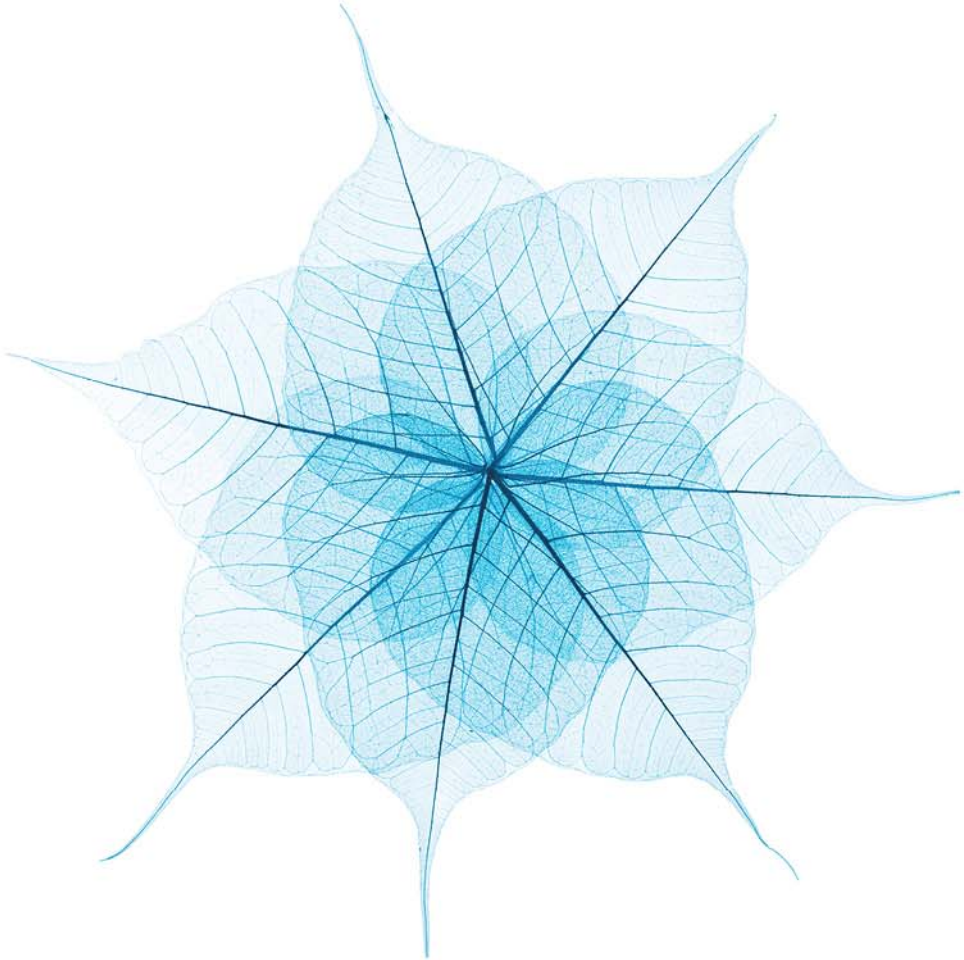
Your World First

C/M/S/
Law.Tax

Individual responsibility – extending SMCR to the entire industry



Simon Morris
Alison McHaffie
September 2017

Looking at …

1. What's going on?
2. What will it look like?
3. The implementation project
4. Senior managers
5. Certified & other staff – & what fit and proper means
6. The rules – and what they mean

The agenda for change

Extension of the bank/insurer regime to all FCA-regulated firms

- CP17/25 envisages implementation Q3 2018 after consultation closing November 2017
- FCA aims for
  - Simple, proportionate & clear
  - Simple and practicable to understand & implement
  - Tailored to reflect different risks and complexities
- But no soft touches – the FCA emphasises high expectations
  - Planning
  - Implementation
  - Execution

2. What will it look like?

The new structure in a nutshell …

Three classes of firm

1. **Enhanced regime –** 1% of firms
   - Significant IFPRU firm
   - Large CASS firm
   - AUM £50bn (3 year view)
   - Inty reg busi revenue £35m+
   - CC reg lending revenue £300m+
   - Non-banks 10k+ reg mortgages
2. **Core regime**
3. **Limited scope, including**
   - APF non-mainstream activities
   - Limited permission CC
   - Pure GI intermediaries

Three classes of staff

1. **Senior manager**
   Prior regulatory approval
   Statement of responsibility
   Responsibilities Map (ER only)
   Handover pack (ER only)
   Subject senior manager + first tier rules
2. **Significant harm – managers & dealers**
   Firm certifies as fit and proper
   Subject first tier rules
3. **Nearly everybody else**
   Subject first tier rules

In other words …

	Prior approval	Statement of responsibility	Annual vetting for F&P	Subject to senior manager rules	Liable for breach in your area	Subject to conduct rules
Senior manager	✓	✓	Must also be fit & proper	✓	✓	✓
Certificate staff			✓			✓
Other staff			Must also be fit & proper			✓

3. The implementation project

Six initial considerations for the project

a) Briefing senior management

b) Resourcing the project

c) Project ownership

d) Providing training

e) Revising policies

f) Protecting individuals

- D&O coverage
- Reassurance

The key tasks …

1. Categorising staff & allocating responsibilities
2. Preparing Statements of Responsibility
3. Drawing the Responsibilities Map (for an Enhanced Regime firm)
4. Codifying fit and proper for the business
5. Grandfathering approved persons or applying for fresh approval
6. Training all staff
7. Papering the HR aspects

Impact for HR

1. Recruitment, identifying roles in scope now/in future/clear role descriptions
2. Regulatory pre-approval
3. Employment contracts
4. Additional remuneration for new responsibilities/Insurance/Indemnity
5. Performance management/objectives/appraisals
6. Annual certification
7. Identifying and escalating breach of conduct rules
8. Disciplinary/termination
9. Updating policy and procedures to meet SM & CR
10. Regulatory references
11. L & D providing appropriate training
12. Supporting handover certification

10 lessons from past projects

Project

1. Senior management commitment & adequate resourcing
2. Transferring to HR department
3. Robustness of records – each step taken
4. Clarity on responsibility – and lines of oversight
5. Embedding BAU procedures – recruitment, change & references

Outcome

6. Concern over responsibility – importance of reassurance
7. Incentivises prudent decision taking
8. Enhances clarity of governance
9. Improves functional oversight
10. Emphasises importance of record-keeping

4. Senior managers

Who is a senior manager?

The job description …

- Takes or participates in decisions
- Part of the firm's regulated activities
- With risk of serious consequences

With designated controlled functions

And responsibilities that must be allocated to a CF

There are three ways of becoming a senior manager …

1st way – your job description

Executive

SMF1 Chief Executive function EC

SMF2 Chief Finance function E

SMF3 Executive Director function EC

SMF4 Chief Risk function E

SMF5 Head of Internal Audit function E

SMF7 *Group Entity Senior Manager function* E

SMF16 Compliance Oversight function ECL

SMF17 MLR function ECL

SMF18 *Other Overall Responsibility function* E

SMF24 Chief operations function E

SMF29 Apportionment of responsibilities & oversight of systems and controls L

Non-executive office bearers

SMF9 Chairman function EC

SMF10 Chair of the Risk Committee function E

SMF11 Chair of the Audit Committee function E

SMF12 Chair of RemCo function E

SMF13 Chair of NomCo function E

SMF14 Senior Independent Director function E

There are also ordinary **NEDs**

2nd way – you hold a "must have" responsibility

Certain responsibilities must be allocated to an appropriate SMF in Core & Enhanced firms …

a) Obligations under new regime (usually CEO)

b) Financial crime (perhaps MLRO)

c) CASS compliance

d) Ensuring board understands obligations (Core firms only)

e) Responsibility for asset management (market Study) governance responsibilities

f) Plus for Enhanced firms, responsibility for

   i. Firm's business model

   ii. Stress testing

   iii. Compliance with Management Responsibilities map

   iv. Independence of internal audit/outsourced internal audit – compliance – risk functions

3rd way – you head a key function at an Enhanced firm, such as …

- Administration of insurance
- Benchmark information
- Collections & arrears
- Corporate investments
- Customer complaints
- Customer service
- Design and manufacturing of products
- Financial or investment advice
- HR
- Incentive schemes
- Investment management
- Investment research
- Issuing commitments
- Lending decisions
- Market making
- Marketing materials
- Middle office risk management in securities trading
- Mortgage advice
- Origination and underwriting
- Payment services
- Processing
- Sales
- Settlement
- Retail & wholesale lending
- Trading for clients

And an SMF …

- Must be pre-approved by the FCA
  - Subject to the 12-week rule
  - May grandfather; otherwise
    - After references
    - And Statement of Responsibilities
    - And summary of handover material
- Must be fit and proper
- May combine appointments
- Must have a handover pack (Enhanced firms only)
- May share (= joint) or split

Responsibility of NEDs

All NEDs (office bearer or not)

- All conduct rules if office bearer
- If not, first tier conduct rules + SC4
- Fit & proper
- Regulatory references

Generally

1. Scrutinise management
2. Monitor reporting of performance
3. Integrity of financials
4. Controls & risk management robust
5. Scrutinise remuneration policy
6. Consider resources, appointments & conduct standards

Duties of integrity, competence, TCF & compliant operations:

1. Understand business & risks
2. Be informed
3. Attend & contribute
4. Challenge when appropriate
5. Ensure proper minutes
6. Your committee
   a) Meets regularly and thoroughly
   b) Open inclusive challenging dialogue
   c) Accesses necessary information
   d) Reports to board

Statements & maps …

Statement of responsibility for all senior managers

Individual statement of responsibilities

- Prepare & lodge when seeking approval & on significant change
- Important opportunity to clarify & codify responsibilities
- Standard form with limited free text

It must be

- Be practical and usable
- Consistent with responsibilities map (for Enhanced firm)
- Complete, not cross-referenced and only contain FCA-relevant material
- Show how responsibilities fit with governance & management

Responsibilities map – enhanced firm

A computer folder with files

- Single, comprehensive up-to-date document to ensure collective allocation of responsibilities complete
- Describing management and governance arrangements
- Showing no gaps and how fit together
- Not limited to UK or to regulated activities

Containing

- Names & responsibilities (reconciling with SoR)
- How responsibilities allocated
- Reporting lines
- Management & governance arrangements
- Including group responsibilities

5. The certification regime & other staff

Certified staff will be …

Employee who performs a specified **significant harm function**

= provide certain services whom the firm supervises, directs & controls

– Involved in the firm's regulated activities

- Is not an SMF
- Is based in UK/deals with UK customers and
- Activities involve a risk of significant harm to firm or customers

And the significant harm functions are

- **Client dealing** – deal, arrange, advise, manage
- **Functions requiring qualifications** – principally retail investment and mortgage advisers
- **CASS oversight**
- **Significant manager** – with significant responsibility for a significant business unit (considering its risk profile, use of capital, contribution to P&L, staffing and customers)
- **Managers of certification employees** – both direct and indirect
- **Benchmark submission & administration**
- **Proprietary & algorithmic trader**
- **Material risk taker, including**
  - Head of Risk, Internal Audit, Compliance
    - And divisional reports
  - Head of Risk in 2%+ of capital business unit
    - And divisional reports
  - Head of material business unit
    - And divisional reports
  - Head of legal, finance, HR, IT
  - Authority over product approval
  - All of their managers
  - Remuneration criteria - €500k/top 0.3%/>others

And certified staff …

- Must be certified as fit and proper
  - To perform every aspect of stated functions, listed in broad terms
  - For 12 months, then reassessed; reassess if function changes
  - Unless up to four week's cover where not require qualifications
- Fit & proper means can perform efficiently & compliantly
  - Integrity
  - Knowledge, competence & experience
  - Qualifications & training

Determining fit and proper

1. **What is the position?**
2. **Its key requirements & main responsibilities?**
3. **Assessing (and recording how)**
   a) Honesty
      - Criminal – proceedings – professional – employment record – non-disclosure
   b) Integrity
      - Breaches – recklessness – condoned misconduct
   c) Competence & capability
      - Experience
      - Qualifications
      - Training
      - Competent
      - Sound judgement
      - Compliant
   d) Financial soundness
   e) Conclusion
      - Addressing negative features
      - Reconciling any gaps

With further attributes for SMFs & NEDs …

For senior staff, fit & proper extends to

- Market knowledge
- Business strategy and model
- Sound & prudent management
- Risk management and control
- Financial analysis and controls
- Governance, oversight and controls
- Regulatory framework and requirements

All other staff

All other staff – apart from twenty designated categories such as cooks, cleaners and receptionists will be subject to 1st tier conduct rules

Staff = employee and providing services to bank subject to its supervision, direction & control

A firm must

1. **Advise** those subject to COCON of the rules
2. **Contractually oblige** an SMF & NED to observe COCON
3. **Report** breaches
   a) Knowledge or suspicion of non compliance
   b) Disciplinary action for breach – warn, suspend, dismiss, dock pay
4. **Train –** take all reasonable steps to ensure understanding, including by training
   a) Broad understanding generally
   b) Deeper understanding specifically

6. And what about the rules?

First tier – rules for everybody

Individual Conduct Rules

- **Rule 1**: You must act with integrity.
  - Manage risk, exercise sound judgement, observe rules as well as honesty
- **Rule 2**: You must act with due skill, care and diligence.
  - Understand the business, the regulations and act compliantly & competently
- **Rule 3**: You must be open and cooperative with the regulators.
- **Rule 4**: You must pay due regard to the interests of customers and treat them fairly.
  - The TCF requirement made a personal promise – do the procedures enable this?
- **Rule 5**: You must observe proper standards of market conduct.
  - All markets, not just listed securities

Second tier – Senior Manager Conduct Rules

- **SM1**: You must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively.
  - Review nose-to-tail and ensure constant line of sight
- **SM2**: You must take reasonable steps to ensure that the business of the firm for which you are responsible complies with relevant requirements and standards of the regulatory system.
  - Have a dashboard of MI & act on it
- **SM3**: You must take reasonable steps to ensure that any delegation of your responsibilities is to an appropriate person and that you oversee the discharge of the delegated responsibility effectively.
  - Check before you trust & hold to account
  - Monitor & be vigilant
- **SM4**: You must disclose appropriately any information of which the FCA or PRA would reasonably expect notice.

Senior manager responsibility

What do the senior manager rules mean?

1. You must **map the business** & identify the risks
2. You must be satisfied these are **properly controlled**
3. You must **skilfully delegate** and supervise subordinates
4. You must **understand the business** and get (and give) the right MI
5. You must determine (or observe) the **right standards** & remedy where not

There will be three grounds for individual discipline

Since 2001 –

1. You **failed to comply** with rules of conduct; or
2. You have been **knowingly concerned in an authorised person's contravention** of a relevant requirement

And from 2018 –

3. The firm contravened a rule [not a Principle for Business]
   a) Which **fell within the responsibility of a senior manager/NED** in his senior management function; and
   b) He **did not take reasonable steps** to avoid the contravention (this is, as for 1 and 2, for the regulator to prove)

And what about the new ground for discipline?

a) The firm contravened a rule

- Typically SYSC or COBS

b) And this fell within your responsibility

- How will we know?

c) And you did not take reasonable steps to avoid the contravention

- What steps did you take?
- Were they reasonable, even if not wholly successful?
- How will reasonableness be measured?
- How can you show what the steps were, some years later?
- How will the regulator approach this?

What a senior manager needs to …

1. **Be aware** of regulatory requirements & wider environment;
2. **Investigate & review** your area of responsibility;
3. **Implement, police and review** appropriate policies;
4. **Structure and control** day-to-day operations, managing delegations;
5. **Obtain & monitor** appropriate internal management information;
6. **Raise issues** & follow them up;
7. **Take pre-emptive action** to prevent breaches;
8. **Adequately respond** to any breach;
9. **Seek and obtain** appropriate expert advice or assurance;
10. **Deploy adequate resources**, especially for control functions;
11. **Keep a proper record** of what you hear, say and do;
12. **Maintain an audit trail** of actions, initiatives, decisions & remedies.

Some examples in practice … CEO engagement

The business model that Mr Palmer developed and maintained … allowed [agents] to be **afforded a high level of flexibility and freedom** as to how they could operate …

Mr Palmer must have been aware that the Firms' business model **gave rise to material risks to underlying customers**, and of the need for appropriate controls and mitigating measures to be in place in relation to these risks …

Although Mr Palmer **was not responsible** for the detailed risk management framework and compliance controls, **his role as the CEO** … and his awareness that the business model gave rise to material risks to underlying customers, meant that he **could not simply rely on the Firm's directors** responsible for risk management and compliance to ensure that these risks were being identified and effectively managed

FCA Decision Notice: Charles Palmer (25 Sept 2015)

… It was incumbent upon Mr Joint [Director] to **inform himself as to the essential elements** of the client money rules…

The **delegation of authority** for the running of JASL's day-to-day business that Mr Joint gave to Mrs O'Brien **did not absolve him from responsibility** for taking adequate steps to inform himself regularly about the business and financial affairs of JASL and to monitor Mrs O'Brien's activities.

Mr Joint's practice of **never asking for any financial information** or **taking any interest** … was unacceptable … he had an **ongoing responsibility to monitor how Mrs O'Brien was performing** and to **identify any issues which required attention himself rather than leaving it to Mrs O'Brien to raise any issues with him**

Upper Tribunal: Terence Joint (21 November 2015)

Executive competence

Mr Tootell was Chief Executive of Co-Operative Bank.

He was **centrally involved in a culture** which prioritised short-term financial gain at the cost of taking prudent and sustainable actions

He did not take adequate steps to ensure that the **Banking Risk team was properly structured and organised** to enable it to provide proper independent challenge and guidance

He was aware that the Corporate Loan Book had been identified as a significant risk to the capital position of the Firm but **did not exercise adequate oversight** in order to ensure that an effective strategy was adequately developed and implemented by the business …

He did not take adequate steps to ensure that the Board were **fully and adequately briefed about risks** inherent to the business of the Firm

PRA Final Notice: Barry Tootell (14 January 2016)

Chief Executive of Millburn Insurance was fined & prohibited for failing to

- **give sufficient consideration to the risks** resulting from its expansion including risks resulting from its delegation of underwriting authority and its use of reinsurance;
- take reasonable steps to **mitigate an identified risk** in relation to Millburn's reinsurance.
- establish and implement **appropriate systems and controls** to monitor and control the nature of the business that was being underwritten for Millburn; and
- establish and implement **appropriate systems and controls** to ensure that Millburn was able to meet its regulatory obligations in relation to technical provisions, capital, reinsurance and financial reporting …

PRA Final Notice: Colin McIntosh (1 February 2016)

Control function effectiveness

Mr Smith was MLRO and compliance officer at SBUK

- In successive years, and despite the warnings of the Internal Auditors, Mr Smith **failed to put in place compliance monitoring plans** which were appropriately focussed
- Despite suffering from being overworked personally and from a lack of resource in the MLRO department, Mr Smith **failed to impress upon senior management the need for further resources**
- Mr Smith continued throughout the Relevant Period to **reassure the board** and SBUK's senior management that SBUK's AML systems were working effectively.
- Mr Smith did not **take sufficient steps to address the concerns** raised by the Internal Auditors and failed to report adequately the results of internal testing.

FCA Final Notice: Steven Smith (12 October 2016)

Ms Grigg **did not properly understand her responsibilities** as Risk Management Director and failed adequately to identify, manage or control the material risks arising out of the Firms' business model …

… she **failed to scrutinise appropriately the existing risk management arrangements**, particularly risks to customers;

She **failed to implement an adequate risk management framework** … because she failed to ensure

- the **Risk Register** adequately identified all material risks
- the **scope and quality of MI** presented to the Board was sufficient, relevant and reliable; and
- the members of the Group Board **understood fully** the Firm's risk exposure by monitoring risk on a proactive and ongoing basis.

FCA Final Notice: Paiivi Grigg (11 December 2015)

So in summary …

What will happen?

a) Event occurs

b) Regulator investigates

c) Calls for SoR/RM

d) Identifies responsible individual

e) Asks

- "did s/he breach?"
- "was s/he knowingly concerned?"
- "is the bank's breach in his/her area and did s/he take reasonable steps to avoid?"

f) You need

- The action
- The record of …

What you will need to show …

1. **Chief executive**
   - Is *really interested* in all aspects of his or her area
   - Oversees delegates and doesn't just rely
   - Secures an effective risk function
2. **Senior manager**
   - Considers and mitigates risks
   - Ensures risks properly managed
   - Puts in place effective mitigations
3. **Control function**
   - Scrutinises and manages risk
   - Calls for resources when needed

The Board has a role in this …

Because it

a) Ensures organisational structure is effective
b) Monitors firm's business objectives & strategy
c) Ensures risk effectively identified
d) Selects and oversees senior management
e) Is alert & challenging

Plus ensures that

f) Risks mapped
g) Responsibilities allocated
h) Clear flow of information against identified metrics & risks
i) Appropriately overseen
j) And actioned

But responsibility is personal, not collective. You can't say …

1. Unfair to pick me out
2. My conduct was not beyond the range of plausible judgement
3. The FCA never criticised us
4. The strategy was agreed by the Board
5. I didn't design the controls
6. It was the deteriorating economy that caused it
7. I did take some steps to improve things

Every one of these arguments was rejected in *Cummings* – the focus is on personal responsibility and personal reasonableness

But there is a good defence – I was competent!

- There were serious flaws in governance & risk management
- Six major issues current on his appointment as CEO
- On appointment interviewed, discussed, met & challenged
- Also commissioned reviews, appointed new heads
- FCA argued not wide enough but Tribunal said …

1. Reasonable initial assessment & not prompted to dig deeper
2. CEO oversees controls but may rely on delegates
3. Only limited authority in large international group
4. Investigated every control failure and oversaw remedies
5. Thus took reasonable steps despite ongoing serious flaws

Jonathan Pottage (UBS) Tribunal April 2012

So what do these cases tell us?

1) Carry out a detailed initial assessment and continuous monitoring
2) Assess operational risk framework
3) Assess governance and controls
4) Due diligence on appointment and clarity on role and responsibilities
5) Ensure MI covers risks not restricted to commercial and financials
6) Reassess as business changes
7) Think “wider implications” at all times

Or, put another way, do …

⇒ The nose to tail test
⇒ The line of sight test
⇒ The dashboard test
⇒ The action test
⇒ The checking test
⇒ The hold to account test
⇒ The monitoring test
⇒ The vigilance test

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
www.cms-lawnow.com

Your expert legal publications online.

In-depth international legal research
and insights that can be personalised.
eguides.cmslegal.com

---

cms.law