LATHAM & WATKINS

Senior Managers & Certification Regime
Reasonable Steps

David Berman

26 June 2019

Contents

1. Backdrop to SMCR

Backdrop to SMCR

- Key objectives of SMCR
  - Reduce harm to consumers and strengthen market integrity – aiming to:
    - levels to take personal responsibility for their actions
    - Ensure firms and staff clearly understand and can demonstrate where responsibility lies
    - Achieve clearer personal responsibility and accountability
    - Facilitate individual regulatory enforcement actions by FCA

"The extension of the SMCR is key to driving forward culture change in firms … The regime will ensure that Senior Managers are accountable both for their own actions, and for the actions of staff in business areas that they lead"

Jonathan Davidson,
Executive Director of Supervision,
FCA

2. Key Features

Key Features of SMCR

- SMCR will apply on a legal entity basis
- Will replace current “approved persons regime” in its entirety
- Categories of individual:
  - Senior Managers: role involves (or might involve) risk of serious consequences for firm, or for business
  - Certified Staff: role involves (or might involve) risk of significant harm to firm or its customers
  - Conduct Employees: broadly everyone else (save for purely administrative personnel)

Key Features of SMCR

- Senior Management Functions
  - Core: chief executive; executive director, partner; chair; compliance oversight, MLRO
  - Enhanced: all of the above PLUS: chief finance function; chief risk function; head of internal audit; senior independent director; chairs of the remuneration, risk, audit and (if there is one) nominations committee; group entity senior manager; chief operations function; other overall responsibility

Key features of SMCR

- Prescribed Responsibilities – more shortly
- Statements of Responsibilities (for Senior Managers)
- Responsibilities Maps (Enhanced regime only)
- Duty of Responsibility (Senior Managers only)
- Conduct Rules
- Certification of fitness and propriety

Key features of SMCR

- Handover procedures (Enhanced regime only)
- Training for all in-scope personnel
- Non-executive directors
  - Senior Managers
  - Others – certain Conduct Rules, F&P requirements and regulatory references will apply

Key features of SMCR

- Prescribed responsibilities

Anticipated PRs		Application
1.	Performance by the firm of its obligations under the Senior Managers Regime, including implementation and oversight	Core
2.	Performance by the firm of its obligations under the Certification Regime	Core
3.	Performance by the firm of its obligations in respect of notifications and training of the Conduct Rules	Core
4.	Responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime	Core
5.	Responsibility for the firm's compliance with CASS (if applicable)	Core
6.	Responsibility for an AFM's value for money assessments, independent director representation and acting in investors' best interests	Core
7.	Compliance with the rules relating to the firm's Responsibilities Map	Enhanced
8.	Safeguarding and overseeing the independence and performance of the internal audit function (in accordance with SYSC 6.2)*	Enhanced
9.	Safeguarding and overseeing the independence and performance of the compliance function (in accordance with SYSC 6.1)*	Enhanced
10.	Safeguarding and overseeing the independence and performance of the risk function (in accordance with SYSC 7.1.21R and SYSC 7.1.22R)*	Enhanced
11.	If the firm outsources its internal audit function, taking reasonable steps to ensure that every person involved in the performance of the service is independent from the persons who perform external audit, including: • supervision and management of the work of outsourced internal auditors • management of potential conflicts of interest between the provision of external audit and internal audit services	Enhanced
12.	Developing and maintaining the firm's business model	Enhanced
13.	Managing the firm's internal stress-tests and ensuring the accuracy and timeliness of information provided to the FCA for the purposes of stress-testing	Enhanced

*Where possible, to be allocated to a NED or a partner who does not have management responsibilities

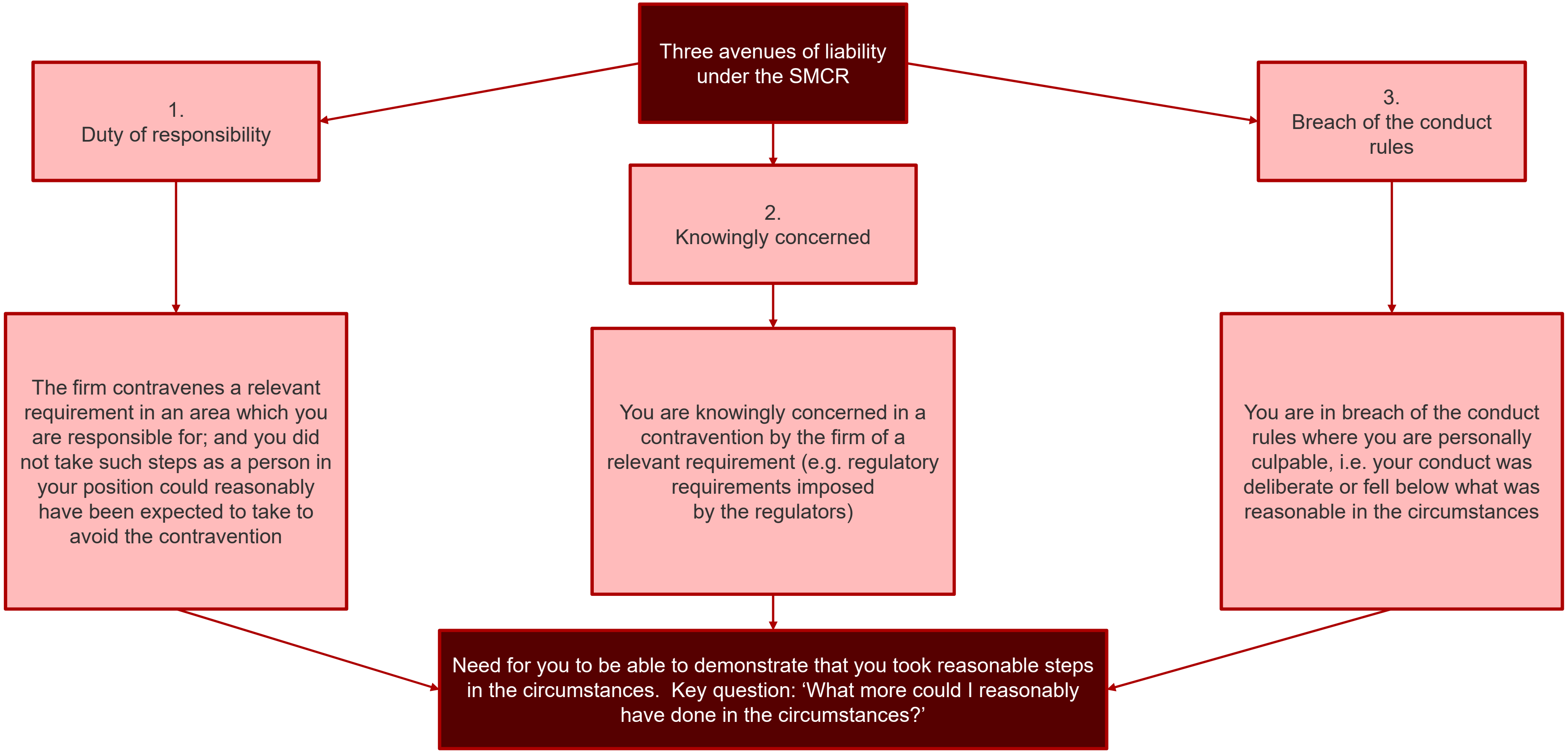
Key features of SMCR

- Conduct rules

	First Tier – Individual Conduct Rules
1.	You must act with integrity
2.	You must act with due care, skill and diligence
3.	You must be open and cooperative with the FCA, the PRA and other regulators
4.	You must pay due regard to the interest of customers and treat them fairly
5.	You must observe proper standards of market conduct
	Second Tier – Senior Manager Conduct Rules
SC 1.	You must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively
SC 2.	You must take responsible steps to ensure that the business of the firm for which you are responsible complies with the relevant requirements and standards of the regulatory system
SC 3.	You must take responsible 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
SC 4.	You must disclose appropriately any information of which the FCA or PRA would reasonably expect notice

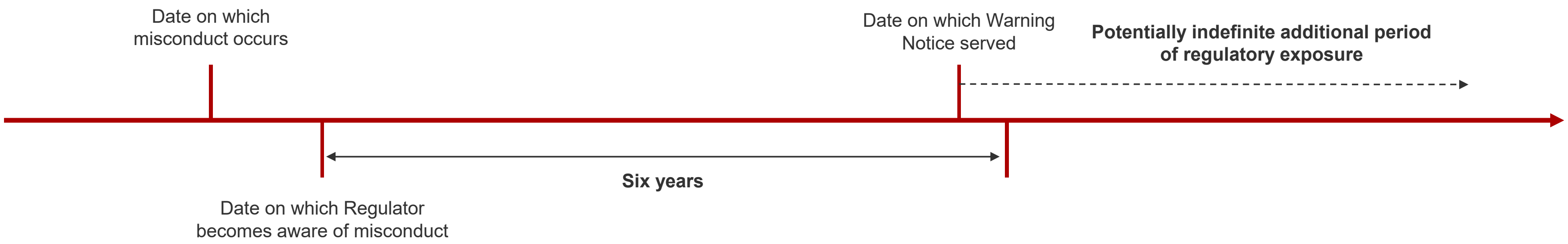
3. Avenues of personal experience

Avenues of exposure under the SMCR



Avenues of exposure under the SMCR

- Post-Tenure Exposure
  - Time limit on regulatory exposure – for how long are Senior Managers exposed under the SMCR?
  - Broadly, six years from the date of the Regulator becoming aware of any alleged misconduct. However, this period could be longer if the Senior Manager has been served with a Warning Notice before the end of six years



4. Regulatory Expectations

Regulatory expectations

- Pottage

Mr Pottage held chief executive and apportionment and oversight roles at certain UBS entities.

The FSA found that Mr Pottage failed to take reasonable steps to ensure that the business of UBS complied with the requirements and standards of the regulatory system.

Particular failings identified by the FSA included:

- Failing to take reasonable steps to identify and remedy flaws in the governance and risk management frameworks; and
- Failing to initiate a review of the systems and controls across the business sooner than he did.

It imposed a £100,000 fine of Mr Pottage.

Mr Pottage referred the decision to the Upper Tribunal.

The Upper Tribunal did not agree with the FSA. The Upper Tribunal found that the FSA did not satisfy it that Mr Pottage's conduct was below that which would be reasonable in the circumstances.

The Upper Tribunal's decision indicates the actions that might constitute reasonable steps.

The Upper Tribunal noted that reasonable steps taken by Mr Pottage included:

1	Undertaking an initial assessment upon becoming CEO – as part of the initial assessment carried out upon becoming CEO, Mr Pottage had held a number of relevant meetings and interviews with managers at UBS.
2	Proactively addressing problems as they occurred – every specific control failure identified in the business had been fully investigated and remedied or was being dealt with in accordance with a defined plan.

Regulatory expectations

- Cummings

Mr Cummings was chief executive of the Corporate Division of HBOS.

During Mr Cummings' tenure, the Corporate Division was the highest risk part of HBOS's business, and had a higher risk profile than the equivalent books at other major UK banking groups. The credit quality of its portfolio was low, and it focussed heavily on property and risk capital, causing it to be highly exposed to changes in the economic cycle.

The FSA commented that the high risk lending strategy pursued by HBOS required a commensurately robust control framework. However, it found that there were significant issues with the control framework during Mr Cummings' tenure.

HBOS plc

The FSA found that Mr Cummings was knowingly concerned in HBOS's failure to take reasonable steps to organise and control its affairs responsibly and effectively with adequate risk management systems.

It also found that Mr Cummings failed to exercise due skill, care and diligence in managing the business for which he had responsibility.

Mr Cummings was fined £500,000 and banned from performing a significant influence function.

The FSA noted that Mr Cummings' failures included:

1	Failing to properly assess, manage and mitigate credit risk by, amongst other things, failing to ensure there was an effective process for prompt identification of transactions showing signs of stress.
2	Allowing a culture to pervade which saw risk management as a constraint to business rather than integral to it.
3	Allowing management information to be of insufficient quality, reliability and utility.

Regulatory expectations

- The "Co-Op" Two

The co-operative bank

Mr Tootell was CFO, and later CEO, at the Co-operative Bank.

Mr Alderson was Managing Director of Co-op Bank's Corporate and Business Banking Division.

During both individuals' tenures, Co-op Bank merged with Britannia Building Society, the long-term effect of which was to force the bank to undergo a liability management exercise to improve its capital position.

The PRA found that Mr Tootell had failed to act with due skill, care and diligence by (amongst other things) prioritising the short-term financial position of Co-op Bank at the cost of taking prudent and sustainable actions to secure the bank's longer-term capital position. He was also knowingly concerned in Co-op Bank's breach of its Principle 3 obligation to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

The PRA found that Mr Alderson had not taken reasonable steps to ensure that Co-op Bank adequately assessed risk arising across the Britannia Corporate Loan Book.

It also found that Mr Alderson had failed to take reasonable steps to ensure that the first line of defence took an adequate approach to risk management and that the available management information was sufficient to monitor compliance with systems and controls. He, too, was knowingly concerned in aspects of Co-op Bank's breach of Principle 3.

The PRA noted that Mr Tootell's and Mr Alderson's failures included:

1	Failing to appropriately escalate risks in accordance with the bank's formal risk management processes. As a result, the risks could not properly be considered, nor could appropriate actions be taken in mitigation.
2	Failing to properly oversee a major due diligence process to ensure that it adequately identified and documented risks.
3	Failing to exercise adequate oversight to ensure development of a clear strategy for a business area which had been identified as a significant risk to the bank.

Illustrative hypothetical scenarios from the FCA

- A firm breaches its capital adequacy requirements as a result of a major loss in a key business unit that has repeatedly breached its risk limits. The risk limits were discussed and set by the Risk Committee and the Board. In this situation, the Regulator might primarily consider whether there are grounds to sanction the appropriate Senior Manger(s), including Heads of the Key Business Areas and the Chief Risk Officer. If, however, the breaches are reported to the Board and/or the Risk Committee, the Regulator may also enquire whether the Board/Risk Committee discussed them and made any recommendations

Illustrative hypothetical scenarios from the FCA

- In an attempt to obtain Board approval for a new, riskier lending strategy, a firm's senior executives submit incomplete and misleading management information to the Board which significantly downplays the risks of such a strategy. The CEO also suppresses any negative or questioning advice on this issue, and consequently the Board approves the strategy which, six months later, causes the firm to breach a number of rules in the Risk Control section of the Regulator's rulebook
- A firm's management fails to monitor the provision of services by a third party under an outsourcing agreement, resulting in an operational risk crystallising in breach of a rule in the Regulator's rulebook

LATHAM & WATKINS

5. Managing personal risk

Managing personal risk

- The importance of demonstrable reasonable steps
- Mind-set and priorities
- Appreciation of where the FCA “is coming from”
- Responsibility cascade
- Approach to culture and conduct risk
- ‘War-gaming’
- Areas of greatest vulnerability…
- Reasonable steps assurance frameworks

Managing personal risk

- Delegation and Control
  - It is perfectly permissible for you to delegate matters. This is understood, and expected, by the FCA
  - However, you must take reasonable steps to delegate appropriately and to ensure that you oversee the discharge of the delegated tasks effectively. As a minimum, you should:

Take reasonable steps to maintain an appropriate level of understanding about matters which you delegated, whether internally or externally	Take reasonable steps to ensure that appropriate persons are responsible for the matters which you have delegated	Ensure there are clear and effective delegation and reporting lines, which may involve documenting these in writing
Take action where progress is slow	Require periodic reports about delegated matters	
Question reports where necessary or appropriate	Act clearly and decisively where there are issues	Challenge implausible explanations

  - While you can delegate authority for dealing with an issue or part of the business, you cannot delegate accountability for it.

LATHAM & WATKINS

6. Scenarios

Scenario 1

- A material control failure has been identified within one of your areas of responsibility. The issue has been duly notified to the FCA (alongside a commitment to undertake an internal investigation)
- You have tasked one of your direct reports with responsibility for commissioning and overseeing a root cause analysis (RCA) into the issue – with a view to understanding whether it was a genuinely "one-off" occurrence or perhaps indicative of wider systems and control failings. You request that the RCA is completed within one month and that the outcome is reported to you in the first instance
- After two weeks, you are presented with a paper containing the findings from the RCA. The paper concludes that this issue was "isolated" in nature and "attributable to human error"; and that no further action is required
- What, if anything, should you do now?

Scenario 2

- Your pack for a forthcoming product development meeting includes a report "for urgent consideration", prepared by the head of Sales. The report is titled "Proposal to expand investor base – opportunistic acquisition"
- On reading the report, you observe that there is a seemingly compelling commercial rationale, and a significant (albeit time-critical) opportunity to seize. The proposition is also directly aligned with the CEO's clear desire to "innovate" and find new sustainable revenue streams
- However, you feel that the report presents a rather one-sided assessment of the proposition, with little discernible reference to risk and the potential down-side(s)
- How do you react?

Scenario 3

- Your latest MI pack includes detailed financial information for various business areas (alongside, for comparison, the previous year’s equivalent figures). You see that the revenues of one business line have increased over the past year by ~300%. The associated footnote indicates that this increase is attributable to a newly-launched product
- How do you respond?

Scenario 4

- You are aware that one of your senior reports has repeatedly failed to undertake his mandatory computer-based training and to attend two professional development off-sites. He is also apparently “relaxed” about the fact that a number of staff who report to him have similarly failed to complete their mandatory training courses
- How do you respond?

Scenario 5

- You are becoming concerned that you are not being kept sufficiently well-informed about impending regulatory developments which may have implications for the firm. You have read a number of newspaper articles recently referring to specific developments that would appear to have major repercussions for the firm. However, none of these appear to have featured in compliance training/bulletins
- What, if anything, should you do?

Scenario 6

- Following “intelligence” received from the Compliance Monitoring team, you suspect that a member of your management team may have disclosed client confidential information to an acquaintance at other institutions. You value this individual highly
- How should you respond?

Scenario 7

- You are attending an interview with the FCA as part of its routine supervisory activity. An FCA representative makes a number of statements which would appear to suggest that he has misunderstood the way in which the firm responded to a series of recent incidents through a remediation/change program. He is evidently under the impression that the firm responded more convincingly and robustly than it in fact did
- How do you react?

LATHAM & WATKINS

7. Practical Guidance

Practical Guidance 1

Questions to Yourself

- Am I satisfied and can I demonstrate that the risk profile for my area of responsibility is appropriate and reflects the firm's risk appetite?
- Am I satisfied I can demonstrate that my team understands and complies with relevant legislative and regulatory requirements (both prudential and conduct of business)?
- Am I satisfied that I foster the appropriate culture in my area of responsibility, and can I demonstrate that an appropriate culture in line with the firm's values has been established?
- Am I satisfied and can I demonstrate that significant events or issues are appropriately escalated and reported in my area of responsibility?
- How do I ensure that any gaps resulting from regulatory changes are identified and appropriate action is taken to address these gaps?
- Having delegated responsibilities, how do I oversee their delivery and ensure that I am kept fully informed of their progress?
- Could I credibly articulate:
  - the firm's stated strategy?
  - the firm's risk appetite supporting that strategy?
  - the firm's risk control framework?
  - the key regulatory risks faced by the firm?
  - the firm's espoused cultural expectations?
- Am I satisfied that my own Statement of Responsibilities and role profile is up-to-date and accurately reflects my responsibilities? If not, am I taking action to address this?
- Is the firm's Responsibilities Map consistent and reconcilable with my Statement of Responsibilities?
- Is my Statement of Responsibilities consistent with the terms of reference of the committees on which I sit?
- In reality, am I also entrusted with, or have I assumed, certain de facto responsibilities which are not documented?
- Do board/committee minutes (to the extent applicable) appropriately reflect my responsibilities? Or might they, for example, present an impression that I am responsible for more than I have signed up to?
- Am I comfortable that I have sufficient oversight of the activities for which I am responsible?
- Am I satisfied that the boards and committees I sit on receive appropriate MI and other information so they can make fully-informed decisions? If not, what action am I taking to address this?
- Can I demonstrate that I fully understand and meet my personal obligations as a Senior Manager under the UK regulatory regime?
- Do I understand the overriding importance to the regulator of clients' interests and market integrity?
- In any given situation, a Senior Manager might usefully ask 'what more could I reasonably have been expected to do in the circumstances?' Or, put another way, 'what could I reasonably be criticised for having not done?'

Practical Guidance 2

Sample interview questions for Senior Managers

- How many certified staff do you have within your area(s) of responsibility?
- Could you summarise the key conduct risks within your area(s) of responsibility?
- Could you explain the three lines of defence model and your role within that model?
- Can you summarise the 'fitness and propriety' requirements and assessment process applicable to employees within your area(s) of responsibility?
- Could you summarise your obligations with respect to handovers and explain how the Senior Manager handover process works in the firm?
- Could you summarise your key responsibilities (as per your Statement of Responsibilities)?
- Could you articulate the risk management framework, risk appetite and tolerances for your area(s) of responsibility? Are you confident that you have sufficient visibility over key operational risk areas? Are there blind spots?
- Could you articulate how your accountability structure chart operates in practice to assist you in discharging your regulatory obligations? Could you explain your delegation model? In particular, how are delegates monitored?
- How do you ensure that employees within your area(s) of responsibility are acting in line with the firm's cultural and behavioural expectations?
- Could you explain how you make sure the systems and controls relevant to or within your area(s) of responsibility remain 'fit-for-purpose'?
- How do you ensure that the right 'tone from the middle' is set and maintained within your area(s) of responsibility?

Practical Guidance 3

Examples of good practice

- Ensure you are alert to ‘red flags’ such as worrying trends, unusual practices or exceptionally profitable products
- Seek and obtain appropriate expert evidence or assurance
- Deploy adequate resources, especially for managing operational risk
- Ask searching questions and challenge implausible explanations
- Ensure the MI you receive identifies risks where relevant
- Exercise reasonable care when considering available information.
- Reach a reasonable conclusion on which to act
- Make sure that knowledge and skills in your function are regularly reviewed and checked as part of development discussions and 1:1s
- Where you are aware of possible breaches, take reasonable steps to ensure that they are dealt with quickly and appropriately
- Attend refresher training on regulatory matters
- Keep abreast of relevant compliance/risk reports, e.g. weekly flash reports relating to all relevant jurisdictions
- Document all formal, on-going delegations and record how you have considered an individual’s capability and competence
- Review your area of responsibility to ensure responsibility has been clearly assigned to a particular individual or individuals with the necessary skills and expertise and oversee them effectively
- Monitor the governance, operational and risk management arrangements in place for the activities of the firm for which you are responsible
- Understand and inform yourself about the activities of the firm for which you are responsible, including ensuring that you:
  - monitor highly-profitable transactions or business areas;
  - monitor individuals who contribute significantly to the profitability of the business area; and
  - maintain an appropriate level of understanding about responsibilities you have delegated.
- Given there should be ‘end-to-end risk accountability’, be aware of which other areas of the firm you rely on for MI and satisfy yourself there are no gaps
- Ensure formal records of all meetings with internal and external committees and boards of which you are a member are maintained, and know where such records are kept and how you can access them
- Ensure that, where involved in a collective decision affecting the activities of the firm for which you are responsible, you are informed of the relevant matters before taking part in the decision, and exercise reasonable care, skill and diligence in contributing to the decision
- Examples of steps that may be considered relevant to preventing a breach occurring or continuing, depending on the circumstances, include:
  - initial business reviews on taking up a Senior Management function;
  - implementing, monitoring and reviewing appropriate policies;
  - ensuring you are aware of regulatory requirements and wider regulatory expectations;
  - instigating investigations or reviews of your area of responsibility;
  - raising issues, reviewing issues and following them up with relevant staff, committees and boards; and
  - maintaining awareness of relevant external developments, including key risks

Practical Guidance 4

What ‘bad’ looks like…

CEO / Director

- Failing to take adequate steps to ensure that the second line of defence was properly structured and organised to enable it to provide independent challenge and guidance to the first-line business
- Being centrally involved in a culture which encourages the prioritisation of the short-term financial position of the bank at the cost of taking prudent and sustainable actions to secure the longer-term capital position of the bank
- Being centrally involved in managing the bank’s finances and capital position in a manner inconsistent with its stated cautious risk appetite and prudent bank management
- Failing to adequately oversee a due diligence exercise in relation to a significant prospective transaction
- Failing to exercise adequate oversight in order to ensure that there was a clear, effective and comprehensive strategy for the loan book(s)
- Failing to ensure that a development or remedial project progressed with the requisite urgency and pace; and to ensure that effective targets and milestones were set
- Failing to take adequate steps to ensure that the board is properly briefed about inherent risks which had the potential to affect the bank’s capital position

Director / Head of corporate banking division

- Failing to ensure that the bank adequately assessed the inherent risks of an acquired loan book
- Failing to escalate these risks to the formal risk management forums and ExCo
- Failing to act in a timely manner to explore options for an alternative strategy (when the existing strategy was known to be flawed)
- Failing to take reasonable steps to ensure that the first line of defence took an adequate approach to the management of risk, including in relation to the identification and management of distressed accounts, and compliance with policies and procedures on collateral valuations and key credit criteria
- Failing to take reasonable steps to ensure that the available management information was sufficient to monitor compliance with systems and controls
- Presiding over a culture which created an environment in which some staff felt under pressure to meet stipulated impairment forecasts; which resulted in over-optimistic decisions being made on impairment budgets, forecasts and provisions

8. Individual accountability versus collective responsibility

Consistency with notion of collective responsibility

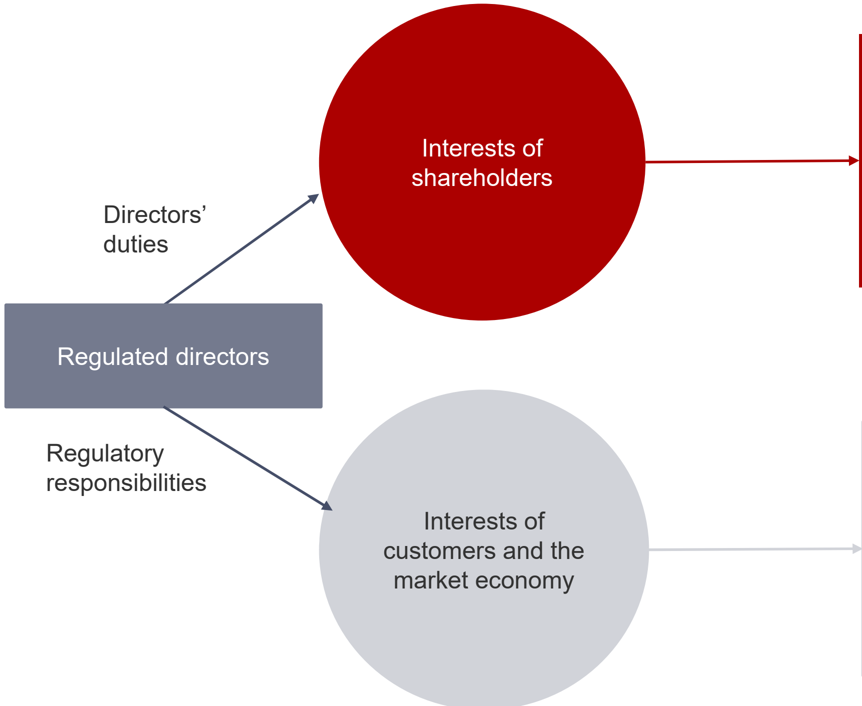
The individual accountability of directors in scope of the SMR will be additional and complementary to the collective responsibilities shared by all directors under UK company law and well-established corporate governance principles, such as the FRC code. In particular, the SMR will operate alongside the statutory and fiduciary duties of directors under UK company law including section 172(1) of the Companies Act, which requires all directors, irrespective of whether they are in scope of the SMR, remain accountable under the Companies Act and, in listed firms, subject to the principles of the FRC Code on a comply-or-explain basis.

PRA Policy Statement 16/15: Strengthening individual accountability in banking, July 2015

LATHAM & WATKINS

9. Regulatory responsibility versus legal duties

Interplay with statutory director's duties



Any UK company director must act in a way that the director considers, in good faith, is most likely to promote the success of the company for the benefit of its members as a whole. This is typically interpreted as acting in the best interests of shareholders.

--------- Potential tension ---------

A director of an authorised firm must discharge regulatory responsibilities, centred on safeguarding customers' interests and the proper functioning of markets. From the FCA's perspective, customer interests are paramount.

THANK YOU

QUESTIONS

&

ANSWERS