ☐ Advanced HVAC system maintains constant temperature.
- ☐ Fire detection and suppression systems provide early smoke detection.
- ☐ A geographically diverse, redundant data center sits on a separate continental power grid.

Question 9: Where are the "single points of failure" within the system?

- ☐ There are no single points of failure. Multiple failures must occur before service is unavailable.
- ☐ All network equipment is monitored 24 hours a day, 365 days a year.
- ☐ System monitoring is not outsourced.
- ☐ Multiple redundant systems protect against service interruptions and data loss.
- ☐ Two or more data storage sites protect against service interruptions and data loss.
- ☐ Uptime guarantee is 99.9%.

Question 10: What is your disaster recovery plan as it applies to data restoration?

- ☐ Snapshots of all data are taken every two hours and stored for two months.
- ☐ Regardless of available storage space, snapshots are never destroyed ahead of schedule.
- ☐ Separate, fully redundant storage systems act as backups for the primary systems.
- ☐ The secondary storage sites are located in different geographic locations on different power grids.

- ☐ Within seconds, all data (including backup files) is synchronously mirrored at both sites.
- ☐ Switching between storage sites takes only a matter of minutes in the event of a catastrophic failure.
- ☐ No data restoration is required to activate secondary sites to become the primary site.
- ☐ Complete storage system failures can occur without any loss of data.

Now, add up the number of checked boxes. The more checked boxes you have, the more secure the system. Security matters!

ImageSilo®—Where Security Matters

ImageSilo is a cloud ECM service from Digitech Systems that both meets and exceeds the guidelines outlined here. With a 99.9% uptime guarantee, ImageSilo provides five layers of security, elaborate backup strategies and multiple redundant systems to mitigate the potential for failures affecting information availability. Add-on services such as email management, automated document routing and print stream processing create a customizable product suite. Outsource your data storage with ImageSilo and get secure online access to information anywhere, anytime—without capital expense or increased IT burdens. Ask us how you can leverage the benefits of ImageSilo to achieve a high return on investment!

For more information, please visit www.digitechsystems.com or call toll free 866.374.3569.