NSCP
THE NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

JUNE 2016 SPECIAL REPRINT
Currents

Compliance Becomes a Boardroom Issue

By Tyler Nunnally and Paul Resnik

Financial services firms face increased financial and reputational risks as regulators switch from prescribing rules to enforcing principles-based standards.

The recent Department of Labor (DOL) fiduciary rule has sent shock waves throughout the financial advice industry. Principles-based regulation is at the core of the DOL rule which is a dramatic shift away from the way suitability standards have been applied in the past. Moreover, signs seem to be pointing to the fact the SEC and FINRA are not far behind. All indications are that there is no turning back.

These regulatory changes are new to the US, but they have already been widely applied across the UK. Principles-based regulation has been the foundation of British financial services' reform since the Financial Services Authority's Retail Distribution Review (RDR) following the Financial Crisis. In addition to having a significant presence in the US, our firm has operated in the UK for well over a decade as a leading provider of investor risk profiling solutions to the industry.

We have witnessed the evolving regulatory landscape in the UK firsthand and have been advising FINRA on matters of investor risk profiling in the US. It is our desire to share these experiences with you in the hope that it will better prepare you for the future and help shape the way that you think about your job as a compliance professional going forward.

OLD WORLD COMPLIANCE VS NEW WORLD COMPLIANCE

At its heart, a principles-based regulatory system changes the compliance burden on financial services firms.

About the Authors

Paul Resnik is Co-Founder and Director of FinaMetrica, www.riskprofiling.com. He can be reached at paul.resnik@finametrica.com.

Tyler D. Nunnally is the US Strategist for FinaMetrica. He can be reached at tyler.nunnally@finametrica.com.

"Old-world" compliance	Prove that specified procedures were followed. Judgment of compliance is "list-based" – was everything on the list completed?
"New-world" compliance	Prove that processes & tools are "fit-for-purpose". Judgment of compliance is "outcome-based" – were systems designed to produce "suitable" outcomes for customers?

This change is profound. It changes the way compliance is implemented, from an operational level right through to the boardroom. Directors must be aware that "new-world" compliance places their businesses at heightened financial, legal and reputational risks.

In the new-world, proving suitability requires you to meet what we describe as the "Five Proofs":

1. Prove that you know the client.
2. Prove that you have identified mismatches and examined alternatives.
3. Prove that you know the products being recommended.
4. Prove that you have explained the risks in your recommended plan and products.
5. Prove that the client has given their "informed consent" to accept the risks that you have explained.

Of course, the foundation of those proofs is an agreed upon and consistent process for quantifying and contextualizing risk. There are four key areas of consistency required:

1. Reliable and valid risk tolerance assessment methodology.
2. Proven algorithms to link risk tolerance measurements to portfolio solutions.
3. An agreed upon and standardized language of risk.
4. A standardized process of demonstrating examples of risk and return in relation to a risk tolerance score.

THE OLD WORLD IS VANISHING

In the old-world, a regulatory failure meant:

1. The business had to admit that its processes and

procedures were deficient; they did not allow for the prescribed steps to be completed.

2. Inevitably, the company would publicly order a review to be conducted so the "operational" shortcomings could be exposed and rectified.
3. The business reputation was restored on an "everyone makes mistakes sometimes" basis.

As the costs of regulatory failure were low, compliance was often delegated, relegated and lacked a real voice within the business. Compliance invariably played catch up to sales. By unspoken convention, or sometimes by decree, the sale always had priority and nothing was to derail it.

Commonly, Compliance was devolved to line-manager / legal department levels, where the focus was on process rather than intent. It was difficult to engage senior executives in compliance discussions, and unprecedented for such discussions to reach board level unless significant legal action was afoot.

The life of a compliance professional had a miserable certainty. Rules were painfully detailed, their jobs frustrating, and they were more often than not expected to "stay in their box." Even when it could see a better way of doing things, Compliance was mostly not listened to, being told that complying with the letter of the law was all that was required. In summary, the "regulation by detailed rules" was ineffective.

WHY REGULATION IS CHANGING

The change in emphasis is an acknowledgment by regulators that the old rules based system has failed to protect investors because a "tick-a-box" style of regulation:

- Is unresponsive to change and evolution in market offerings as regulators are not able to respond quickly enough to ensure the rules keep pace with market developments;
- Encourages an ancillary approach to compliance, where the intent of the rules is often ignored or forgotten; and
- Devolves responsibility for compliance to lower levels of the organization, where it is viewed as a purely operational issue.

A "standards based" approach goes a significant way towards overcoming these issues. As an added benefit for compliance professionals, it offers the prospect of more intellectually challenging and rewarding work, and a far louder voice within the business.

Standards based regulation is dynamic by nature. Firms must evolve their compliance response when introducing new products and services into the market. A regulator can never be as responsive to new product development as the firms that are developing them. By requiring firms to be compliant at all times, the obligation falls back onto the firm to maintain a defensible compliance regime.

With this approach, Compliance is no longer an afterthought, and becomes a partner in designing products and delivering them to market. A great deal of thought must be invested in these partnerships. Subsequently, professionals have to be smarter than ever before because regulators will require firms to produce its rationale for the compliance regimes they implement.

Meanwhile, standards based regulation elevates the discussion within organizations. The simplistic clarity of tick-a-box systems allowed compliance to be devolved to levels of the organization responsible for "doing" and not necessarily "thinking." But the new Compliance requires thinking and decision-making which elevates it to senior management and director levels.

THE NEW WORLD IS HERE

In the new-world, regulatory failure means:

1. The business has to admit that it put its own interests above those of the client by failing to create systems that would deliver the regulator's desired outcomes to the client.
2. The traditional "review" is ineffective, as the failure is not operational, it is structural. That elevates the review to senior executive and board level.
3. Being found to be "acting in self-interest" poses immense reputational risk that may not easily be forgiven, and is likely to lead to litigation.

The cost of regulatory failure in this new world order is earth shattering.

Financial services success is founded on trust; and trust is destroyed when a service provider must admit they ignored their clients' needs, and put their own needs first. Such a breach of trust could destroy a business's reputation overnight. Even a global business could be wounded irreparably by an admission that it lacks probity and honesty.

In this new world, Compliance must become a part of the firm's DNA. It can no longer be treated as remote or trivial, and has to be embedded in the corporate culture. Increasingly, Compliance will become the concern and even a key performance indicator of senior management and board members, so it must have a new and powerful voice within the business.

In this new world, the role of the compliance professional changes fundamentally, and when the certainty and comfort that checklist regulation provides is removed, each firm must write its own rules and processes from scratch.

MEETING THE NEW STANDARDS

The traditional comfort of an externally imposed checklist was always in its completion – when the list was done, you knew that you were done. The compliance was "completed." You had the ticks and signatures to prove it! That checklist

removed doubt. If it wasn't on the list, it usually wasn't on your radar. Compliance professionals knew exactly what they did, and did not, have to worry about.

The standards-based regulations don't just remove checklists – they stand the whole process on its head. Now, compliance professionals must decide for themselves what they should worry about and what needs to be done to address those concerns, so that regulator's standards can be met. It is both a liberating and daunting opportunity which revolves around the concept of "suitability".

As mentioned earlier, proving suitability requires you to meet what we describe as the "Five Proofs":

1. Prove that you know the client.
2. Prove that you have identified mismatches and examined alternatives.
3. Prove that you know the products being recommended.
4. Prove that you have explained the risks in your recommended plan and products.
5. Prove that the client has given their "informed consent" to accept the risks that you have explained.

These five proofs combine to create a logic and framework that leads to "good advice." They also provide a demonstrable and reviewable process should it become necessary to legally justify a recommendation.

Know the Client

You must be able to prove you know your client's situation, needs and aspirations. This can be a detailed process, and many firms have tried to short cut it over the years in order to conclude a sale more quickly. However, this approach is fraught with danger. Profiling your customer effectively requires a detailed understanding of their risk tolerance, risk capacity, needs and current situation. Without this knowledge, it is difficult to support an argument that the advice was "suitable." At best, advice based on insufficient data can only ever be a guesstimate, as opposed to prudent which is a fundamental aspect of a fiduciary duty of care.

Identify Mismatches & Examine Alternative Strategies

This proof is becoming even more relevant with the increasing move toward fiduciary standards. Firms must be able to prove that they examined the alternative strategies available to the client, and made a decision based on what would best suit them.

For example, the best strategy for a client with high debt levels may be to retire some debt rather than invest in equities. These alternatives should be evaluated against the client profile for suitability. Alternatively, to achieve their articulated goals, someone contemplating imminent retirement may need to be encouraged to continue working if they do not have the means available to reach their goals and have no other options.

Know the Products

This is, potentially, the most confronting of the five proofs as many financial advisors do not have a detailed knowledge of the products with which they deal. In many cases, the products simply appear as part of suite of products that the advisor is authorized to offer.

This proof does not require that every advisor have an encyclopedic knowledge of every product and be able to present every detail "off-the-cuff." Rather, it requires that the advice system have a methodology of correlating the product to the client, on the basis that the product is judged to meet the client's financial needs and risk tolerance.

For example, our firm provides that methodology by mapping risk tolerance scores to investment portfolios, and combines measures of both risk tolerance and historical performance. While the algorithms underpinning this process are complex, the outcome is simple: an advisor can now tell the client (or the court), "I chose this option because it was best aligned with your risk tolerance and needs."

In the UK, where investor focused principal based regulation has been in force for a few years, this has resulted in a simplification of recommended portfolios. If you can't explain what it does and how it's likely to behave in a downturn, it's too dangerous to recommend.

Explain the Risks

This proof is vital. Yet it is impossible to meet without the prerequisite of knowing the product. It is necessary to have a methodology that allows for risks to be fully disclosed in terms which the client will be able to understand and comprehend.

For example, our process creates that methodology by mapping the risk tolerance score to a model portfolio, which allows performance risks to be explained in words, graphics and numbers. Risk for a particular equity exposure can then be readily explained in the contexts of past experience and anticipated volatility against two benchmarks: specific answers to questions in the investors risk tolerance assessment, and typical answers consistent with the investor's risk group.

Obtain "Informed Consent"

When a client understands the details and risks of a financial proposal prepared for them based on their profile, he or she can give "informed consent", a term imported from medicine which presents some parallels with financial advice.

In the past, healthcare was very paternalistic; doctors did what they thought was best for the patient. This frequently led to patients not being told of their diagnosis or the risks of a treatment prescribed for them.

Similarly, in financial services, it was common to assure the client that they did not need to be concerned with the details of their investments, as the advisor had made their decisions for them. But those times have gone, just as they have in medicine.

Today, patients' rights to know and decide are paramount in healthcare. Before a medical intervention, the patient's situation is fully disclosed, along with treatment alternatives and risk/benefit analysis for each treatment option. With this knowledge, the patient is equipped to give their "informed consent" to allow the medical intervention to proceed. Similarly, in financial services, a client who understands the risks of a potential action and actively consents to it is more likely to be satisfied with that action and less likely to seek redress against an advisor if financial losses exceed their expectations.

As previously identified, the foundation of these five proofs is an agreed upon and consistent process for quantifying and contextualizing risk. There are four key areas of consistency required:

1. Reliable and valid risk tolerance assessment methodology.
2. Proven algorithms to link risk tolerance measurements to portfolio solutions.
3. An agreed and standardized language of risk.
4. A standardized process of demonstrating examples of risk and return in relation to a risk tolerance score.

We have worked with many organizations around the world and have seen the inside processes of plenty of others. In our experience, very few would be able to demonstrate these consistencies across all engagement channels and across functions within each channel. This is particularly true for operators of robo-advice platforms, as very few robos appear capable of demonstrating suitability. Robo-advice will be addressed in greater detail momentarily.

A reliable and valid risk tolerance assessment methodology is "true to label" and "fit for purpose."

True to label means the assessment should do what it claims to do, which is assess risk tolerance. Many risk tolerance assessments do not assess risk tolerance at all. This is evidenced by the fact that **British** and **Canadian** regulators recently studied a number of widely used risk tolerance assessment tools, and found that the vast majority were "not fit for purpose." The British regulators determined that over half of all suitability claims were derived from investment selections that did not meet investors' attitude to risk.

Establishing that a methodology does address risk tolerance does not automatically suggest it is fit for purpose. We have seen risk tolerance assessments that have no scientific basis; no evidence of validation or reliability; and no disclosure of data.

Similarly, not all algorithms are created equally when it comes to linking risk tolerance measures to investment selections. Algorithms are, at their most basic, simply a decision hierarchy. Within that structure many assumptions, exclusions and decisions are made, and some, or even all of those decisions could be incorrect. Once again, rigorous scrutiny and testing is necessary to establish consistency and reliability in this area. In addition, the language of risk is an acute problem throughout the industry, since as a standard language to describe risk has never been agreed upon. Indeed, it has seldom been discussed as an issue. This is a grievous omission and would be considered unacceptable in other professional domains.

For example, in medicine a blood pressure reading is a universal language understood by all. Everyone knows what a reading of 120/80 is telling them. But in financial advice, the terms "high-risk" and "low-risk" are all but meaningless, as they can mean radically different things to the different people who might utter them.

The standardized language of risk is a precursor to standardizing the explanation of risks and returns in relation to a risk tolerance score. This explanation is critical as it frames the investor's expectations. High volatility is not necessarily a problem provided the client's risk tolerance can accommodate it, and the client understands and accepts the potential for volatility. This process ties into the fifth proof discussed earlier – obtaining informed consent. This consent is only possible when the investor comprehends what he or she is agreeing to.

CREATING & DEFENDING YOUR COMPLIANCE SYSTEM

The business must now define its own processes and procedures based on what it believes is necessary to meet the principle articulated by the regulator. It is:

- A responsive model - as the business changes it must redefine and redevelop its own systems;
- A "reasoned" approach - the business cannot blindly follow a set of external rules; and
- It must be strategic and not just operational - elevating compliance to senior management and board levels.

The new environment demands new approaches to compliance. The emphasis is no longer on reliance and adherence to detailed prescriptive rules. Today, compliance means creating a standard of conducting business that delivers against regulatory objectives.

In this new world, the standards that a business maintains are very much on public display, and open to the public and legal scrutiny. To be compliant, the business must have a valid, defensible basis to explain:

- Why it has adopted its systems; and
- How it has validated that its operational processes and tools meet the regulatory standard.

A key step in creating a robust, defensible compliance system is to test the effectiveness and suitability of the processes and tools used in the creation and sale of products and services. This testing should be done first on the individual components and tools within the system, and secondly, on the overall system itself.

The process is one of due diligence: a way of assessing if a system or tool is both fit for purpose, and true to its label. In a financial services context, it is an investigation or audit of a process, procedure or policy asking:

- What is the regulatory standard to be met?
- What alternatives exist to address that standard?
- Are the alternative solutions fit for purpose?
- Are the alternative solutions true to label?
- What are the relative merits of each solution?
- Why is the alternative of choice superior or at least equal to others?

It is immediately obvious that a business simply cannot publicly argue that it went through a due diligence process, but then selected an inferior or unsuitable alternative. It is an admission of a lack of care or incompetence, or both, that would inflict massive reputational damage and invite individual or class action in the courts. Equally obvious are the many challenges to be faced by compliance professionals and businesses as they move to standards based regulation. There are no "rules." You must create them yourself, and be prepared to defend your logic, reasoning and choices.

CASE STUDY: ROBO-ADVISOR DUE DILIGENCE

The explosion of robo-advice provides a timely case study of the challenges of conducting a rigorous due diligence process. The person undertaking the diligence must, in effect, write their own criteria and methodology for proceeding as there is no "standard form" that must be followed. From the outset, compliance professionals will be required to think and act differently, as there will be no "black-letter-law" to reduce compliance to a "tick-a-box" list. The analysis begins with this fundamental question: "What is a robo-advisor?"

At its most basic:

1. A user completes an online process of giving information about themselves.
2. A computer algorithm matches that data (information) to the "best match" solution.
3. The robo recommends a course of action – an investment portfolio.

Risks can now be identified for each aspect of the robo's operation.

Step 1 – Data Collection

The robo may fail to ask for the correct data or the customer may give false data by accident or deliberately. How are these risks addressed? Is there a sound logic and scope for data collection? Are systems in place to detect data that signifies an irregularity or mistake? How are exceptional circumstances to be dealt with?

It is not enough for a due diligence process to merely establish that an assessment of risk tolerance is being made. The test used may be unfit for the purpose, or untrue to its label. We have seen robo data collections that vary from very good to extremely bad. In the very good, the robo builds a detailed profile of the customer taking into account their risk tolerance among other factors. We explore a due diligence of risk tolerance processes in the following section.

Step 2 – The Algorithm

The basis for matching a set of inputs with an output could be flawed. This is a particularly tricky area to assess thoroughly, as algorithms are often locked away inside black boxes where they are considered proprietary knowledge that cannot be shared.

A locked box of unknowns must surely be one of the greatest compliance risks to be faced. It is, perhaps, no surprise that algorithm flaws were named as the most serious risk in robo-advice by 46% of respondents in a recent survey by the Chartered Financial Analyst (CFA) institute. Some of these unknowns include:

How is the algorithm making recommendations? Are there biases or flaws that could lead to inappropriate recommendations? What checks and balances are required to monitor the recommendations being made? How does this algorithm compare to others in use within the firm, for example in the "human" distribution channel?

A firm cannot disclaim its responsibility for answering these questions by saying "we rely on the algorithm." It will be the financial services firm that is brought to account if the algorithm is found to be wrong. The computer programmers who wrote the algorithm are not the product issuer, and are unlikely to enjoy the capital backing of a global bank or asset manager. Lawyers and regulators will be following the money.

This is a particular risk for purchasers of "white-label" robos, where the algorithm may never be visible to anyone.

Step 3 – The Recommendation

Has the data's passage through the algorithm resulted in a suitable recommendation? Are there any weak links in the chain that could lead to an unsuitable recommendation being made? How would such anomalies be detected and examined?

This is a cursory examination, but it goes some way to detailing the process that might be used to highlight the risks that needs to be considered in a due diligence process. An argument could be made that in order to conduct a rigorous due diligence of a robo-advice system, a compliance professional would need to assess three key risk areas:

1. Business risk
2. Regulatory risk
3. Investment suitability risk.

CASE STUDY: RISK TOLERANCE DUE DILIGENCE

Assessing risk tolerance is a critically important stage of the financial advice process. Regulators consistently point to it as being an absolute foundation for any recommendation, along with a range of other factors. Yet no regulator prescribes what a "good" (or appropriate) risk tolerance assessment process would look like, as compared with a "bad" (or inappropriate) process.

As market leaders in the field, we have developed an evaluation process with the assistance of two experts in psychometrics from the London School of Economics to help firms conduct due diligence on risk tolerance assessment tools. We can begin by following the same steps we took with the robo advice advice. Once again, we start with a fundamental question: What does a risk tolerance assessment do? At its most basic the process, the assessment:

- Elicits responses to questions about risk;
- Uses those responses to help build a person's risk profile; and
- Indicates an investment asset allocation that would be consistent with that risk profile.

Risks can be established for each of those stages which are just a few of the many critical risk points that a compliance team would map in a detailed strategy session. In step 1, we must ponder if the questions are the correct ones to ask to solicit the response data we need. How would we control for unexpected or divergent outcomes? Do the questions do what they purport to do – which is assess risk tolerance? (This is not a moot point – many tools that we have seen do not, in fact, do what they claim to do). Finally, how is the validity of the asset allocation for a particular risk profile to be tested or confirmed?

There are two other critical key questions to address in a due diligence of risk tolerance assessment tools:

1. Is the risk tolerance assessment tool fit for purpose?
2. Is the risk tolerance assessment tool true to label?

These are the investigations we recommend be undertaken to establish the answers:

FACE VALIDITY – On reading the questionnaire, does it make sense? Will clients be able to understand the questions and give relevant answers? On their face, do the questions appear to be about financial risk tolerance as opposed to tolerance of more generalized risks? Is there a variety of questions that probe different aspects of personality?

DESIGN PROVENANCE – Does the test have expert origins? Did relevant field experts or academics contribute to its development? Can their credentials and work be independently verified?

ACADEMIC RESEARCH, TESTING & SCRUTINY – Is the data available for academic review and use? Have results been published in academic peer reviewed journals? How often is the test reviewed and retested?

QUESTIONNAIRE ASSUMPTIONS – What are the origins of the questionnaire? Is it based on data or theory? Do the inherent assumptions in the questions appear fair?

RELEVANCE: NORMS & TEST SAMPLE – Has the questionnaire been tested against a sample population that is real and relevant (for example, a consistent age group)? Is there thorough information about the norms and the process which develops norm groups?

USABILITY TESTING – Has the test been proven to be useable? Can people complete the test alone without human assistance?

Other questions can be asked around the test's understandability, factor analysis, correlation matrix, reliability and construct validity. But for our purposes here, this list demonstrates the hidden complexities that can flow from asking those two apparently innocent questions:

- Is the risk tolerance assessment tool fit for purpose?
- Is the risk tolerance assessment tool true to label?

CONCLUSION

In closing, we have covered several important issues for you to consider and hopefully left you with a lot to think about. As the regulatory landscape evolves, there will be an ever increasing requirement to adapt to change. It necessitates new policies and procedures and in some instances, a need to completely rewrite compliance rulebooks. Perhaps most importantly, it requires a new way of thinking about compliance and risk management. Firms and compliance professionals will have to change in order to thrive and to survive. As the old saying goes: "Adapt or perish, now as ever, is nature's inexorable imperative."

To continue the discussion on robo-advisors, the authors have graciously provided a link to the firm's latest report entitled "The Robo Revolution". Click here to access the report:
http://www.riskprofiling.com/complimentaryereport ★