SOTERIA™
By Insightful Technology

WHITEPAPER

If the regulatory 'fire alarm' sounded, would your business be able to assemble all data in time, without getting proverbially burnt for late delivery, incomplete records, or through substantial outside resource spend?

Regulatory Compliance:

The 'Fire Alarm' Test for Financial Services

To certain businesses within the Financial Services Industry, MiFID II seemed to come and go a little like the 'Millennium Bug': a plentiful amount of fear and propaganda created around the legislation preceding 3rd January 2018, and yet with seemingly minimal-felt impact post-event, other than the nuisance of having to be seen to comply.

Indeed, a sector of the market, perhaps notably smaller organisations, still mistakenly consider compliance as merely a tick-box exercise, and MiFID II as open to interpretation, with phrases such as, "realistically this doesn't apply to us", or "we're a small/niche organisation so our regulated communications are limited", fairly commonplace.

Whether it is this rather naively-adopted outlook on MiFID II and regulatory compliance in general, or the opposite, where organisations understand the ramifications of the regulation and believe their "existing systems will suffice", perhaps the biggest aspect of compliance that remains under-evaluated within the business (the elephant in the room), is what would actually happen if the regulator came knocking. Could they adequately source, consolidate, refine and present the necessary associated communication and trade data around an activity, within the required timeframe, and in accordance with Article 76 of the legislation? Additionally, could they prove that the data has been captured and kept in a way that prevents deletion, and equally hasn't been tampered with?

Simply put, if the regulatory fire alarm sounded, would the business be able to assemble the necessary curated data to the regulator in time, without getting proverbially burnt for late delivery, incomplete records, or through substantial additional human resource spend?

The fundamental questions that regulated businesses are usually faced with at this point are:

- *Do you know where your data is stored?*
- *Do you know how to access it and also how long that process takes?*
- *Do you have the permission to access your data once you have located it, or do you know the relevant person who does?*
- *Do you have the ability or permission to collate the data and then refine it for relevance?*
- *Do you have the ability to recall all of the data, including metadata and both system- and data-audit trails for Evidential Weight and Duty of Care, to show that nothing has been tampered with or deleted, in a court of law?*
- *Do you have the ability to provide the regulator with secure access to your case, without having to physically download the data to an encrypted hard drive?*
- *If the answer is no to the above, do you know how long the downloading process will take? Do you need to send the data overseas and if so, how long will that take?*
- *Can you present your completed case within 72 hours of being requested to do so?*

enquiries@soteriasoftware.co.uk | www.soteriasoftware.co.uk | +44 (0) 207 283 2090

The first and perhaps biggest burden that most organisations realise once posed with these questions, is that they have often deployed multiple systems, in possibly multiple geographic locations, all with separate data silos for the various forms of human interaction they need to capture, be that for voice or electronic communication, or trade data.

Furthermore, a business may have acquired multiple other entities over time, all with different disparate solutions which have then been unsuccessfully cobbled together and therefore have exposed areas of weakness or "blind spots".

To compound the problem further, some of these disparate silos (which may historically be on-premise recorders and not agile cloud-based storage solutions), although compliantly storing the data, may do so in a "cold" fashion, meaning permission to access the records could take up to 7 days. This therefore makes it nigh on impossible to search, locate and retrieve the relevant information relating to a case in time, let alone make it accessible or presentable to a regulator.

Real-time capture and storage of business communications in the cloud, rather than overnight or 3-day batch filing, as well as the 'Normalisation' of this data — where common tagging of electronic objects is applied across disparate data systems, enabling the creation of a single global view of all media — are key drivers here, and facilitate the immediate searching across all content, attachments, and metadata, irrelevant of the data type or location, for further analysis.

If content is made fully searchable, surveillance tools that are preferably part of the same software solution and not additional middleware, can then not only historically filter through these datasets rapidly, but can also proactively monitor and alert upon new data that is created, as it is captured. Whether this is used to search for vocabulary or behaviour that is deemed suspicious or outside of healthy parameters, the workflow naturally establishes pre-emptive as well as post-event compliance measures.

While spoken interaction, be that through mobile, fixed line, trading turret or Skype for Business channels, is still considered a challenge for organisations to capture, let alone search for relevance, and while Artificial Intelligence tools such as Voice-to-Text transcription or translation are understood to be an ever-developing artform, it is possible with the right solution to not only real-time monitor captured voice data, but also proactively search and be alerted upon its content, with high accuracy weightings of between 85-95% now achievable.

However, for voice data to truly benefit the business and aid in the speed of trade reconstructions, as well as overall voice surveillance, the quality of the audio is fundamental in obtaining higher accuracy. Each line should therefore be captured as a separate stream in stereo rather than mono, with no compression or over talk, so that each person's communications can be analysed separately.

If this approach is invested in, the value of that solution and captured voice data then stretches far beyond the ability to instantly pinpoint relevant key phrases in lengthy calls, which has historically been the arduous task undertaken by physical manpower, and which has never prevented the likelihood of human error, or the impossibility of being able to monitor all people on all calls, all day long.

Real actionable value of transcribed voice data can be seen in workflows such as the proactive population of text into CRM systems or deal tickets, which saves time, energy and resource. Additionally, translation tools can facilitate the understanding of a conversation when reviewed, should the call not have been spoken in the analyst's native language.

It is appropriate to mention here that while this level of content discovery may not be achievable on archived voice recordings, it is still possible with the use of normalisation to search the content or attachments of other electronic archived data, to then enable the inclusion of these files within global search results. Equally, the quality of the audio would only limit the screening of the audio recording's content; it would not prevent the object being found in an initial search using metadata such as the timestamp, or identifiers such as the phone number.

In creating a scenario where businesses can real-time analyse communication data of all types against simultaneously searched trades or other logged activity, it provides the true enabler for transforming previously reactive approaches to compliance, in to truly proactive ones, and it is also what has empowered the growth of First Line of Defence departments, especially within the tier 1 banks, to combat the personal liability and accountability of non-compliance that is now enforced through the Senior Management and Certification Regime.

Additionally, with the correct solution in place, not only can the real-time capture, search and analysis of data be ensured, but also the simultaneous creation of 3rd party verified audit logs for both the system and all data objects, technically known as 'Non-Repudiation'.

It is this supporting information that provides the business with the assurance each record is complete and tamper-proof, and that any interaction with an object, or any keystroke within the system, is logged, should there be a need to show Evidential Weight and Duty of Care in a court of law.

The final challenge in responding to any regulatory request is making the case (that has taken long enough to compile), immediately available to the regulator. Historically, this has often involved lengthy processes of downloading vast amounts of data, from potentially multiple geographic locations, onto encrypted hard drives, which are then delivered to the regulator, in some scenarios being flown overseas. While this may have been the only option in the era of the Millennium Bug, recent advances in technology and cloud architecture now make it feasible to create securely containerised case files within the implemented system, where remote time-lapsed logins can be arranged for the regulator, so that no data has to leave jurisdiction and it can be reviewed instantly where it has been stored.

While a daunting prospect at first, addressing the need for robust compliance solutions and processes to proactively respond to regulatory requests is in fact a hidden opportunity for financial organisations. Not only does it encourage the review of outdated architecture, it also empowers the very achievable business transformations that new and agile cloud- based SaaS solutions can provide. In many cases, it enables the reduction of multiple physical on-premise solutions and middleware, which in turn positively impacts total cost of ownership, as well as creating faster and more actionable intelligence and efficiency practices that are now invaluable in the modern business place.

enquiries@soteriasoftware.co.uk | www.soteriasoftware.co.uk | +44 (0) 207 283 2090

In recent conversations with new market entrants, so called "Challenger Digital Banks", they have highlighted their competitive edge as a result of building compliant cloud-based architectures from 'greenfield', therefore operating without the burden of multiple data silos or legacy systems. With this in mind, surely the decision for already established banks to harness the same power of a cloud-based compliant SaaS platform, and ensure their business longevity and competitivity, would be a no brainer?

Just remember:

While technology is the enabler, as long as there is human involvement in business activity, no software or hardware can account for someone's sense of morality, and therefore any technology is only as good as the operational policies and mandates that support it.

About Insightful Technology

Through our SaaS platform Soteria™, we provide financial organisations around the world with the ability to compliantly capture, analyse, store and surveil business communications and market data in real-time, regardless of the source, and in a single, global and hierarchical view.

Our Artificial Intelligence, Business Intelligence, and End-to-End Workflow capabilities include Proactive Monitoring and Alerting, Analytics and Reporting, the functionality to immediately create Trade Reconstructions with containerised Regulator Login Access, and also the ability to pre-populate 3rd party solutions such as CRM systems or Best Execution Templates, with accurate Voice-to-Text transcriptions, translations and notes. Using Soteria™, we not only drive compliance, surveillance and risk mitigation on a global scale but also business efficiency.

Our mobile voice recording technology which underpins 'Truphone Mobile Recording' is currently used by 10 of the top 12 tier 1 global banks, and we also have over 180 other financial organisations, including buy- and sell- side firms, using Soteria™ throughout their front, middle and back office departments. Soteria™ can also be implemented by other regulated industries, including government agencies, legal institutions and pharmaceutical companies.

enquiries@soteriasoftware.co.uk | www.soteriasoftware.co.uk | +44 (0) 207 283 2090