STAR COMPLIANCE

THE COMPLIANCE OFFICER'S ULTIMATE COMPLIANCE GUIDE

How To Build A Compliance Program That Will Keep You Up To Date, Up To Speed, And In The Know

Conflicts of interest and market abuse in enterprise financial firms can come in all shapes and sizes. Top of mind for most compliance officers is likely personal trading, also known as personal account dealing, and insider trading. But conflicts of interest and market abuse can also manifest themselves in activities such as private investments, gifts and entertainment, outside business activities, and political donations.

Big Data, algorithm-driven automation, and global firm operations have made the job of the compliance officer very different from what it was not that long ago. The job is now a constantly evolving one. And while professionals in any field are responsible for staying on top of changes in best practices, processes, and procedures, compliance officers of today in particular have their work cut out for them.

They still need to be investigators in the traditional sense, of course. But as compliance platforms become increasingly ubiquitous and increasingly capable, compliance officers need to become increasingly tech savvy. This is a trend that's unlikely to change. As such, the modern compliance officer needs all the help she can get. With that in mind, we offer this compliance officer's ultimate guide for building a compliance program that keeps you up to date, up to speed, and in the know on every topic of concern for your enterprise financial firm.

> "Culture can nudge you to do the right thing or the wrong thing. But culture is always moving, and pressure can create cultural drift. Compliance officers are in the drift prevention business at their firms."
>
> **Dr. Robert Hurley, Professor of Executive Education at Columbia University and President of Hurley Associates**

CHANGES IN REGULATION

But before delving into changes to the job as relate to changes in technology, it's worth touching on changes to the job as relate to changes in regulation—in the UK, the US, and globally. The past two decades have seen an increase in both the amount of new regulation and the degree to which existing regulation is enforced. New regulation includes:

- Europe's General Data Protection Rule, or **GDPR** went into effect on May 25 2018. The GDPR utterly inverts the relationship between data processors and data subjects for any company that does business in the EU. The data rights of the data subject now take complete precedence.

- Europe's Markets in Financial Instruments Directive, or **MiFID 2** went into effect on January 2 of 2018. MiFID 2 is a quantum leap in terms of regulatory reach beyond its predecessor, MiFID 1, and will affect nearly every aspect of trading in the EU.

- France's **Sapin 2** took effect on June 1 2017. It's the country's second legislative attempt to take on corruption, increase transparency, modernize the economy and—in the words of the government—bring France in line with the "highest international standards" in these areas.

- South Africa's Financial Sector Regulation Act, or **FSRA**, went into effect in spring of 2018. Among other things, the FSRA introduced the globally trending **Twin Peaks** financial regulation model to the continent's economic powerhouse—a total revamping of the previous regime.

- The **California Consumer Privacy Act** went into effect on January 1 2020, but the state wont start enforcing the law until July 1 2020. The Golden State's answer to the GDPR and Big Tech data-privacy scandals, it also upends the relationship between data subject and data processor, and could be a model for future federal regulation.

- New York State's **23 NYCRR §500** went into effect March 1, 2017, but has been in the works since the Target and Home Depot data breaches of 2014. It's meant to "*promote the protection of customer information as well as the information technology systems of regulated entities.*"

There's more, of course, but those are the big six. For now. In 2016, 52,506 international regulatory changes and announcements were released. Since 2008, banks have paid over $204 billion in compliance related fines and infractions. In 2016 alone, $42 billion in fees were collected. In terms of regulation generation, the global financial crisis is the gift that keeps on giving. Expect data privacy to be another global regulation generator.

CHANGES IN TECHNOLOGY

As touched on already, compliance platforms becoming increasingly ubiquitous and increasingly capable means compliance officers need to become increasingly tech savvy. And yes, keeping up with these changes in the tech is something that needs to be attended to from a professional development standpoint. But while stepping into this can seem daunting, there's plenty of upside for the enterprise financial firm compliance officer.

This regulation coming fast and furious from all corners of the globe is something that needs to be kept up with. And in *this* daunting task, compliance officers will find that the increasing capability and sophistication of modern compliance technology will make all the difference. Automation means freedom from the day-to-day portions of the job that previously had to be accomplished manually.

Pre-clearing trade requests. Hounding errant employees to complete their certs. Maintaining insider lists on spreadsheets. Freeing up compliance officers from tasks like these allows them to focus on the bigger picture portions of their jobs. But before we dig into the details of what to look for in a compliance platform, it's worth spending some time exploring the best methods for getting buy-in on the idea.

> "Compliance officers will need to become more like technology officers, while technology officers will need to become more like compliance officers. But we're ultimately still investigators."
>
> **STAR Platform User and CCO of Asset Manager with $310B in AUM**

RETURN ON INVESTMENT

So *you're* convinced of the need for greater automation and increased sophistication in your compliance platform, but now you have to convince the person or persons who have sign-off authority. Companies typically judge a cost with *return on investment*, or ROI. The idea is to get to a clear-cut number that will quickly tell upper management whether or not something is worth spending money on.

The problem with compliance efforts is, it's much harder to get to a clear-cut number. Like the cop on the beat, a compliance officer's alertness, experience, and mere presence on the job may stop potential problems before they ever completely manifest. So how do you insert something that didn't happen into an ROI equation? For starters, there are some clear costs and benefits you can assign to a compliance program. Compliance team salaries and investments in vendor services and technology come to mind. Increased earnings from a compliance program that gives your firm the confidence to do business in a high-risk market is another. These kinds of costs and benefits are ripe to be inserted into an equation.

A qualitative cost could be the cost savings associated with not paying fines, or employees not facing criminal charges. Company reputation, individual professional reputation, and brand value could be considered qualitative returns of a robust compliance program. But how do you convert these soft considerations into hard numbers? The answer is, companies regularly assign hard values to soft costs and benefits. Intellectual property is highly valued and regularly factored into overall company worth. A compliance program needs to be thought of similarly, and the case can be made. The trick is making the case to the right people and letting *them* come up with the numbers.

Find those in upper management who already understand the value of compliance, who don't need to be convinced of its intrinsic worth or the returns the best people and best software can generate. Company leaders should be very attuned to the value of the company brand, the company's reputation, and their own personal reputations. Ask them to quantify what these tangible-intangibles mean. They should mean a lot. A company that's not operating with integrity might not be operating for very long, period. A company that's operating more ethically might also be recognized as such in the marketplace. It's not unreasonable to think this could be a differentiator, and therefore drive earnings and growth.

And for companies that operate globally, a well-staffed and fully automated compliance program will also help drive earnings and growth. We already mentioned the benefit of having the confidence to enter high-risk markets. But operating in markets with even the lowest levels of corruption still mean volumes of regulation to be applied to your firm's compliance program. Compliance is a lot like insurance. That is, people spending money to protect against things that may never happen.

COMPLIANCE PLATFORM MUST HAVES

Now to what you should be looking for in automated compliance software. It's common to associate conflicts of interest more with internal, firm concerns than with external, market and regulatory concerns. Conflict of interest concerns are often listed as personal trading, rogue trading, outside business activities, outside investments, gift and entertainment spending, and donating to political campaigns. Market abuse is often singularly thought of as insider trading. But these two areas of concern to compliance officers have significant overlap in how they're best dealt with from a tech perspective.

PRE-CLEARANCE

At the most practical level, compliance means participation—in the tech, processes, and best practices the firm has decided holistically get the job done. And willingness to participate means understanding that adhering to the company code of ethics and any applicable regulations is fundamental to the continued safe and profitable operation of the firm and the continued safe and profitable operation of the employee. In other words, compliance officers have to rely a great deal on voluntary disclosures.

Which brings us to pre-clearance: the compliance officer's best friend. It's the starting point for early detection of many conflict of interest and market abuse issues. Get employees in the habit of pre-clearing critical activities and you're halfway there in terms of compliance. Pre-clearance, of course, means employees need to *pre-clear* certain activities before proceeding. This can apply to trades, gifts and entertainment, outside investments, outside business activities, and political donations.

Employees pre-clear by logging into an automated compliance platform, filling out a pre-clearance request form, and awaiting an automated approval or denial decision. The platform can make this kind of decision safely because the firm code of conduct was programmed into the system's *rules engine* from the start. The software assesses the employee requests against your rules and gives permission or refusal to make the requested trade.

In cases where rapid approval or denial isn't possible, the system will escalate the request to a multi-level review process. And any compliance platform should be web-based, so employees can use it from anywhere. This will increase employee participation. Remember, compliance may be your first job, and that of your fellow team members, but it's no one else's. Do whatever you can to make things easy.

Reconciliation also goes hand-in-hand with pre-clearance, and keeping track of this employee trading data is more efficient with broker-feed reconciliation. A good compliance vendor will establish as many broker feeds as possible, and offer them as part of the platform subscription. These feeds allow employee-provided data to be reconciled against broker data, enabling all records to be updated and anything out of the norm to be detected. And, of course, this kind of system entirely negates the need for paper statements to be manually checked.

> For our top-level executives, if certs need to be completed and important deadlines are looming, we make a friendly but firm phone call or even pop into the office.
>
> **STAR Platform User and Enterprise Financial Firm Compliance Officer**

CERTIFICATIONS AND ATTESTATIONS

Certifications and attestations are more than just *pro forma* exercises your employees trudge through to tick off required regulatory boxes; they're your enterprise financial firm's proof of regulatory rigor—providing an extra measure of certainty your business is doing everything in its power to detect and prevent conflicts of interest and market abuse.

By submitting attestations, employees confirm that all recorded information, business activities, and transactions are accurate and comprehensive. At intervals you determine, a well-built compliance platform can collate all data on each employee into an attestation or certificate for them to check and approve. All approved certificates should be able to be stored by the compliance platform for future reference, to be viewed or downloaded by your team whenever necessary.

Good software can also push information out to employees. This could include the latest firm policies, or breaking changes in regulation—anything you feel, in the end, might buttress your case to industry watchdogs that you're doing everything you can to ensure regulatory compliance. Back to the idea of participation, getting employees to complete their certs is another eternal challenge of the compliance officer. Here are a few possible solutions and notions to keep in mind:

- Vary The Medium—There's more to messaging than email. Use your compliance software's dashboards. Use the company's internal television system. Make personal phone calls.
- Escalation—At what point do you copy managers? At what point do you suspend a dawdler's ability to execute trades?
- Good Software—Compliance software can make or break this follow-up phase of the certs process. Can you set automated reminders? Can you set automated escalation points?
- Fun And Games—Make it a competition. Consider doing a department-by-department completion scorecard. Offer a prize to the winning team.
- Think Outside The Box—One enterprise financial firm was known to use its disaster recovery phone service, part of its business continuity plan, to robo-call procrastinators.

On the subject of thinking outside the box, one compliance officer speaking at a StarCompliance user conference offered this unique strategy for luring his younger charges into engaging with their compliance duties. "Memes have worked well for Millennials. For the young, the tech savvy. Building critical messaging into GIFs, and maybe getting a laugh along with it. Whatever it takes, right?" Another offered this: "I've gotten on the phone with spouses who don't understand why they should be subject to trading restrictions when it's not their company."

For more actionable advice on improving your certifications process, download our FREE checklist: **Optimizing Your Certifications Process.**

INTEGRATED SURVEILLANCE

A good investigator will never stay locked away in her silo. She'll want to consider and integrate as many sources as possible into an investigation. A good compliance platform operates similarly. The right software will collect data from existing systems across your firm, like HR and order-management systems, and even historical trading records—all to be automatically cross-referenced when any pre-clearance request is made.

This data integration means not just more accurate decisions when it comes to approving or denying trade requests, but also giving your compliance team the best shot at identifying the firm's highest risk actions and individuals. It means an even better chance of picking up on anomalies or other unusual patterns of behavior that may raise eyebrows and warrant further investigation. Some compliance platforms can also be configured to draw data from internal and external sources, like news feeds. Cross-referenced with pertinent internal data, this puts even more investigative power into your hands.

REPORTING

Whether they're helping you get a handle on the goings-on in your corner of the company, or keeping the c-suite similarly informed, reports keep management at every level in the know. A good platform doesn't just put the raw data you need within easy reach, it gives you the kind of sorted and sifted data that provides a 360-degree view of employee behavior and activity. It should also allow you to easily search for specific data in any field and export information for further analysis.

Sophisticated visualizations, graphs, and charts should be a given for any modern compliance platform, making the volumes of data you have to deal with easy to interpret and easy to compare. The ability to generate comprehensive, meaningful, easily accessible reports should also be a given, with the capacity to distribute these reports automatically and at customizable intervals to whomever needs to see them. Reports that can be displayed in-app, saved for later use, or exported to Excel spreadsheets should also be no great feat for any piece of modern compliance software.

CASE MANAGEMENT

Of course, once your integrated compliance platform vigilantly puts you on the trail of an individual or group of individuals that warrant further investigation, the platform should then be able to manage the case all the way through to resolution. The right system will enable you to collate data and evidence in a single place, add annotations, and assign cases to relevant team members for immediate resolution or further investigation.

Case cycles should be able to be recorded on the compliance platform for audit purposes, with management reports available to help identify trends and support continuous improvement.

INSIDER LIST MANAGEMENT

Any company that trades on the stock exchange is required to keep a list of anyone who has inside information at any time, including contact details. It's your job as compliance officer to keep this list up to date and to inform employees when they've been placed on it. For large companies with hundreds of employees working on multiple projects, this can be a big administrative task.

Look for a compliance platform that offers an insider-list management product: a sophisticated tool that manages the recording of all employees involved in any project, including when they come onto the project, what information they're privy to, and when they leave. It should also handle all communications with the employees concerned. A tool like this means if regulators ever request information about any potential insider trades, you have all the detail they need at your fingertips. And it's yet another way for you to keep information tidily corralled.

COMPLIANCE PLATFORM SHOULD HAVES

Here are three available services that can make the job of the compliance officer much easier. Look for these offerings as you vet vendors. Good ones will include them at least as add-on items.

1 Global News Data

When trying to connect the dots surrounding suspected insider or rogue trading activities, too much information is never enough, so long as it's presented in an organized and relevant manner. Current affairs info and news can be crucial to connecting these dots. Look for news feeds that cull information from diverse, respected sources, like established publishing houses and even social media voices.

By passing news stories through filtering and indexing systems, items that are most relevant to you can be highlighted and prioritized. A system should cross reference these news events with your employee trading data, looking for any unusual trades made prior to significant market events which could have been based on inside information. This will give you the full market context for every trade.

2 Global Financial Data

It goes without saying how important this kind of information is when it comes to trying to solve a puzzle. A provider of global financial markets data and analytics can give you access to time-sensitive pricing, evaluation, and reference data for millions of securities traded around the world, including equities, UITs, mutual funds, debt instruments, as well as hard-to-value assets, like wine and art.

3 Beneficiary Management

This capability lets you manage lists of individuals or political entities benefiting from political donations made by your employees. This gives you a more complete picture, as you're able to see both sides of donations activity. A contribution data service is a third-party feed that supplements your own political donations data, making you even more sure your firm's donation limits aren't exceeded.

For the A-Z on choosing the right compliance platform, download our FREE checklist: **Buying The Right Compliance Platform.**

> I differentiate between negligent insider trading and malicious insider trading. I don't advise people to be suspicious all the time, but in the financial sector being alert and skeptical are useful traits.
>
> **Dr. Alexander Stein, Founder and Managing Principal at Dolus Advisors**

THE DATA SECURITY DIFFERENTIATOR

Data is practically a new currency. And like any currency, at some point someone will try to steal it. In 2017, 179 million records were exposed—the result of 1,579 reported data breaches. In 2015, the financial services industry alone lost $28 billion to data theft. A compliance vendor's approach to data security can teach you a lot about the company as whole. It's a differentiator for the age of Big Data.

Look for a vendor that takes physical security seriously. This means locating the data center in an unmarked structure. Fencing, guards, and biometric checks. False entrances and vehicle blockades. Locked server cages and cabinets. Climate control and fire-suppression systems. Look for a vendor that replaces its servers on a regular basis, because old equipment is more likely to fail than new equipment. Look for a vendor that uses trusted technologies, backed by support and maintenance agreements.

Look for Tier-3 network topology. Tier-3 means redundancy. Components that can be replaced without interrupting operations. 99.98% data-center availability. Look for *failovers*, so if a firewall has a failure another kicks in. Look for a *hypervisor*, which lets a single server host multiple virtual servers and shift workload if a physical server dies. And don't forget about certifications. ISO 27001 is the industry gold standard for managing sensitive company information and ensuring it remains secure. ISO 22031 goes a step further: addressing business continuity and certifying a company has plans in place for disruptive incidents.

For technical controls look for *defense-in-depth*, which means data defenses working at multiple levels in the network. It means layers and levels and the firewalls in between them. Look for anti-virus and anti-malware software. Security information and event management systems. Patch management solutions. DDoS protection. A vendor should also perform vulnerability tests on its own systems.

Look for single sign-on and roles-based access control. Look for granular user-permissions and encryption of data in-transit and at rest. Ask about visibility walls. Determine if the software development life cycle includes static-application security testing, static-code analysis, and developer secure-code training. Data privacy is more and more seen as an integral part of data security. As such, a vendor that takes data security seriously is a company that can be taken seriously at every level.

For the full list of what to look for in a compliance vendor's approach to data security, download our FREE e-book: **Data Security: What To Look For When Vetting A Compliance Vendor.**

SWITCHING PLATFORMS STRESS FREE

When it comes to switching from an existing compliance platform vendor to a new one, two overriding concerns are *migration* and *integration*. *Migration* means bringing over all existing data to the new platform and hoping everything comes over intact. *Integration* means making clean and seamless connections from the new platform to all other existing company data systems, like CRM and HR systems, firm-trading and open-order systems, expense systems, and broker feeds.

Another stressor can simply be embarking on what seems like a herculean task. "New clients usually have several concerns," says StarCompliance Associate Director of Professional Services Kelsey Amar. "The years of transactions they're desperate not to lose. Then ensuring that the hard-won broker feeds are brought over properly. But also getting all the requirements straight for the building and testing of the new platform." All of which makes it as important to find a vendor that possesses mastery of the transition process as it is finding a vendor that makes a great product.

Following is an example of what a well-managed migration and integrations process should look like. Every vendor will operate a little differently, but there's an industry standard thoroughness and logic to any well-executed installation.

1. After a product demo, discussion of a general direction, and an agreement to move forward, there's a kickoff meeting. A timeline is provided which tells the client everything needed to begin the build process.
2. The vendor schedules a *deep-dive*, where a small team of implementation experts goes onsite with the client for further, in-depth information gathering.
3. The vendor prepares a document based on everything that's been gathered and discussed to this point, so there's no uncertainty regarding what client and vendor have so far seen and agreed upon.
4. The client is then sent another document to further flesh out requirements. This will translate the client's specified rules, processes, and code of conduct into what will ultimately be their new compliance platform. Every aspect of the coming build is mapped.
5. The client signs off and the vendor begins the build.
6. When the initial build is finished, the vendor thoroughly tests everything internally.
7. The vendor provides the client a testing site. This site exists completely in a test environment. Nothing is live. The client is still using its legacy system at this point.
8. Vendor and client meet again to develop a testing plan. Together they develop scenarios both sides feel will realistically simulate what the client will face when the platform is live.
9. There is a user-acceptance phase. Again, this takes place purely in the testing environment. This is where any needed corrections are made and the new platform is fine tuned.
10. Finally, the production environment is prepared. When both vendor and client feel at ease with where the new compliance platform is, it goes live.

There's a point in any software build process when the implementation team has to bow out. They've done their job, built a good product, and it's time to hand the client over to support. There's no getting around this, but it can make new clients nervous. Look for a vendor that gets this part of the process.

Again, Star's Kelsey Amar: **"Eventually we have to cut the cord, but we try to be as gentle as possible. We have a client meeting and do a two-week soft transition. Support is slowly looped in. By the end, clients know they're in good hands. Star takes pride in ensuring the migration process goes smoothly. My department, Professional Services, is entirely dedicated to managing the transition: start to finish."**

> Sometimes people think they're above it all. At a certain point, I may get their supervisors involved. But I always try and be consultative first, and save a more restrictive approach for use as a last resort.

STAR Platform User and Enterprise Financial Firm Compliance Officer

ADOPTION AND ROLLOUT

So now you have the new platform. It's up and running as advertised, but you have to get people using it. Unfortunately, when it comes to learning something new for a job, resistance is natural, particularly if it's something not directly related to the work a person gets paid for. This is the case with compliance software. But a company that's made the considerable investment in compliance software will expect their employees to use it. And it will likely fall to you, the compliance officer, to make sure that happens.

Good software is, naturally, at the heart of it all. Spend the money to get software that's user friendly and intuitive. The only thing worse than having to do work you don't want to do in a new app is doing work you don't want to do in a new app that's hard to get around in. Keep training targeted and short. Use real-life scenarios, thus making it as relatable as possible. And rather than holding large group sessions, train in small groups with employees who will be using the same features.

Now comes buy-in. Start small. Get hardcore buy-in first. Getting "points on the board" quickly will build momentum. Consider rolling out the new compliance platform in stages, building support group by group. The first stage of deployment could be to a small group of known early adopters, or those struggling most with the old system. And if any app-champions evolve out of this process, use them as platform ambassadors and informal "go-to" experts for other employees as the rollout continues.

The most important kind of buy-in might be leadership buy-in. Don't assume that because compliance got the sign-off on new software leadership is 100% behind it, or even has a firm grasp on why it was purchased. As such, you may need to press your case for platform adoption in both directions of the company hierarchy. Consider having your c-suite attend general training and learn the new software shoulder to shoulder along with everyone else. What better way to demonstrate leadership buy-in?

Get help from marketing, as well. Marketing is all about getting the word out. Building excitement around the launch of a new product. Marketing can help you get buy-in for your new compliance platform at every level of the organization. Consider making a promotional video. Flyers on bulletin boards are tried but true. Make the most of your in-house television system. Marketing will come up with the proper strategies, tactics, and materials if given the opportunity to do so.

Finally, think of training and rollout as ongoing. Many professions operate like this. Once licensed, pilots are always licensed, but need to fly a certain amount of hours to stay "current." Project Management Professionals have to complete a certain amount of regular study to keep their certificates valid. If you can't be quite so formal with your firm's compliance training, try to return to it on a quarterly or yearly basis. This will help keep learning manageable for those whose primary job isn't compliance.

Looking for more ways to ensure compliance software adoption? Download our FREE checklist: **New Compliance Software: 5 Ways To Help Ensure Complete Adoption.**

> Technology will change compliance. And yes, some jobs will be lost, but most compliance professionals will be able to devote their time and energy to doing more productive compliance work, rather than just managing the data.

STAR Platform User and CCO of Asset Manager with $310B in AUM

EMBRACING CHANGE

The job of compliance officer is already changing. Technology is on the march. Regulation is in no danger of letting up, nor will the need for people who can stay on top of it. Conflicts of interest and market abuse have the potential to bring down individuals and firms alike. Compliance officers will more and more need all the help they can get. Compliance technology will increasingly be able to provide that help.

StarCompliance has been writing compliance software and building compliance platforms for nearly 20 years. Hundreds of thousands of people use our software in enterprise financial firms in more than 50 countries. Optimizing compliance programs is our ultimate calling. Let us help you optimize yours

Book a FREE demo now.