A Risk-based Approach to Compliance Monitoring

SHCOG Securities Houses Compliance Officers Group

Presented by Peter Haines

11th September 2023

Contents

- The ongoing importance of monitoring
- The need for expertise
- The importance of a risk-based approach
- Some monitoring crimes
- Directional testing
- The output – a risk-based monitoring plan

Introduction

Can you answer the following questions?

- “How do you identify and manage compliance risk”
- “How have you put together a risk-based monitoring plan?”
- “Does the monitoring plan employ your resources efficiently whilst targeting the higher risks?”

Overriding Questions

- Is monitoring still important?
- Is it more or less important than five years ago?
- Has there been any change in emphasis in the past 2-3 years?
- Does it still need to be risk-based?

- What level of expertise is needed for monitoring to be effective?

Overriding Questions

- Is monitoring still important?
- Is it more or less important than five years ago?
- Has there been any change in emphasis in the past 2-3 years?
- Does it still need to be risk-based?

- What level of expertise is needed for monitoring to be effective?

Why a Risk-Based Approach?

- Compliance resources are scarce
- Why waste time looking at areas of low compliance risk?

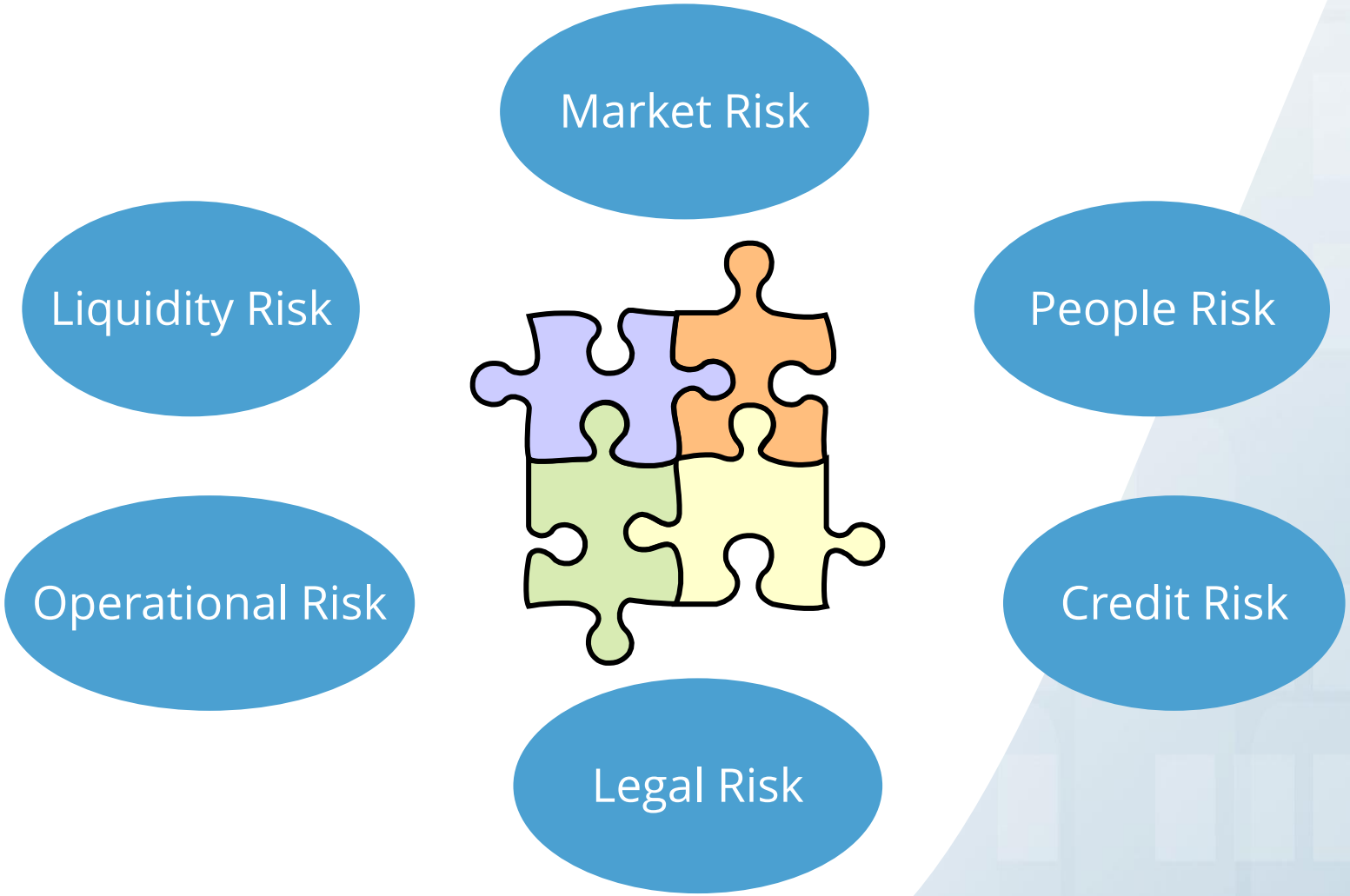
Why a Risk-Based Approach?

Basel Paper on the compliance function in Banks 2005

- "The risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities (together, "compliance laws, rules and standards")

- So you need a Compliance Risk Assessment Process
- Just be careful how you use the acronym….

Where Does Compliance Risk Sit?



ESMA on Compliance Risk

General Guideline:

- The compliance function shall, as part of its tasks, conduct a risk assessment to ensure that compliance risks are comprehensively monitored.
- The compliance function shall establish a risk-based monitoring programme on the basis of this compliance risk assessment to determine its priorities and the focus of the monitoring, advisory and assistance activities.
- The findings of the compliance risk assessment should be used to set the work programme of the compliance function and to allocate the functions resources efficiently.
- The compliance risk assessment should be reviewed on a regular basis, and, when necessary, updated to ensure that the objectives, focus and the scope of compliance monitoring and advisory activities remain valid.

Compliance Risk Matrix

Rules	Division A		Division B		Division C		Division D		Division E		Rules Total
	Impact	Probability	Impact	Probability	Impact	Probability	Impact	Probability	Impact	Probability	
SYSC 2 senior management arrangements *	8	6	8	6	8	6	8	6	8	6	240
	48		48		48		48		48		
SYSC3 systems and controls *	8	6	8	6	8	6	8	6	8	6	240
	48		48		48		48		48		
SYSC4 General organisational requirements *	8	6	8	6	8	6	8	6	8	6	240
	48		48		48		48		48		
SYSC5 employees and agents	8	6	8	6	8	6	8	6	8	6	240
	48		48		48		48		48		
SYSC6 Compliance, Audit and Fin Crime (incl. KYC)	10	6	10	6	10	6	10	6	10	6	300
	60		60		60		60		60		
SYSC7 Risk	10	6	6	6	10	6	6	6	6	6	228
	60		36		60		36		36		
SYSC8 Outsourcing	10	4	10	4	10	6	10	2	10	2	180
	40		40		60		20		20		
SYSC9 Record keeping	10	7	8	6	8	6	8	6	8	6	262
	70		48		48		48		48		
SYSC10 conflicts of interest (incl. remuneration)	10	6	10	6	6	4	8	6	10	6	252
	60		60		24		48		60		
TCF / Conduct risk	7	6	7	6	6	4	8	6	7	4	184
	42		42		24		48		28		
Best Execution	0	0	0	0	10	6	10	6	0	0	120
	0		0		60		60		0		
Appropriateness	0	0	0	0	6	2	6	2	0	0	24
	0		0		12		12		0		
Dissemination	10	4	10	4	10	4	10	4	0	0	160
	40		40		40		40		0		
Regulatory Reporting	8	3	8	3	8	3	8	3	8	3	107
	11		24		24		24		24		
Business Area Risk Totals	1270		1110		1216		1280		824		

The Monitoring Crimes

- The idiot question!
- Lack of thought – “I’ve always done it this way” or “the last bloke told me to do it this way before he left”
- January, 50 tested, no errors found
- February, 50 tested, no errors found
- March, 50 tested, no errors found
- Lack of direction
- [All process, no outcomes – or vice versa[

Building a Regulator-Proof Programme

- Understand the risk
- Understand the population
- Prove the population
- Devise the test
- Test directionally
- Think of process and outcomes
- Then think outside of the box…

Directional Testing

Assets — Overstatement

Liabilities — Understatement

Capital

Turnover — Understatement

Costs — Overstatement

Profit

Directional Testing

Suggested Approach

Poll 1

- How to design intelligent testing
- Are we an Audit function?
- Think outside the box
- Example: portfolio suitability
- Wealth management clients outline their risk appetite
- You have 100 portfolios – 20 high risk, 50 medium risk, 30 low risk.
- Where would you bias your sample?

Directional Testing

- Directional testing is crucial in order to conduct effective monitoring
- For example: Gifts and Entertainment
- In monitoring gifts and entertainment, where would you look first?

Poll 2

Directional Testing

- You are monitoring AML
- You start with AML risk classification
- Do you bias your sample to low, medium or high risk?

Poll 3

- You then proceed to AML KYC
- Do you bias your sample to low, medium or high risk?

Poll 4

Process and Outcomes Testing

- Process Testing: sometimes referred to as “internal controls testing” or “compliance testing”
- Refers to a test of the internal controls surrounding a process, designed to provide comfort that a key process is working
- For example: checking that supervisory checklists have been completed and signed by relevant supervisors

Process and Outcomes Testing

- Outcomes Testing: sometimes referred to as “substantive testing”
- Refers to a test of the absolute - designed to provide comfort that an outcome has been achieved
- For example: checking against the expenses that no inappropriate hospitality has been provided

Action Points

- Develop or review your compliance risk matrix
- Obtain senior management approval of your approach and the matrix
- [Use the results of your matrix to inform the active elements of your compliance programme]
- Review the matrix at least annually
- Design or review your monitoring programme
- Make it risk-based and directionally appropriate
- Use compliance risk to determine frequency and sample size
- Review your CMP at least annually

Conclusions

- A risk-based approach to compliance monitoring is essential
- As is a systematic approach

Answer the questions:

- “How do you identify and manage compliance risk”
- “How have you put together a risk-based monitoring plan?”
- “Does the monitoring plan employ your resources efficiently whilst targeting the highest risks?”

Questions

Thank you for attending

Any Questions?
peter.haines@peterhaines.co.uk