



EFFECTIVE BOARD ENGAGEMENT

Meagan Birch, MLRO & Compliance Officer

THE FABLE OF THE WATERMELON EATER

Bringing about change in a group of people is perhaps the most difficult task anyone can undertake. An old fable sheds light on one technique for encouraging change. This story is for us strangers who wander into a land and find people who are afraid of monsters.

Once upon a time, a man wandered into a strange land. Hence, he became “the stranger” to those who lived in the land.

The inhabitants of the land befriended the stranger – they provided him with food, shelter, and the necessities of life plus a few of the luxuries. Since they were kind to the stranger, they told him to stay away from one field that was inhabited by monsters. They were earnest in their warnings. The stranger’s curiosity was too powerful for him.

One day, while alone, he wandered into the field to see what monsters were there. He was surprised to find that the “monsters” were watermelons. He didn’t understand how the people had decided that the watermelons were monsters, but he would show the people that they had nothing to fear from the monsters (a.k.a. watermelons).

THE FABLE OF THE WATERMELON EATER

The stranger cut the vine of a large watermelon, carried the watermelon from the field into a village of the people, and ate the watermelon to demonstrate how harmless it was. The people were terrified.

This stranger was a bigger monster than the monsters that lived in the field. In horror, they killed the stranger.

Years later, another woman wandered into the same strange land and again the inhabitants were welcoming. They warned her of the monsters in the field. This stranger's curiosity also was too powerful for her. One day, she wandered into the field to see what monsters were there.

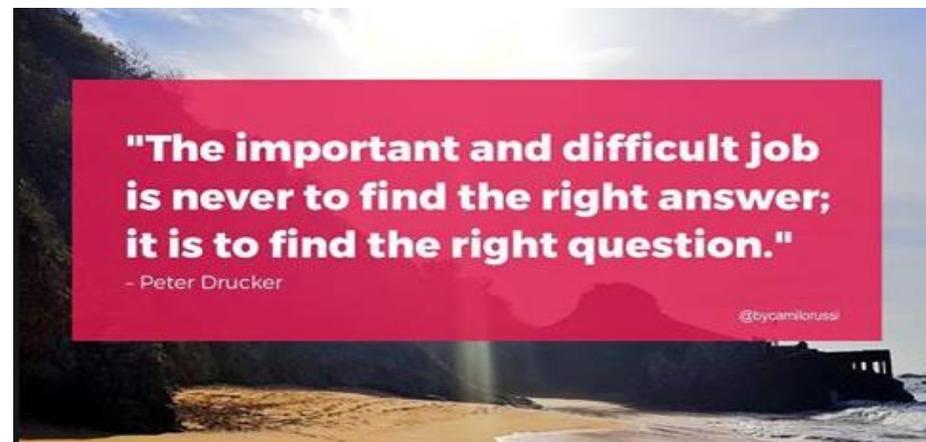
She was surprised to find that the “monsters” were watermelons. She didn't understand how the people had decided that the watermelons were monsters.

THE FABLE OF THE WATERMELON EATER

She went back to the village where the people let her live with them. Each day she would talk to the people about the monsters. She agreed that the monsters were indeed fearsome. She learned why the people decided that the watermelons were monsters. Weeks passed with continuing talk about the monsters.

In time, this stranger convinced the people that the monsters were very similar to large melons that people in her land far away grew and ate. She built up the courage of the people to the point where they went into the field and took a watermelon back to their village. After watching the watermelon for many days, they all decided it was safe to eat it.

Now the people of this land grow their own watermelons and enjoy eating them.



RISK & COMPLIANCE

The Brief

Historically, Compliance needs have been managed by the legal department who oversaw compliance with the support of service from an advisory firm as needed. The previous CF11/10 resigned and the Firm is required to appoint a new CF11/10 within 12 weeks.

There are 4 weeks left when a compliance consultant is hired. As a smaller company the overall compliance risk is considered to be LOW. This could have contributed to a light-touch approach to Compliance.

The Firm continues to grow and is now just over 150 strong. With the upcoming regulations of **GDPR** and **Senior Manager Regime** combined with desire to secure **ISO Compliance** – it is recommended that the approach to Compliance is improved to ensure the Firm is fit for stability and growth.

Key Priorities for Compliance:

- Compliance **Current State Assessment**. The Compliance Officer will review the Firm's existing Compliance Control Framework and determine if there are any areas that require improvement. The findings will be discussed at Risk Committee and at Board to approve next steps
- Assessment and **Remediation of the Compliance Controls** and Compliance Manual with associated policies and procedures
 - Many procedures are not documented and in the event of an incident or being asked to share them they will have to be created by different teams who have other formal responsibilities; some governance forums do not have a documented Terms of Reference and others still have ToR's that are out of date.
 - Compliance Policies; some are current but others have not been updated recently to ensure they reflect current need/ways of doing business. E.g. when surveyed, only 3 out of 20 employees knew about the Firm's Whistle-blowing policy or where to find it.
 - (Expected to take 3-6 months of focussed work)

RISK & COMPLIANCE 2

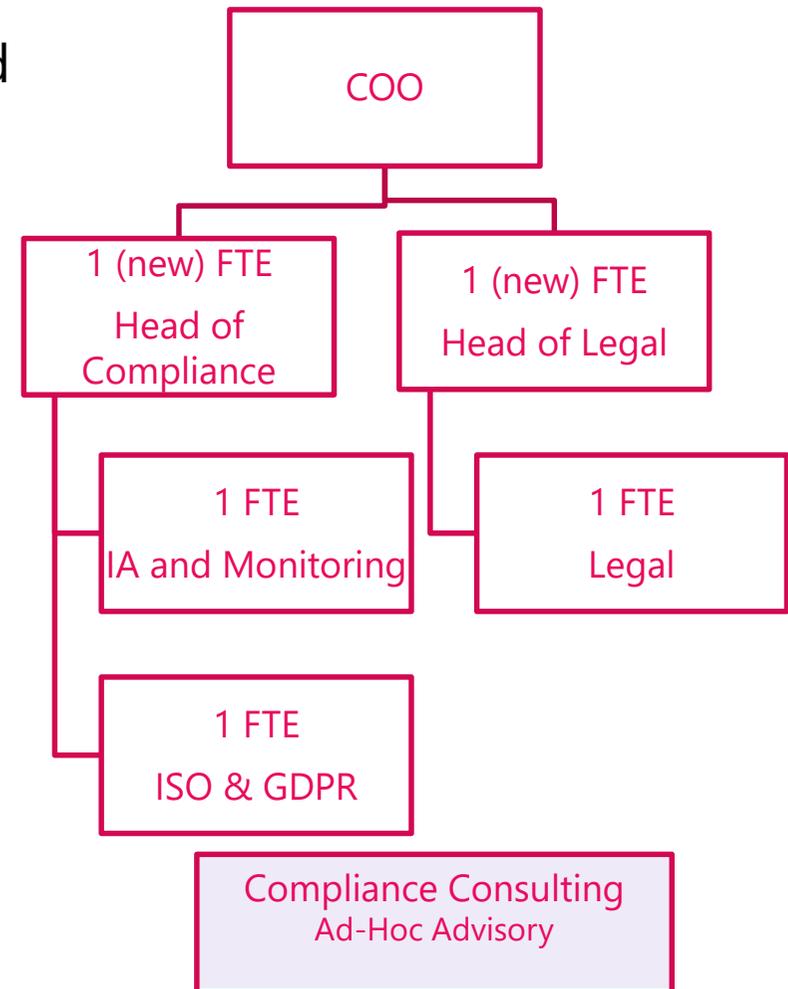
- **GDPR** – Compliance function will establish and lead the project to ensure compliance across the Firm – expected to take 4 months (July 18).
- Preparation & Submission of the **Compliance Officer's Report** (due Monthly to Board/Risk Committee) and **MLRO Report** (Due now) to the Board for Approval
- **ISO Certification** – Compliance function will establish and lead the project to implement and deliver all actions required for ISO Certification
- Create and Establish the **Information Security, Internal Audit & Compliance Monitoring** functions with fully documented policies and procedures
- Design, deliver & embed a **Compliance culture** – hosting a monthly Lunch & Learn on Compliance Topics; ensuring training programme is complete and effective; establish Risk Champions that feed Risk Committee

CREATING A LASTING COMPLIANCE FUNCTION

Planned Activity

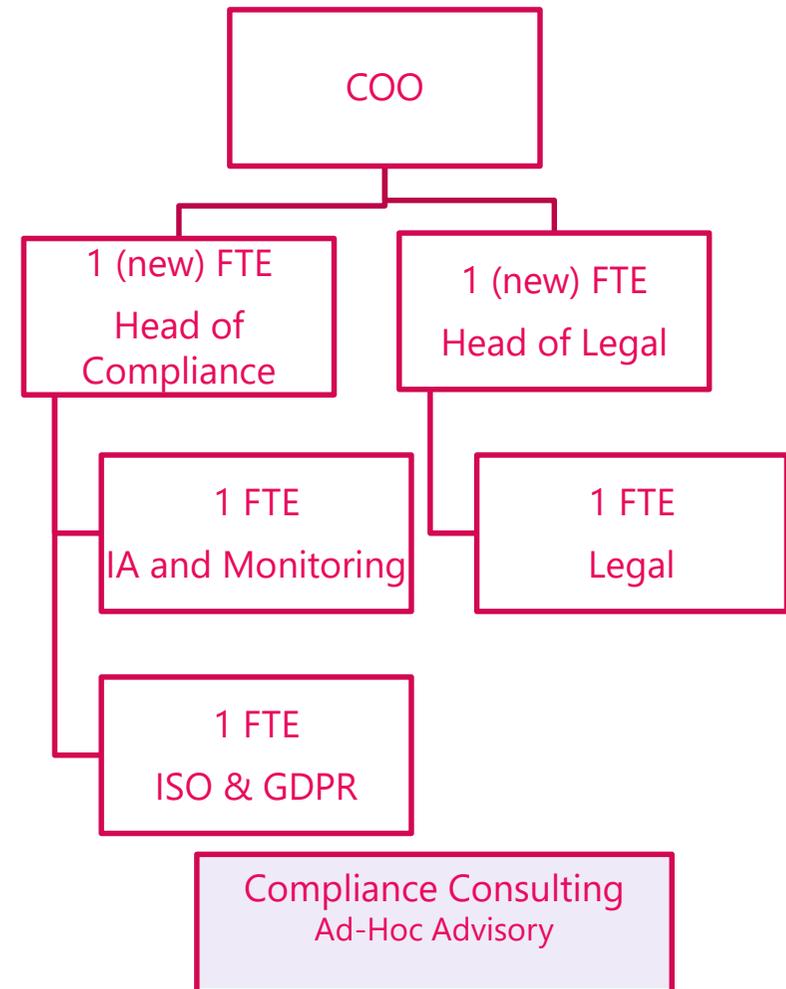
Establishing a Compliance Function as a dedicated and independent team to meet the current demand and to prepare for upcoming regulatory requirements of the Senior Manager Regime which go live in January 2019.

1. Create a new Compliance Team that will lead all activity as listed out in the next slide. The responsibilities captured are what has been identified to-date and will likely expand as we learn more in the coming months.
2. The Compliance Officer has primary responsibility for day-to-day management of advisory services for Compliance.



CREATING A LASTING COMPLIANCE FUNCTION

3. The Compliance Team will also lead on **ISO Certification** by Dec 2018. ISO Certification requires an Internal Audit function.
4. Compliance will lead **GDPR** activity as it is Regulatory Change to ensure compliance ASAP. It is expected to lead the project management activities and this project will also inform a new Information Security role
5. Compliance will have overall responsibility for **Monitoring** and internal testing of effectiveness of controls
6. Overall **Risk Management** will also managed by Compliance whilst leading on remediation



COMPLIANCE FUNCTION RESPONSIBILITIES



RISK & COMPLIANCE

Encouraging Improvements

Proposed Approach:

1. Identify the resources within the Firm that will help deliver a diverse agenda
2. Agree a Phased Approach (that the company can support and buy-in to for delivery)
3. Review All Compliance Controls
 - a) What's Working?
 - b) What requires improvement?
 - c) What's missing?
4. Shine a light on the reality
5. Encourage company to engage
6. Build a team for delivery & educate these key resources to help spread message
7. Try to keep it fun, digestible and engaging!

STAKEHOLDER ITEM	EFFORT	Key Obstacles
Review of Existing Compliance Framework	45 days	Poor Documentation, no handover, lack of interest from business leaders and in some cases poor regulatory / compliance knowledge, apathy
Drafting of Current State Assessment	45 days (and counting)	Every review highlights need for new controls, procedures, policy – staying calm and see it as a journey
Document Compliance Roadmap	5 days	How to make the assessment deliverable by non-compliance resources to effect change recommended
Stakeholder Briefings	10 days – resource constraint	
Delivery to the Board		