The Compliance Conundrum
Providing secure collaboration for financial services content via mobile and cloud

Sponsored by

Alfresco

AIIM
About the White Paper

As the non-profit association dedicated to nurturing, growing and supporting the user and supplier communities of ECM (Enterprise Content Management) and Social Business Systems, AIIM is proud to provide this research at no charge. In this way the entire community can leverage the education, thought-leadership and direction provided by our work. Our objective is to present the “wisdom of the crowds” based on our 80,000-strong community.

We are happy to extend free use of the materials in this report to end-user companies and to independent consultants, but not to suppliers of ECM systems, products and services, other than Alfresco and its subsidiaries and partners. Any use of this material must carry the attribution – “© AIIM 2013 www.aiim.org / © Alfresco 2013 www.alfresco.com”.

Rather than redistribute a copy of this report to your colleagues, we would prefer that you direct them to www.aiim.org/research for a free download of their own.

Our ability to deliver such high-quality research is made possible by the financial support of our underwriting sponsor, without whom we would have to return to a paid subscription model. For that, we hope you will join us in thanking our underwriter for this support:

Alfresco Software, Ltd
Bridge Avenue, The Place,
Maidenhead SL6 1AF
United Kingdom
Tel: +44 (0)1628 876 600
Web: www.alfresco.com

Process Used

While we appreciate the support of our sponsor, we also greatly value our objectivity and independence as a non-profit industry association. The market commentary made in this report is independent of any bias from the vendor community.

About AIIM

AIIM has been an advocate and supporter of information professionals for nearly 70 years. The association mission is to ensure that information professionals understand the current and future challenges of managing information assets in an era of social, mobile, cloud and big data. AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organisation that provides independent research, education and certification programs to information professionals. AIIM represents the entire information management community: practitioners, technology suppliers, integrators and consultants. AIIM runs a series of training programs, including the Certified Information Professional (CIP) course.

http://www.aiim.org/Training/Certification

About the author

David Jones is a Market Analyst with the AIIM Market Intelligence Division. He has over 18 years’ experience of working with users and vendors across a wide range of vertical markets. His experience has focused on taking complex technologies, such as business intelligence and content management, and developing them into commercial solutions largely in the retail, web and customer relationship management (CRM) areas. He has also worked as a consultant providing big data, data mining and ECM strategy and implementation solutions to clients worldwide. David has authored a wide range of papers discussing drivers and strategies for topics such as Social & Cloud Computing, Information Security, Big Data, SharePoint and Business Process Management. David has a BSc in Computer Science, and is a qualified CIP, ECM® and SharePoint®.
# Table of Contents

**About the White Paper:**
- About the White Paper ................................................................. 1
- Process Used ............................................................................. 1
- About AIIM ................................................................................ 1
- About the Author ........................................................................ 1

**Introduction:**
- Introduction .............................................................................. 3

**The Need to Collaborate:**
- The Need to Collaborate ............................................................ 3

**24/7 Information:**
- 24/7 Information ....................................................................... 4

**The Compliance Challenge:**
- The Compliance Challenge ......................................................... 5

**Moving to the Cloud:**
- Moving to the Cloud .................................................................. 6

**Hybrid ECM:**
- Hybrid ECM ............................................................................. 7

**Delivering Hybrid ECM:**
- Delivering Hybrid ECM ............................................................... 7
  - Insurance Claims ....................................................................... 8
  - Mortgage Application .............................................................. 8
  - Investment Banking ................................................................. 9

**Conclusions:**
- Conclusions ............................................................................. 9
- References .................................................................................. 9

**Underwritten in part by:**
- Alfresco ..................................................................................... 10
- AIIM ......................................................................................... 10
Introduction

Financial services organisations still find themselves at the early-adopter stage for many new technologies.

This heavily regulated industry provides a very public stage for any misdemeanours, due in part to the personal nature of much of the information managed, but also due to the large amounts of money involved. This has manifested itself into an overly conservative IT stack, delivering sub-standard, dated systems, with little or no collaboration facilities or mobile access – forcing users to take drastic and completely un-regulated action to get these facilities.

While many industry sectors are experiencing the benefits of cloud and mobile access to information, financial services organisations lag behind. These organisations no doubt have a need to share information outside of their own metaphorical four walls – whether sharing information with clients, collaborating with para-planners, or creating Memorandum of Understanding (MOU) documentation for investment deals.

In fact, despite the recognised dangers of doing so, these information assets are being shared with these parties already – but not via routes planned and secured by the organisation. They are being shared by email, USB stick or cloud-based file-shares – and the reality is that this unauthorised information sharing is not only potentially damaging, but is likely to be making the organisation non-compliant in the eyes of their regulators.

In addition to the need to collaborate, those employed within the financial services industry are subject to the same trends and fashions as everyone else in that many now own and use their own tablets, mobiles and cloud-based services for work purposes. These employees are not trying to be subversive and awkward for the IT department – indeed they are often trying to work outside of the office and beyond office hours – but in many situations the facility to access information remotely is performed by substandard and dated interfaces. In addition, un-managed, and unplanned-for, mobile access can create more problems than it solves.

Furthermore, the elephant in the room for both collaboration and mobile access is compliance – or more specifically the absolute need to remain within the very strict and tightly-policed financial service industry regulations. So should the financial services industry continue to stand on the sidelines of the modern IT playing field, or can new technology solve the very problems that it appears to have created?

One technology, hybrid ECM, appears to be able to do this. It aims to provide a platform to allow organisations of all types to maintain strong governance and management protocols over their information, while securely opening up the information for sharing and collaboration. It delivers this securely via the cloud, for use by the right people, in the right context, on the right device – whatever that combination might be.

This paper defines the conflicting informational desires and challenges facing the modern financial service organisation. It explains in detail the approaches used by hybrid ECM solutions to expose, information resources in a secure way, and provides a use case for how this could be applied in-situ. It concludes with a series of recommendations for how organisations can use hybrid ECM to securely share their information assets.

The Need to Collaborate

Financial services organisations and employees are no strangers to collaboration – even simple tasks such as the authorisation of an application for a new bank account requires input from numerous sources, but improving the productivity of collaboration is crucial as finance organisations seek a return to profitability and efficiency after the banking crisis.

Indeed, the need to collaborate and its value is not in question – but the ability to perform this collaboration electronically, as efficiently as possible, and increasingly with entities beyond the organisation itself, most certainly is up for debate.

Internal collaboration is an area that is largely understood and slowly, but surely, is starting to deliver benefits to organisations. In an ideal world that would be all that was needed, but pretty much every complete business process requires input from something or someone from outside of your team, department or even business – hence the need for external collaboration.

This need is often met with a strong arm from internal IT departments – the electronic equivalent of mile-high walls, topped with barbed wire and covered by security cameras. The IT department in their minds are
purely doing their best to ensure the security of the information assets of the organisation, but that does not help the general user. Indeed where restrictive IT infrastructures are in place, users are being forced to find alternative ways to collaborate and get their jobs done effectively.

AIIM research (Figure 1) highlights just how many employees - and their managers - are resorting to using so-called “freemium” cloud file stores to share documents outside of the firewall – with 60% of respondents definitely using these. These alarming figures do not just illustrate how innovative modern users have become – but also the extent to which corporate information is being exposed on public cloud services, many of which, by their own admission, certainly do not have enterprise-level security and compliance facilities.

Figure 1: To what extent do you think your users or managers are bypassing on-premise content management in an ad-hoc way (for example by sharing documents with external partners via Googledocs, Dropbox, iCloud, etc.)? (N=307)

24/7 Information

The Compliance Conundrum - Providing secure collaboration for financial services content via mobile and cloud

Of course, collaboration is just one aspect of the changing and conflicting needs of a modern financial services organisation. The massive increase in the use of mobile devices and the growing migration towards a Bring Your Own Device (BYOD) to work culture has an equally profound effect.

Research by online retailer Pixmania\(^1\) shows that smartphone owners are working 460 hours a year above and beyond their contracted hours – largely by checking emails on these devices - and this would appear to be just the tip of the iceberg. Device capabilities are constantly increasing, and integration to work processes is becoming deeper and more engaging – meaning that usage will become increasingly detailed, immersive and time-consuming. Indeed, AIIM research has shown that 33% of organisations, expect to see “half or more” of their employees using iPads, tablets or digital clipboards for filling in forms in 5 years time.

From a Financial Services perspective mobile and tablet device usage offers numerous benefits: not only can employees and customers access up-to-date information on products and policies, but they can interact with business-specific processes – customers being able to request changes to a travel insurance policy while on holiday, brokers managing stock portfolios in the airport lounge, or loan applications signed on tablet devices in the home of the client for example.

This growth in mobile access to organisational data and processes increases the number of possible touchpoints through which data needs to be accessed. Whether it is sharing information to partners, checking email on a mobile, or getting a client signature on a tablet device, there is now a growing need to extend organisational data beyond the firewall – but of course, every piece of information and interaction that is to be viewed or actioned in this way poses a number of compliance and security challenges for the organisation.
The Compliance Challenge

We have discussed above the numerous benefits to be had both by mobile access and collaboration, but many of the people currently running IT departments in financial services organisations are arguing vehemently against this. These people have been charged with providing systems that not only allow the business to operate as efficiently as possible, but also to ensure that these systems are disaster proof, secure beyond question, and entirely compliant with industry regulations. They now find their users and superiors demanding interaction via tablets, collaboration with external organisations, and mobile capture of forms and signatures – all the while with the same levels of security, compliance and efficiency.

Compliance itself comes in many forms: basic information governance; the need to ensure privacy and security of personal and financial information; and anti-money laundering reporting and enforcement (which is expected to cost banks $5.8m in 2013). Each of these flavours of compliance has its own nuances but, in general, there are three main areas of pain for those trying to balance compliance, security, and information governance with flexibility, collaboration and mobile:

Technically exposing content beyond the firewall is not simple. Any legacy systems that are in place will either need to be modified or upgraded. The organisation will need to decide whether to stipulate which mobile devices and platforms they will support, provide numerous device specific apps, or run with simple to manage but ultimately unsatisfactory VPN and/or remote desktop facilities. Ensuring security for either of these instances is an ever changing and challenging field, however, there are solutions available to deliver these facilities – whether as a whole new implementation, or component-based as add-ons or interfaces to existing systems.

Financially the costs of compliance failure and security breaches are scary – and the risks come from both inside and out. In 2010 a Bank of America employee leaked customer information to an identity theft ring at an estimated cost of $10m, whereas in 2011 Citibank servers were compromised with hackers gaining access to 360,000 customer details, at an anticipated cost of $2.7m.

Interestingly research by the Ponemon Institute identified that the more effective the security strategy that is in place in an organisation, the lower the cost of non-compliance. This highlights that even those who are fully prepared will have breaches at some stage, but those with their house in order at least are able to minimise the effect and cost of those breaches – presumably being able to lock down much sooner, and restrict access to other areas of the information.

Politically many organisations are naturally nervous of exposing themselves outside of their own environment and also of failing to maintain their information governance. Indeed, Figure 2 shows which types of risk organisations feel are the biggest in relation to failing information governance. The same survey indicated that 28% of the largest organisations (over 5,000 employees) have been fined or suffered poor publicity in the past three years as a result of accidental loss or exposure of customer or staff-sensitive data. In 38% of cases, the financial impact of fines, damages or costs resulting from poor information governance were substantial, and in 8% it was dramatic. For example, some of the biggest fines on banks from regulators have been imposed for failure to observe anti-money laundering requirements, which mostly involve keeping accurate records of due diligence.

Given the sensitivity of the information that is stored by financial service firms, they find themselves in a situation akin to public sector organisations, hospitals, schools and other institutions handling personal, delicate data. It is interesting to see that inability to respond to information requests and infringement of industry specific compliance regulations rank fairly low in the list as risks – dwarfed in-fact by higher profile financial and negative publicity aspects.

But the risks do not necessarily outweigh the benefits. The lead being taken by the European Court of Human Rights by making use of cloud-based content management demonstrates how organisations can balance the risk and reward aspects at play here, and can be used as suitable evidence when organisations are required to make an internal business case for moving towards an on-premise implementation.
Moving to the Cloud

Having stoked the fire by exploring the need to expose content outside of the firewall, and then having poured a little water on it by balancing all of the potential technical, financial and political challenges associated with actually doing it, it is reassuring to discover that there are tools and techniques available to satisfy both parties.

One of the mechanisms being used to enable the deployment of information outside of the firewall is that of cloud services. Adoption of the cloud in any guise has previously been somewhat indifferent – often due to concerns about data location and security. More recently a shift in perspective appears to be occurring, with 46% believing that the cloud will be the location of choice for document and content management within 3 years.

This shift is being fuelled somewhat by private uptake of cloud-based file sharing services such as Box and Skydrive (as discussed earlier), which provide the simplest form of content management in the cloud. Other options available to financial service organisations include completely cloud-based content management systems (with all data and management in the cloud), cloud-based access systems (where management facilities exist in the cloud, essentially providing a web-window to on-premise information), and various combinations of both of these – known as hybrid ECM solutions.

Hybrid ECM

The term “Hybrid ECM” is used to describe a solution that combines the benefits of an on-premise and cloud approach.

Hybrid ECM sees the main data repository of information sitting on-premise within an organisation – with access to that information from within the firewall operating as a standard on-premise solution. In addition a cloud-layer exists that provides a collaboration area for selective pockets of information that need to be accessed or shared outside of the organisation. This information can only be accessed by authorised users and these pockets of information are subject to 2-way synchronisation, ensuring that they are up-to-date and maintained as if they were sitting in the on-premise system.
Delivering Hybrid ECM

This hybrid approach has significant benefits for financial services organisations. The cloud layer should only store information that needs to be shared at any given time – maybe for a specific loan account or insurance transaction – therefore ensuring that content remains within the governance regime and controls of the main on-premise solution, unlike alternative custom-build integrations to some popular consumer cloud solutions. The cloud system is running in tandem with the on-premise system, so any existing permission integrations are maintained in the cloud layer, ensuring consistent application of taxonomy, classification and permissions to both systems. A further benefit is that any workflows that operate against the various information assets will continue to function – something that is not always possible with cloud-based solutions as many do not provide enterprise-level workflow components.

Sensitive information, such as that of a personal nature, is of particular concern to the financial sector in relation to being exposed in the cloud. For such information the hybrid solution will ensure that only suitably authorised users have the ability to expose this data, and that appropriate approval mechanisms are followed before it could be published to the cloud (if at all) – greatly reducing the levels of security risk associated with deploying a pure cloud solution.

It appears that users are becoming aware of the benefits of hybrid solutions – AIIM² have found that 38% would rather use a hybrid solution linking cloud and on-premise than a pure cloud system.

And there is more to hybrid ECM than just content access. The secure level of integration that the hybrid ECM platform provides to on-premise information and processes provides a perfect touchpoint for mobile content creation and capture - be it using an on-board camera, a touchscreen to accept a signature, registering location via GPS, or even using face-recognition as an authentication method.

In the same way that only authorised users can access information, only users with sufficient authority will be able to make use of these facilities, or typically will have limited means of interacting with these remote workflow processes – for example, a user may be able to enter data into a limited number of fields on a mortgage application form, or sign their name to accept an insurance contract, but only an authorised user will be able to submit the complete application.
These new levels of mobile engagement and collaboration, both access-based and interactive, need to be carefully managed. This can be controlled in a number of ways – the ideal being contained in so-called workspaces, suitably extended to provide container-based applications for remote devices – ensuring that content can only be accessed once user-level authentication has been performed on the device itself.

This workspace would have a defined group of participants – each with specific rights – a defined set of content, and a cluster of appropriate workflows. While being “hosted” in the cloud, the workspace would fall under all of the same user, content, taxonomy and governance regimes as any on-premise content. This alignment of metadata and taxonomy becomes especially important when content created “in the cloud” needs to be brought into a records management regime once back on-premise.

This combination of controlled access to on-premise data, collaborative workspaces, single monitoring point for on-premise and mobile workflows, and robust mobile security make hybrid ECM a compelling option for financial services. Such a solution can help organisations satisfy both their business users’ desire to remotely access and collaborate on information, and in tandem expose the benefits of social and mobile access to organisational content - while still remaining within the required governance frameworks and ensuring enterprise-grade security.

**Insurance Claims**

The claims process that follows an automobile accident is complex and involves numerous parties. XYZ Insurance implemented a Hybrid ECM solution that allows the insurance agent handling the claim (Tom) to manage the various information assets and interested parties throughout the process. The client calls Tom and he enters the basic claim information into the XYZ systems. The XYZ business process engine kicks into gear and auto-generates a series of forms: some for the client, some for the independent claims adjuster, and some for Tom.

Tom is then able to make the relevant forms available to the client via a private, yet cloud-based workplace – an area that the client can log in to and complete the forms, but also upload any other relevant information such as images of the vehicle and the accident site. Once Tom has received these he can make these and other relevant content available to the claims adjuster, who can determine whether he needs to arrange a visit to view the vehicle, or whether enough information is already available. The adjuster can then in turn complete his forms and upload any additional content such as repair estimates or further photographic evidence.

Throughout this process, both Tom and the client can see exactly what information is available and missing, and what stage the claim is at. In addition, XYZ have significantly reduced their costs: capture and data entry are being performed by the client at no cost to XYZ, and the claims adjuster may not even need to visit the vehicle if the online evidence is sufficient.

**Mortgage Application**

A mortgage application is one of the most important financial transactions any individual will encounter in their lifetime, and as such requires a large number of documents and form filling – all of which needs to be verifiable and accurate. ABC Bank have integrated their website with their hybrid ECM platform to allow users not only to fill out mortgage application forms online, but to then continually monitor the application process as it continues. The system has also been extended to provide areas for documentation from surveyors, planning departments, county councils and the bank itself – each area accessible only by the relevant entity.

The whole process is governed by a number of integrated workflows – for example, informing surveyors that a property needs to be viewed, then sharing the results of that survey with the bank’s mortgage executives and the customer themselves. The integration not only means that all parties are 100% aware of where the process is, but also reduces the need for numerous in-person visits, potentially allowing the bank to take mortgage applications from a much wider geographical area. Alternatively, it could be used to increase the number of on-site meetings, with the mortgage executive, and potentially the estate agent, being able to capture documents and any relevant signatures from the customer via a mobile or tablet device.
Investment Banking

The world of investment banking may appear to be murky, confusing and full of intrigue to many, but for those involved it is a series of relatively simple banking transactions and processes - all of which are preceded and backed up with significant amounts of documentation. Not only are there requirements for application forms and standard proof of identification for the individuals involved, but more often than not Proof of Funds (POF) documentation is also required.

INV Capital have utilised a hybrid ECM solution to allow the parties involved, who may be based anywhere on the planet, to self-capture and upload this evidence and any other required documents - business plans, offtake agreements, guarantee letters, and the like. INV have also integrated a 3rd party digital signature solution, removing the need for physical documents to be signed and couriered around the world – massively reducing the amount of time normally associated with assembling all of the ingredients in one place to start the investment process.

Throughout the whole process, enterprise-grade security is in place for all of the documentation, ensuring the utmost privacy for the institutions and individuals involved. Furthermore all content is synchronised back to the on-premise ECM system for storage, only exposed via secure workspaces when needed.

Conclusions

Financial services organisations would appear at first sight to be in a no-win situation. They deal on a daily basis with information of a sensitive, personal, or financial value - all of which needs to be managed under the very critical eyes of industry regulators. They are however, increasingly being placed in a position where this information needs to be generated, accessed, and shared outside of their own systems. Unfortunately, the painful publicity and severe financial penalties associated with compliance and security breaches have led financial organisations to shut up shop, to batten down the hatches, and refuse to expose their information assets – but this has led them to miss out on the significant potential benefits associated with turning their information loose.

This paper has tried to deliver a balanced discussion on the subject. It has explored the reasons for opening up the information access channels, but has also countered the argument by highlighting the challenges of doing this, and some of the penalties of getting it wrong.

But moving forward, a win-win scenario appears to have emerged. Hybrid ECM allows financial services organisations to deliver on the benefits of collaboration, mobile access and “in-motion” information, while at the same time providing the compliance and security safeguards that are required by the enterprise. The use cases have touched on some examples of how hybrid ECM can streamline existing processes simply by involving customers and partners, earlier and more often.

There will still be doubters within the organisation – those who feel that the risk of exposure is too great. The businesses that allow these negative voices to overwhelm those looking to progress down the road of secure but open data, collaboration and mobile will be those who suffer. The organisations that do adopt more progressive information governance and management will benefit in the long term, with happier, more informed clients, more engaged, effective staff, and with financial savings and profit being the icing on the cake.

References

1. Daily Telegraph - Smartphones and tablets add two hours to the working day
   http://www.telegraph.co.uk/technology/mobile-phones/9646349/Smartphones-and-tablets-add-two-hours-to-the-working-day.html
2. AIIM Content in the Cloud Industry Watch 2012
3. FAST enterprise search at core of European Court of Human Rights website
4. The True Cost of Compliance – Ponemon Institute, January 2011.
5. Financial Crime Compliance and Failure
6. AIIM Information Governance Industry Watch 2012
About Alfresco

Alfresco is how great businesses share, organise and protect their content. Nearly 7 million people in over 180 countries use Alfresco Enterprise, Cloud and Mobile to manage over 3 billion pieces of content worldwide. Whether on the go or in the office, Alfresco empowers today’s teams to do great work. And, with 1 in 8 Alfresco customers operating in the financial services sector, there are compelling reasons why these customers are choosing the freedom of open source with Alfresco.