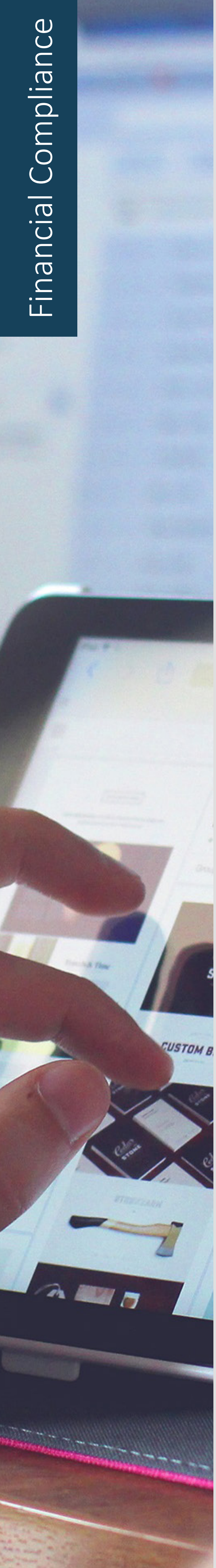
Financial Compliance

Is your financial services company struggling to keep up with a deluge of compliancy regulations? Looking for solutions that are familiar, yet capable of addressing your needs? Look no further.

Crow Canyon Software



the financial acronym jungle

The financial industry may have recently attained the unique status of being subject to more regulatory and compliance regulations than any other business sector in the U.S. The list of governmental agencies and legislations associated with oversight of the American finance sector reads like an alphabet soup: SEC, FDIC, CFPB, OTS, OCC, NCUA, FINRA, UDAAP, CCAR, PATRIOT ACT, and SOX. Depending on the nature of the business, companies are typically subject to multiple compliance regulations from a variety of different public entities... and we haven't even mentioned compliance with private sector accreditation entities (there are currently over 160 finance-related accreditations available). CAMLS, CAA, CBEC, AEP, AWMA, and so on... the acronyms are almost neverending.

compliance: a serious business

Doing business in the financial sector is not for the faint of heart. Nowadays, navigating the ups & downs of security valuations has taken a backseat to fulfilling the multitude of requirements needed to maintain a state of regulatory compliance. The job title of Compliance Officer, almost unheard-of 20 years ago, is now the "Hottest Job in America" according to the Wall Street Journal.

Quite simply, the risk of running afoul of financial legislation now vastly outweighs the cost of hiring teams of compliance specialists headed by a CCO (Chief Compliance Officer). The high fines coupled with the real risk of incarceration are more than enough to cripple not only individual investment advisers, but entire financial brokerages.

Against this backdrop comes the sober reality, at the operational level, of how to attain and maintain full compliance with a plethora of governmental regulations. Gone are the days of paper forms and file folders; we are now entrenched in the digital age and, with it, comes digital solutions.

breaking down "compliance"

At its core, tackling the challenges of compliance comes down to effectively managing the flow of information. After all, the whole concept of compliance essentially boils down to a simple formula:

```
compliance = right action + data curation + effective communication
```

By "right action," we simply mean doing business within a legal framework (i.e., not breaking the law). This can be facilitated by employee education and pro-active initiatives designed to keep teams aware of current legislation. Regulatory standards can change overnight, so it is critical for businesses to approach compliance from a holistic perspective by ensuring the entire organization understands the need for compliant behavior and how to align their actions accordingly.

"Data curation" is the storage of critical data for a (typically) mandated time period. The need for data curation stems from the primary weapon in every regulator's arsenal: the audit. Audits often occur without warning and are designed to ensure that companies are doing business within a regulatory framework. This means that sensitive business data, such as financial transactions, customer records, conversations, money transfers, banking details, and contracts all need to be meticulously saved, secured, and maintained... preferably in a centralized and accessible location. A breach of any one of the above could trigger penalties or more serious repercussions.

The final ingredient, “effective communication,” is a fairly wide umbrella that includes both internal and external communication. Communication is best facilitated by a centralized platform, powered by familiar tools, that is capable of saving all content (e.g., e-mails, conversations, etc.). For example, an Office 365 environment would enable employees to e-mail using Outlook, save files to OneDrive, collaborate using SharePoint, and support platform-wide searching whether on or off premises. In the above example, admins could use the Office 365 Compliance Center to configure the lifespan of content (i.e., auto-deletions) and which users should be granted access rights.

In terms of compliance, all communications (whether internal or external) will be subject to viewing by regulatory authorities in order to prove and/or resolve compliance issues. Given this, accurate data curation and effective communication are critical to proving that employee actions do not violate the law.

strategy: let technology do the heavy lifting

In today’s litigious and highly-regulated business environment, the days of file folders and paper pushing are relics of the past. The concept of personal privacy has given way to a need for security and regulation. The financial world now bears no resemblance to its predecessors from years past when deals were jotted down in notebooks and tossed aside when the tax man knocked on the door. Today’s world is a digital one, where content is stored on cloud-based servers and security is represented by passwords instead of skeleton keys. The financial world has rapidly scaled upwards and manual solutions are simply no longer feasible. Technology has taken over — there is no choice other than to embrace it.

In the world of financial compliance, there are two areas where technology can be leveraged to more efficiently achieve regulatory compliance:

Financial Data Management

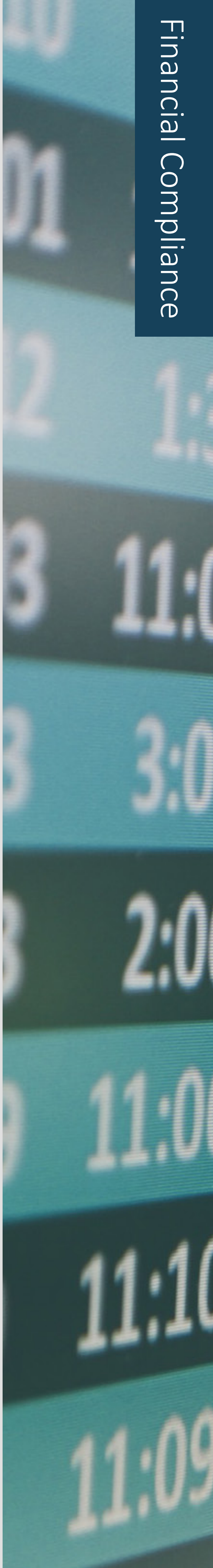
Simply put, this is the process of ensuring that sensitive content remains secure. This is facilitated by using software that can automatically recognize sensitive data across the enterprise, securely save that content in an accessible location, and support Data Loss Prevention (DLP) policies to ensure that sensitive content is not leaked outside of the corporate network.

Document and License Management

Financial documents are not static “sign-and-forget” pieces of paper — they are organic documents that possess their own unique lifecycle. Whether it’s a contract, investor profile, or a promissory note, documents undergo changes during their term. Document Management uses software to facilitate the management of this lifecycle while promoting communications across all levels of the enterprise.

Not maintaining licensures could be grounds for legal action at both the brokerage and broker levels. A software platform should enable organizations to easily manage & centralize the licensing process in order to remain compliant with licensing regulations.

In the sections below we will explore these topics in more detail and discuss some specific technology-based solutions.



financial data management

Regulatory agencies expect that your company will save & maintain internal and external financial data for a specified period of time. This data should be highly secure, yet accessible to employees with the proper permissions. Accidentally losing sensitive information or inadvertently sharing it with unauthorized users is a quick way to lose your license while invoking the wrath of compliance audit teams. Effectively managing financial data requires a 3-pronged approach:

- Automatically recognize sensitive data;
- Securely save all data;
- Prevent the loss of sensitive data.

Your software platform of choice should be capable of automating laborious tasks as much as possible, particularly for large-scale enterprises. Microsoft Office 365 and SharePoint are platforms that have stood the test of time and are capable of addressing many of the data management challenges inherent in maintaining financial compliance... including automated data recognition.

SharePoint 2016 has a new feature called Sensitive Information Types, which is used to help users automatically identify sensitive content that is saved across their enterprise, such as OneDrive (cloud-based storage), Outlook (e-mails), Lync (conversations), and so on. Sensitive Information Types are defined by patterns identified by regular expressions (or a function) and are available for use in Data Loss Prevention policies (more on that below). For example, you can configure a policy that automatically searches for social security numbers, credit card numbers, and bank account numbers. Proximity logic and corroborative evidence is used to ascertain the validity of the sensitive data, which can then be securely saved.

Speaking of saving, Microsoft Office 365 includes OneDrive — a cloud storage solution that is highly accessible, configurable, and integrated with other business applications (e.g., Excel, Word, PowerPoint, etc.). OneDrive negates the need to physically carry storage devices; being cloud-based means that your company's sensitive financial data, such as a broker's transaction records, are automatically saved and can be accessed via a Web browser from any device.

Now that you've identified your company's sensitive data and have securely saved it, the challenge becomes, "How to keep that information secure?" This is made possible via the creation & implementation of Data Loss Prevention (DLP) policies. This security methodology is designed to ensure that your employees do not (accidentally or intentionally) send sensitive data to people outside of your corporate network. Microsoft has embraced DLP with a rollout of functionality to OneDrive, Outlook, SharePoint, and traditional Office 365 business productivity apps. The core concept here is that data should be protected no matter where it resides, whether it's in an e-mail being typed or in a PowerPoint document. Essentially, administrators use the Office 365 Compliance Center to create DLP policies, which are then broadly enforced across all user end-points, such as SharePoint or within Word and Excel.

The enforcement of DLP policies takes place in real-time, so there will be no opportunity for critical user mistakes to be made. For example, if a user enters questionable information in an e-mail (e.g., telling a colleague the banking logon details for an outgoing investment), a notification will appear in real-time informing them of the issue. The user can then change the data or, if they have sufficient permissions, can even modify the DLP policy on-the-spot.

document and license management

The length of time spent handling sensitive financial data is a bit of a balancing act: If documents are retained for too long, then they may pose an unnecessary legal risk. If they are modified or deleted too soon, then legal actions may also be taken. Document life management is a tricky business but, fortunately, is supported by the Office 365 Compliance Center. This feature enables users to specifically state exactly when, and under what circumstances, documents should be deleted from the system.

Office 365-supported document management enables admins to create highly flexible deletion rules, such as:

- Specify a time period until deletion;
- When to calculate the deletion date (i.e., from date of creation or the date of last modification);
- Delete the document permanently or move it to the Recycle Bin.

Policies can even include multiple deletion rules and SharePoint site owners will be able to select the rule that is the most relevant for their site.

In addition to addressing the end-of-life terms for documents, it is critical to examine the actual lifecycle of financial documents. Most documents are non-static — their validity is often tied to real-world actions, from agent performance bonuses to automatic put & sell option assignments. In these instances, implementing a SharePoint-compatible Help Desk solution would enable your organization to keep track of organic documents, license renewals, and even automate the document creation process (e.g., contracts).

Some key features that a SharePoint-enabled Help Desk system can offer include:

- Create a knowledgebase repository for all templated documents, contracts, notes, etc.;
- Build user-friendly customizable forms to create templates for fast contract creation;
- Take control of document milestones with comprehensive trigger-based notifications & alerts with intelligent e-mail routing;
- Integrate Outlook so that inter-party e-mail communications instantly become tickets that can be routed, tracked, and memorialized for future review and auditing;
- Configure the document approval process using user role-based communications — ensure that sensitive messages about document details (e.g., contracts, financial statements) go to the right recipients;
- For large organizations with a high-volume of agreements, contracts, and quarterly statements: Measure, track, and analyze the entire document lifecycle management process. View reports on users, time spent during a document's lifecycle, and pin-point areas that require further refinement;
- For 3rd party service agreements, create surveys to gain an understanding of the document management experience from the viewpoint of your partners.

Crow Canyon Software

Crow Canyon Systems

W: www.CrowCanyon.com
E: sales@crowcanyon.com
T: 1-888-706-0070