MIFID2: Are you ready for the new era in record-keeping?

Who this paper is for:
Compliance, Legal and IT MIFID2 decision makers that need guidance on how to become strategically compliant with MIFID2 record-keeping whether they do or do not have an existing content-archiving system.

pwc

This consultation paper deals with strategic record-keeping operations. It explains how ad-hoc record-keeping under MIFID2 will be detrimental to firms in the long run. First the problems of ad-hoc record-keeping are explained, and then it is shown how these problems can increase the risks of failure to comply with MIFID2. A strategic programme that solves the problems of the ad-hoc approach is proposed and outlined. The reduction in these problems and risks is demonstrated to prove how a strategic programme can help ensure compliance with MIFID2 record-keeping, all the while maximising the operational efficiency of the record-keeping programme itself.

Introduction: MIFID2 raises the stakes

With the MIFID2 regulatory regime beginning on 3 January 2018, EU-based financial firms will not only face a new era of heightened record-keeping involving many more records than was previously required, but also the negative effects of new oversight, monitoring, e-discovery and forensics processes for the firm's clients and regulators. MIFID2 record-keeping will not just be about expanded content archival – it will deal with its implementation in a way that will help firms best execute processes in a strategic and efficient manner.

The task faced by management teams to ensure their firms are compliant with MIFID2 record-keeping may be daunting given the complexities of the directive and its regulations. We feel this task is best completed by way of an overall approach to record-keeping operations, culminating in the decision to create a firm-level "programme" that is designed to handle all the new requirements posed by MIFID2 – as opposed to ad-hoc, tactically focused processes, which ensure minimal compliance with great risk and little preparation for the processes of oversight, monitoring, e-discovery and forensics. With a strategic programme, firms will have the means to ensure record-keeping compliance and be prepared to effectively deal with the negative effects of MIFID2.

Ultimately, a robust and strategic record-keeping programme should encompass a process of integrating content archiving into the management of line-of-business applications from the very first day of MIFID2. This process should put operational archiving best practices into place to ensure that records are archived in such a way that their state and inventory are always known - thus making oversight, searching and retrieval easier in the future.

The problem: the ad-hoc approach

The record-keeping of business-generated content is often an afterthought in the management of line-of-business applications, and a common belief is that record-keeping is merely something to be dealt with at the end of the operations process, often by backing up or storing data into a content archiving system. But a problem arises here, for firms often think that because they are backing up or archiving content in a digital archiving system, they are performing proper record-keeping. While backup or content archiving may meet the barest of MIFID2 recording requirements, they cannot meet all of them, especially those regarding ease of retrieval, monitoring and oversight.

The central problem with ad-hoc record-keeping is the inherent risk of a "content blackout". This situation occurs when data that must be archived is not actually archived, or worse, that the lack of archiving goes undetected until the data is required for business, compliance, regulatory or legal reasons. If the time gap is small, then remediation actions can be carried out, but the longer a blackout occurs, the less chance the original data can be recovered.

Furthermore, a content blackout does not necessarily require a complete loss of data. If certain data is not properly classified and inventoried, then it could indeed be somewhere in the archives but is probably difficult to find without removing large volumes of data from the archives and processing it through a big data system to reclassify it –at significant expense.

With most business now being conducted electronically, a content blackout is one of the most troublesome things that a modern financial institution can face. Without proper business records, any number of things can go wrong with customer service, compliance, audit, regulatory inquiries and legal actions – not to mention the needs of the firm to search for their own data for business purposes.

In the modern, technology-driven era, ensuring the proper collection, monitoring, inventory and distribution of archival content across several content generating and consuming systems is as important as the archiving of the content itself. Archiving and content management systems are only as good as the ability of the firm to get the content into its archives.

Complexity: MIFID2 record-keeping requirements

MIFID2 creates high demands on record-keeping, both on the breadth of content to be recorded and its accessibility for inquiry by clients and regulators.

In general, MIFID2 record-keeping obligations can be categorised into three types of data, as demonstrated in the following table:

Content Type	Storage on Unalterable Medium	Minimum Retention Period
Orders[1] & transactions	Yes[2]	Minimum 5 Years[3]
Telephone & electronic communications (Including written notes from in-person meetings)[4]	Yes[5]	Minimum 5 Years, maximum 7 Years[6]
General records on clients, orders and transactions[7]	Yes[8]	Minimum 5 Years, maximum 7 Years[9]

While MIFID2 makes little distinction between the three categories, we feel a record-keeping programme should look at all three categories as a whole, and apply record-keeping policies uniformly across all three categories.

This paper does not intend to provide a thorough summary of MIFID2 record-keeping requirements, as many resources can already be found on the Internet and on ESMA's website. Ultimately, your legal and compliance team will have to determine which parts apply to your organisation. We have nevertheless compiled a brief summary;

- Records must be stored in a durable medium.

- Records must not be altered. As finance is now an industry driven by computer data, this generally means that any records generated in software-based applications must be stored in a "write once, read many" digital medium – often called "WORM storage".

- Records must be kept for a minimum of 5 and a maximum of 7 years – even longer for records where special client relationships exist.

- MIFID2 demands strict oversight over the management and operations of record-keeping.

- It also demands the periodic monitoring of the record-keeping programme and its content, which can further complicate matters.

- Content must be recorded so all steps in a transaction can be reconstructed.

- Lastly, it requires content to be "readily accessible" – in the digital era, this basically means in near real-time.

The primary goal of management and operations teams in MIFID2 record-keeping planning is to ensure compliance with the above topics, and eliminate all content blackouts and the negative effects which go with them.

[1] MIFID2 Directive: Article 16(6) & MIFID2 Delegated Regulation: Section 8, Articles 74, 75
[2] MIFID Implementing Directive: Section 8, Article 51(2)
[3] MIFID Implementing Directive: Section 8, Article 51(1) & MIFID2 Delegated Regulation: Section 8, Article 72
[4] MIFID2 Directive: Article 16(7)
[5] MIFID2 Delegated Regulation: Article 76(10)
[6] MIFID2 Directive: Article 16(7)
[7] MIFID2 Delegated Regulation: Section 8, Article 72(2), 73, 74, 75 & MIFID2 Delegated Regulation: Annex I
[8] MIFID2 Delegated Regulation: Section 8, Article 72(1)
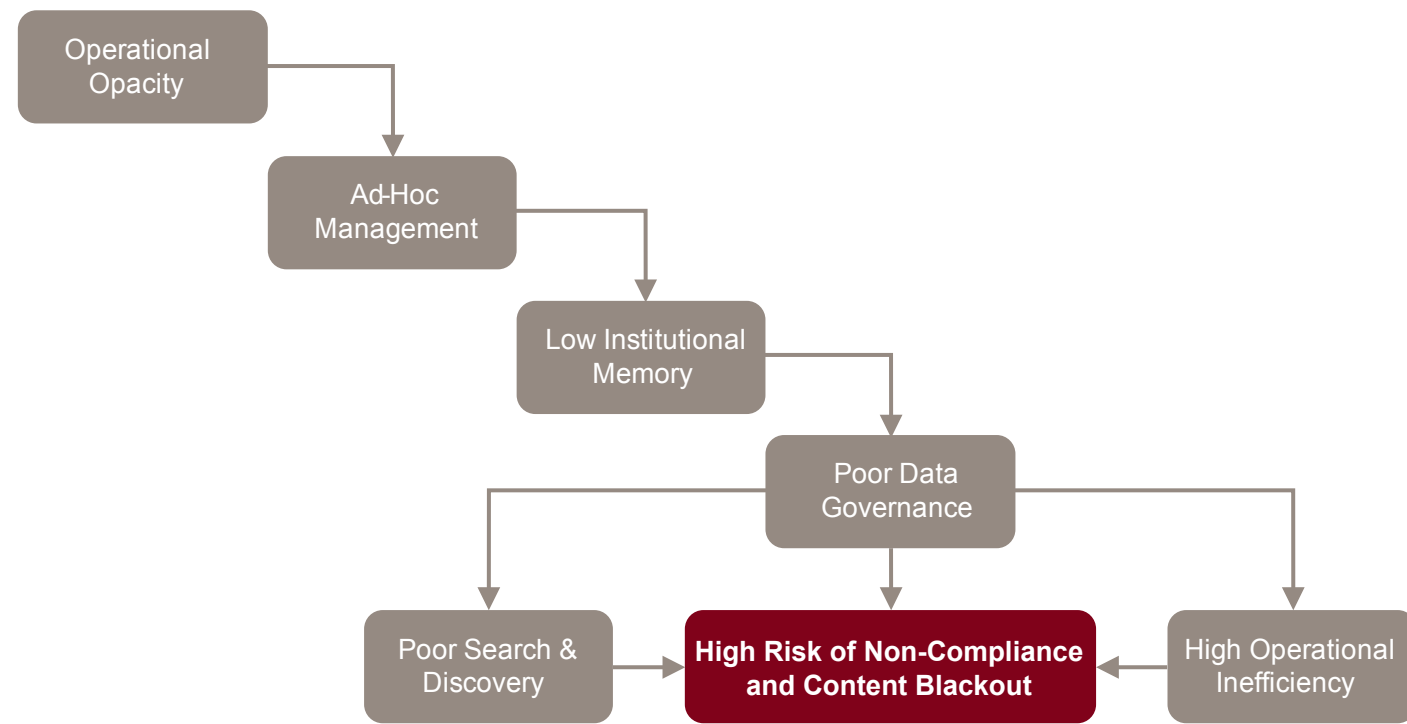[9] MIFID2 Directive: Article 16(7)

The negative consequences of poor record-keeping

The previous section explained that MIFID2's record-keeping requirements are broad and impact many areas of a firm's business and technology operations. What, then, are the possible negative consequences of ad-hoc record-keeping?

The problems outlined below describe a snowball effect where poor processes lead to the emergence of operational failures in process and workflows that are necessary for MIFID2 record-keeping compliance. These consequences often do not fully manifest until months or even years after ad-hoc record-keeping has begun – typically during a legal,

information to find both the content and the context by which the content was created and collected? Will this be done in a timely manner as dictated by MIFID2? Looking beyond MIFID2, will low or fragmented institutional memory suffice for GDPR compliance?

- Poor data governance – With low institutional memory often comes poor data governance. A firm must be able to answer the following questions to maintain a firm grasp on the inventory and state of record-keeping.
  - Who created the data?
  - Which data was created?
  - Where was the data created?

- How was the data created? (Which processes)
  - When was it created?
  - When was it collected and archived?
  - Who or what has received the data?
- Difficult search & discovery – The inefficiencies of low institutional memory and poor data governance snowball to make data searching and exporting more difficult. Monitoring becomes compromised due to the risk of not being able to readily see content subsets or supersets. The inability or lengthy amount of time needed to gather records for exporting will lead to greater exposure to regulatory fines,

sanctions and reputational risk.
- High operational inefficiency – The above-mentioned consequences can ultimately lead to the need for a multitude of manually-driven processes and checklists across systems and IT verticals, which results in the firm spending more money than is necessary (e.g. on labour) just to keep ad-hoc record-keeping afloat.

The overall effect of this failure is a high risk of content blackout and non-compliance with MIFID2. The following table outlines the consequences of ad-hoc record-keeping and their impact on MIFID2 compliance:

Negative cascading effects of ad-hoc record-keeping.

regulatory or financial situation when the stakes are the highest.

- Operational opacity – Modern financial firms will have a multitude of MIFID2 content-generating systems. When ad-hoc and patchwork processes are implemented as an after-thought to line-of-business application record-keeping, how can effective record-keeping oversight be done across a patchwork of processes and multiple systems? How can compliance personnel in charge of

oversight examine the current state of record-keeping in an effective manner? How can efficient and standardised monitoring be achieved across the environment upon installation, and in the future when technology and the organisation of the firm evolve?
- Ad-hoc management – Which individuals will have oversight of the process? Will they have direct or shared responsibilities? Will management be done via applications or infrastructure silos with different processes, without a common reporting mechanism? Will

process and reporting workflows be done via spreadsheets and emails? What happens when people come and go within the firm, or when the firm itself changes by way of mergers and acquisitions?
- Low institutional memory – Operational opacity and ad-hoc management often lead to low or fragmented institutional memory, especially when management-related tasks are performed on spreadsheets and via emails. When the time comes to produce records, will there be enough

MIFID2 Requirement (Heavily para-phrased)	Ad-hoc Consequence	Negative Operational & Regulatory Effect
Management should have effective oversight and control over policies and procedures and the recording of phone and e-communications. DR: 72(3) & 76(2)	Operational opacity	Reduces oversight and archiving process monitoring abilities with lack of centralisation, standardisation and transparency.
	Ad-hoc management	Inability to effectively define roles and responsibilities jeopardises oversight, the assignment of management responsibility and the distribution of responsibilities as the firm evolves.
MIFID2 requires content to be readily available for inquiry and content reconstruction. DR: 72(1)a/b **Records must be monitored periodically.** DR: 72(6)	Low institutional memory	Incomplete institutional memory makes content more difficult to find for inquiry and monitoring.
	Poor data governance	Greater effort to track data lineage and content types for reconstructing financial transaction history for search, monitoring and discovery. Content blackouts leave gaps in data, creating search gaps for monitoring and discovery. Visibility of data for GDPR also affected.
MIFID2 requires content to be readily available for regulator or client inquiry. DR: 72(1) & 76(10)	Difficult search & discovery	Greater effort to collect relevant records for regulatory or client inquiry and monitoring. Mounting problems may lead to content blackout in inquiry.
No MIFID2 requirement for operational efficiency.	High operational inefficiency	All the above result in spending more time and money to maintain record-keeping operations, for less than optimal results.

The strategic approach to record-keeping

Keeping in mind ad-hoc content archiving is not proper record-keeping, what would a proper record-keeping programme for MIFID2 look like?

With a strategic programme, a firm-wide policy is created to address the overall record-keeping needs of the company. Content archiving becomes an integral part of the process of managing line-of-business applications, and the processes that generate MIFID2 content. Operational content collection and archiving and monitoring best practices are implemented to solve the problems of ad-hoc record-keeping – but how exactly do we get from what needs to be done to the actual implementation and execution? What exactly are these "operational best practices"?

The key lies with the MIFID2 Delegated Regulation, which outlines the formal and operational requirements for investment firms. Specifically, in Article 76:

- Article 76(1) - Firms must establish a clear written policy on which electronic records they will save.
- Article 76(2) – The firm's management body should have effective oversight and control over its relevant policies.

It is clear from these two sections that a policy must be developed, and that this policy must serve as a template for the oversight of electronic records. If we think strategically, such policy requirements need not be confined to electronic communications, but to all the firm's records saved under MIFID2. Orders, transactions and general business records stand to benefit from a firm-wide policy. If we extend the policy and add an operational framework with procedures to implement it, we have the core of a strategic record-keeping programme. The key elements of this programme should include:

A strategic programme as the union of policies and procedures.

Electronic Communications Policy

Strategic Record Keeping Programme

Operations Process & Procedures

E-communications extended to General Record Keeping Policy

1. Definition of the overall programme
2. Policy on record-keeping, specific to each content type
   a. Policy on creation of content in non-communication systems
   b. Policy on usage and creation of content in communication systems
3. General organisational oversight of the programme
4. General organisational roles and responsibilities of the programme
5. Process for on-boarding new content types
6. Process for decommissioning outdated content types
7. On a per content basis, the following standardised processes and procedures:
   a. Collection
      i. Identification of content to be collected (general business information)
      ii. Technical definition of content to be collected (technical systems information)
      iii. Categorical definitions of content to be collected (data classification)
      iv. Processes for data collection and preparation for archiving
      v. Identification of content ownership (business, technical and vendor)
      vi. Definition of unique identifiers (people, applications and algorithms)
      vii. Definition of content connectivity (process of connecting different users, systems and content IDs across systems)
   b. Archiving
      i. Process of archiving content
      ii. Reconciliation of collection processes for archiving processes
      iii. Workflow for break-fix
      iv. Vendor management
   c. Monitoring
      i. Process of monitoring content archiving
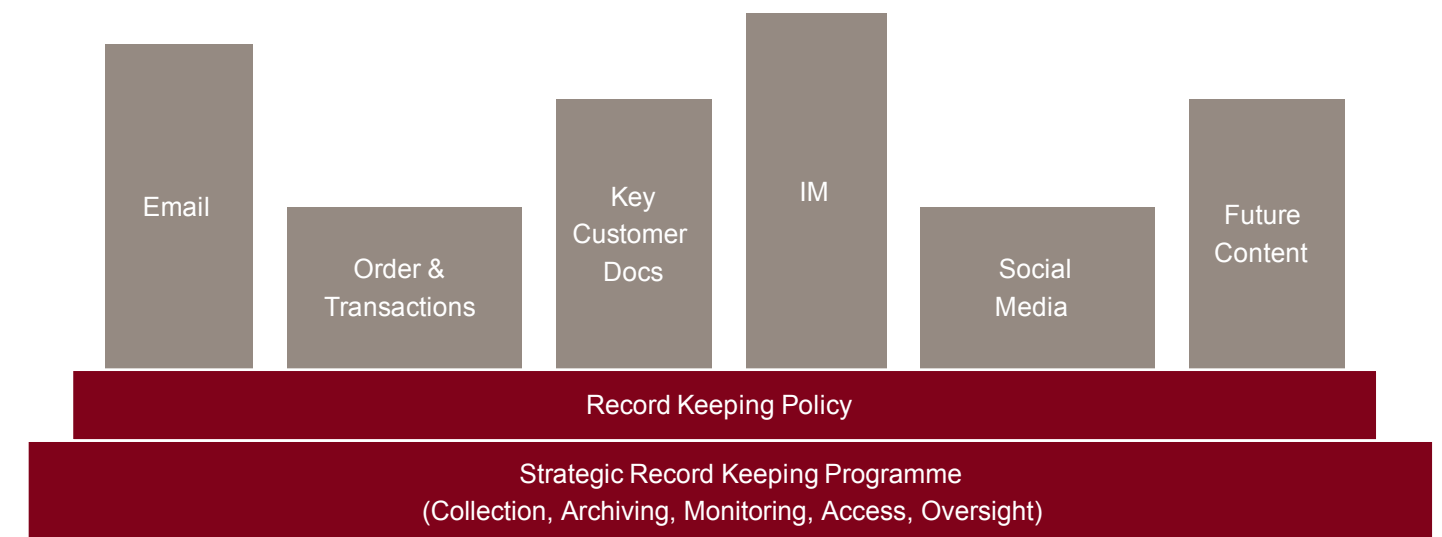   ii. Identification of active vs passive collection (where source content counts are known or unknown)
      iii. Boundaries for alerts
      iv. Workflow for break-fix
   d. Access - Distribution
      i. Process of managing content accessibility and distribution
      ii. Audit of accessibility and distribution
   e. Oversight
      i. Process of oversight and the audit of content creation from archiving lifecycle
      ii. Reporting mechanisms for all stakeholders

With the above-listed elements in a written programme, firms will significantly increase their compliance with MIFID2, all the while reducing the risk of content blackouts and the negative effects of ad-hoc record-keeping.

Regardless of content silo, a strategic record-keeping policy will provide the basis and foundation for a robust record-keeping programme.

Email | Order & Transactions | Key Customer Docs | IM | Social Media | Future Content

Record Keeping Policy

Strategic Record Keeping Programme
(Collection, Archiving, Monitoring, Access, Oversight)

Problem solved: robust record-keeping

With a robust operational framework in place, firms will get a head start on future ad-hoc record-keeping issues and reverse the consequences outlined above, and at the same time enjoy the following benefits:

- **Operational transparency** – IT administration and management oversight personnel are on the same level and have access to the same operational processes and summary data. All success and failure is completely transparent. With comprehensive knowledge, the firm can deal with problems instead of being blind to them.
- **Systemic Management** – Ownership of data and tasks are clearly defined, and chains of custody exist for data and the operational processes surrounding the collection, archiving and distribution of content. The firm has a means to detect and respond to client and regulatory "fire drills".
- **High institutional memory** – Institutional memory now exists for the firm's records, independent of the personnel that may come and go or changes to the firm itself.
- **High data governance** – You now know the full data lineage of all generated content. It is saved as institutional memory and can be accessed without having to export the archives en masse to reconstruct lineage.

- **Easy search & discovery** – The efficiency gained will result in less time, effort and money to recover data when faced with regulatory, compliance, audit and legal inquiries.
- **High operational efficiency** – With the removal of redundancy and the centralisation of tasks, the firm is spending money more efficiently to manage its record-keeping operations, thus making one of the most burdensome requirements of MIFID2 easier to comply with.

If we apply the strategic approach to our previous table, we can extend the table to demonstrate the positive benefits in a global manner:

MIFID2 Requirement (Heavily para-phrased)	Ad-hoc Consequence	Negative Operational & Regulatory Effect	Strategic Solution	Positive Operational & Regulatory Effect
Management should have effective oversight and control over policies and procedures and the recording of phone and e-communications. DR: 72(3) & 76(2)	Operational opacity	Reduces oversight and archiving process monitoring abilities with lack of centralisation, standardisation and transparency.	Operational transparency	Makes oversight easy to accomplish, and allows for robust firm responses to issues via standardised and centralised processes and procedures.
	Ad-hoc management	Inability to effectively define roles and responsibilities jeopardises oversight, the assignment of management responsibility and the distribution of responsibilities as the firm evolves.	Systemic Management	With a system in place, the firm can ensure direct administration and oversight responsibilities, which in turn serves as an essential control function for the record-keeping programme.
MIFID2 requires content to be readily available for inquiry and content reconstruction. DR: 72(1)a/b **Records must be monitored periodically.** DR: 72(6)	Low institutional memory	Incomplete institutional memory makes content more difficult to find for inquiry and monitoring.	High institutional memory	With a programme and processes in place, the firm has complete memory of all record-keeping processes, and can readily produce records for monitoring and inquiry. The organisational context of the data at the time the content is created, collected and archived can also be readily determined.
	Poor data governance	Greater effort to track data lineage and content types for reconstructing financial transaction history for searching, monitoring and discovery. Content blackouts leave gaps in data, creating search gaps for monitoring and discovery. Visibility of data for GDPR also affected.	Rich data governance	Data lineage, ownership, classification and inventory provide for easy access to content and the reconstruction of events. Monitoring is facilitated when searching for well-governed and classified data. If the firm is impacted by GDPR, data lineage and content distribution are easily determined.
MIFID2 requires content to be readily available for regulator or client inquiry. DR: 72(1) & 76(10)	Difficult search & discovery	Greater effort to collect relevant record for regulatory or client inquiry and monitoring. Mounting problems may lead to content blackout in inquiry.	Easy search & discovery	Search and discovery are easily facilitated with excellent institutional memory, data governance and collection best practices.
No MIFID2 requirement for operational efficiency.	High operational inefficiency	All the above result in spending more time and money to maintain record-keeping operations, for less than optimal results.	High operational efficiency	A surprising benefit – it takes a lot of work to achieve but is worth it in the long run. (As firms that have poured tens to hundreds of millions of dollars into litigation reserves would attest to.)

Information systems

EU firms are currently at different levels of readiness to handle the IT aspects of a strategic record-keeping programme. Some will have an existing content archiving system from which to work, and some may have nothing but backup systems in place. Content archiving with WORM type storage is fairly common in 2017, and there is a plethora of vendors with on-site, cloud and hybrid solutions to choose from.

Wherever a firm may be in terms of its IT readiness to obtain the real rewards of a strategic record-keeping programme, its management must work with its IT teams and vendors to come up with a means of managing the operations around its existing or future content archiving. Much of the workflow involved in the actual archiving process itself is what provides the benefits of a strategic record-keeping programme. As previously mentioned, archiving content in of itself is not proper record-keeping if the processes surrounding the archiving are not properly managed.

Finding the proper workflow system to manage archiving operations will be a more difficult challenge than finding a content archiving system. Content archiving vendors have by and large left the messy part of content archiving workflow management to the firms who purchase their solutions, and most companies have created a patchwork of home-made systems, third-party utilities and processes to manage workflow. With MIFID2, this ad-hoc system can spell trouble if it does not address the problems highlighted above.

Finding a readymade system for MIFID2 record-keeping operations can be possible if budgets allow for large-scale providers who can tailor their solutions to the size of companies. For all but the largest EU firms, this assistance may be more than they can afford. With the advent of FinTech this decade, awareness has grown around this gap in the content archiving market, and some vendors are beginning to customise their solutions around MIFID2.

Regardless of the workflow system that is used, it must at the very least not be based on spreadsheets and email for essential metadata. Otherwise institutional memory will suffer, given the well-documented faults of spreadsheets and email as substitutes for databases.

When looking for new workflow systems or adding systems to existing content archiving systems, management should ask the following key questions to ensure their systems can support the operational needs surrounding MIFID2 content archiving:

MIFID2 Requirement(s)	Questions for IT Systems/Solutions	Relevance to Strategic Record-Keeping
Requirement of management to have effective oversight and control over policies and the recording of telephone and electronic communications.	Can data governance and lineage information be applied to the content?	Application of organisational, system and technical metadata is important for searching, discovery, oversight, reporting, audit and monitoring.
	Does operations monitoring exist?	Content collection, processing, archiving and reconciliation processes must be monitored to ensure there are no content blackouts, or if they occur, that they are responded to immediately.
	What kind of reporting exists?	Robust reporting systems that are standardised will help IT operations and the firm's management ensure the record-keeping programme is running correctly across content collection, archiving and distribution processes. Associated retention periods of recorded content must be transparent. These are essential for the firm and for regulator inquiries.
When faced with the inability to record content, a workflow must be available to record the history of what happened.	Is there a workflow for day-to-day operations and exceptions?	System monitoring will generate alerts and exceptions. How can they be tracked and managed? A system must be in place to manage exceptions and the actions which were taken.
Requirement to keep track of users with self-owned and firm devices.	Can creators of content be tracked? (People and computers)	Identity management is a key component of metadata management, for the ease of searching across all content types for client or regulatory inquiries.
Periodic monitoring of records.	Which content monitoring and audit tools are available?	Ease of search and discovery will help compliance teams perform their monitoring function, and prove it by providing audit reports to regulators.
Requirement to store in a durable medium that prevents content alteration or deletion within the retention period.	How is content collected and stored in a durable medium that prevents content alteration? Can record retention be extended?	Archive processing and monitoring tools are essential for IT operations to ensure collected data is in fact being archived. Later, when records approach their retention limit, tools and reports are required to show which data is being deleted.
		Tools allowing for retention period extensions are vital. The audit of search, view and export events is important, in addition to the audit of attempted edit or delete events.

Conclusion

Whether creating a new record keeping programme from scratch or enhancing an existing one, by focusing on the strategic aspects as outlined in this focus paper, firms large and small will be rewarded with enhanced and operationally-efficient compliance with the record-keeping requirements of MIFID2 – with the added benefit of being well prepared for the client and regulatory crises that may come.

SIDEBOX: Much ado about nothing?

Is all this planning really necessary for MIFID2 record-keeping?

In the USA, where regulations surrounding the WORM archival of broker/dealer communications have existed since the 1990's, firms were still being fined as recently as December 2016 for the failure to keep proper records. In a press release by FINRA[1], the US financial industry regulator, 12 firms were fined $14.4 million for failure to keep records in WORM-based storage systems, thus impeding FINRA's ability to perform its investor protection functions.

While $14.4 million may not seem much for 12 firms, keep in mind the following:

• The firms are now required to become compliant with record-keeping regulations. It's not that they just pay the fine and carry on. This will cost time, labour and money to get right.

• They received negative press because of this press release.

• Loss of records can impact client litigation, often adversely for firms.

• With almost two decades worth of IT systems and processes available for proper record-keeping, these failures still occurred.

FINRA stated in their 2017 Exam and Regulatory Priorities Letter that a key focus of their 2017 audits will be compliance with USA record-keeping regulations.[2]

MIFID2's record-keeping requirements are part of its investor protection function, and regulators will most likely lean heavily on these requirements to ensure investor protection in the EU beginning 3 January 2018.

Failure to keep proper records is a serious matter.

[1] http://www.finra.org/newsroom/2016/finra-fines-12-firms-total-144-million-failing-protect-records-alteration
[2] http://www.finra.org/industry/2017-regulatory-and-examination-priorities-letter

Contacts PwC:

PwC
Birchstrasse 160
Postfach, 8050 Zürich

Günther Dobrauz
Partner
guenther.dobrauz@ch.pwc.com

Michael Taschner
Senior Manager
michael.taschner@ch.pwc.com

Philipp Rosenauer
Manager
philipp.rosenauer@ch.pwc.com

Orkan Sahin
Senior
orkan.sahin@ch.pwc.com

Contacts KSF Technologies:

KSF Technologies AG
Stampfenbachstrasse 48
8006 Zurich
Switzerland
Tel: +41 44 365 77 30
Fax: +41 44 365 77 07
info@ksftech.com

Michael Imfeld
Managing Partner, Business Development
michael.imfeld@ksftech.com

Allen Frasier
Director of Compliance
allen.frasier@ksftech.com