RISK APPETITE

A Perspective on Sound Practice

Overview of the study

- A multi-phase study spanning 6 months

- 25 participants from global financial institutions

- Focus on practical applications and insights

- Almost all participants had an existing top-level appetite statement and were moving to the next stage of development

Timeline

- Set up *(November 2012)*

- Questionnaire *(December 2012)*

- 1-2-1 interviews *(January 2013)*

- Round Tables *(February 2013)*

- Final Report *(April 2013)*

What did we look at?

ORX members reviewed their current practice and the challenges they faced in applying an operational risk appetite within their firms. Specifically;

- How do you build a sound operational risk appetite statement (ORA)?
- How do you express ORA?
- How and where do you cascade ORA down an organisation?
- How do you integrate and measure ORA within the business?
- How do you make ORA actionable?
- How do you make reporting ORA relevant to the business?

Main conclusion: Operational risk appetite implementation is difficult but worthwhile, given the additional regulatory scrutiny now placed on financial institutions

Why so challenging?

Operational Risk Discipline

- **Measurement** – Op risk lacks a common metric that works across businesses

- **Understanding & Language** – it means different things to different people "…everybody does operational risk…"; but no common language

- **Feedback loop** – capital levels are relatively unresponsive to improvements in the control environment

- **Embedding** – Operational risk frameworks too often remain remote from the business
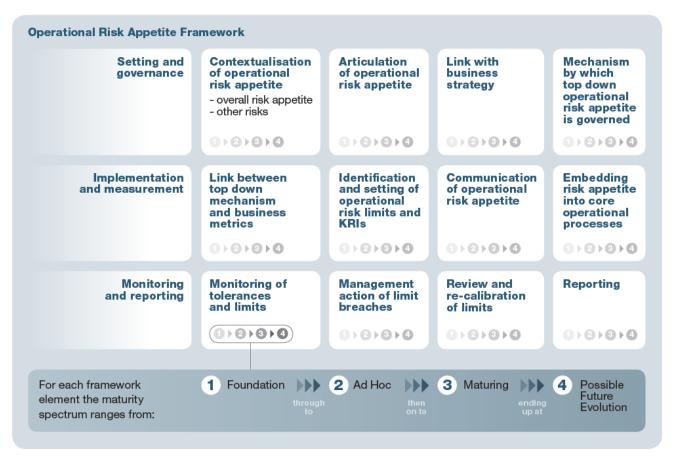
Common Challenges remain

- **Strategy decisions**
  - Op risk still receives only informal consideration
- **How far to Cascade decisions**
  - still varies as to how far measures and limits should be cascaded.
- **Accountability for setting ORA**
  - remains unclear who is responsible; business or operational risk?
- **Embedding activities**
  - Difficulties injecting related data into existing monitoring, reporting and escalation processes

Main Building Blocks for ORA

Sound practice is to use a common language to talk about ORA

- Participants agreed to use a single framework for ORA

- The framework consists of 12 building blocks

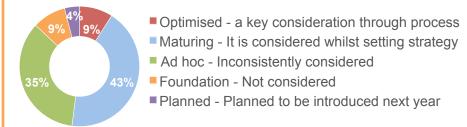- Helped them explore links with overall appetite in relation to other risk types

Operational Risk Appetite Framework

Setting and governance	Contextualisation of operational risk appetite - overall risk appetite - other risks	Articulation of operational risk appetite	Link with business strategy	Mechanism by which top down operational risk appetite is governed
	①▸②▸③▸④	①▸②▸③▸④	①▸②▸③▸④	①▸②▸③▸④
Implementation and measurement	Link between top down mechanism and business metrics	Identification and setting of operational risk limits and KRIs	Communication of operational risk appetite	Embedding risk appetite into core operational processes
	①▸②▸③▸④	①▸②▸③▸④	①▸②▸③▸④	①▸②▸③▸④
Monitoring and reporting	Monitoring of tolerances and limits	Management action of limit breaches	Review and re-calibration of limits	Reporting
	①▸②▸③▸④	①▸②▸③▸④	①▸②▸③▸④	①▸②▸③▸④

For each framework element the maturity spectrum ranges from: **①** Foundation ▶▶▶ through to **②** Ad Hoc ▶▶▶ then on to **③** Maturing ▶▶▶ ending up at **④** Possible Future Evolution
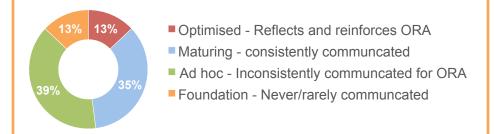
Setting and Governance

Sound practice for assigning ownership and accountability for setting ORA:

- A key role for the business, rather than the risk function

- Operational Risk should play a consultative role with veto powers

- Place the discussion of operational risk in a strategic context – drop op risk jargon

- Ensure you cascade your ORA to the level in your firm that is best positioned to manage the risk

To what extent is top level ORA considered during top level strategy setting?
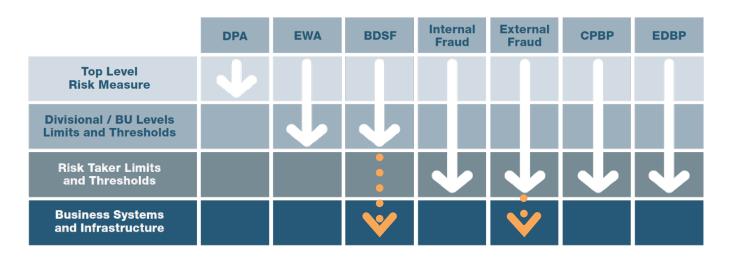

- Optimised - a key consideration through process
- Maturing - It is considered whilst setting strategy
- Ad hoc - Inconsistently considered
- Foundation - Not considered
- Planned - Planned to be introduced next year

To what extent is there effective "Tone at the top" communication for ORA?

- Optimised - Reflects and reinforces ORA
- Maturing - consistently communcated
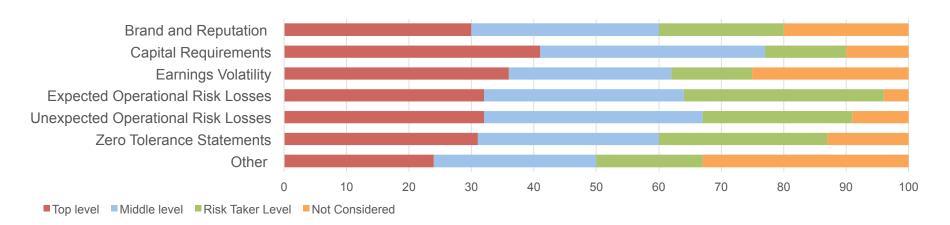- Ad hoc - Inconsistently communcated for ORA
- Foundation - Never/rarely communcated

Setting and Governance

As a general concept; the level to which you cascade ORA is dependent on risk event type

	DPA	EWA	BDSF	Internal Fraud	External Fraud	CPBP	EDBP
Top Level Risk Measure	↓						
Divisional / BU Levels Limits and Thresholds		↓	↓				
Risk Taker Limits and Thresholds			⋮	↓	↓	↓	↓
Business Systems and Infrastructure			↓		↓		

To what level of the organisation is ORA cascaded down through the following considerations?

Legend: ■ Top level ■ Middle level ■ Risk Taker Level ■ Not Considered

Categories (top to bottom): Brand and Reputation, Capital Requirements, Earnings Volatility, Expected Operational Risk Losses, Unexpected Operational Risk Losses, Zero Tolerance Statements, Other
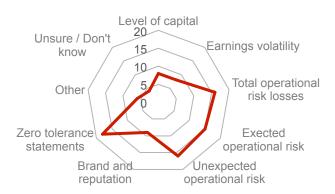
Implementation, Measurement & Monitoring

How is ORA expressed at the middle level of the organisation?

How is ORA expressed to the Risk Takers in the organisation?
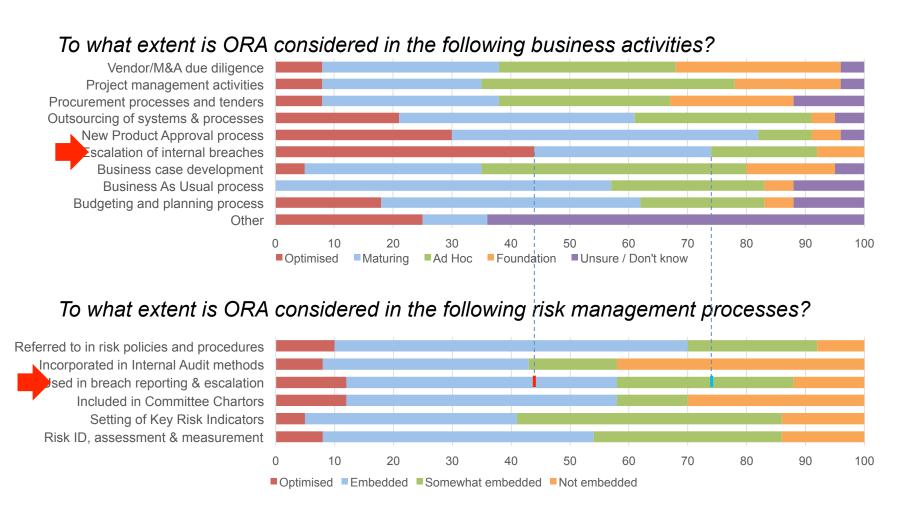

Sound practice for embedding ORA data into escalation and reporting activity

- Underpin and align ORA to a consistent risk taxonomy

- Link measurement of risk to management of risk

- Be wary of using capital metrics due to limited links to BU level KRIs

- Inject related business data into existing monitoring reports

- Leverage what the business does already will help fast-track the design and development of your ORA

Implementation, Measurement & Monitoring

To what extent is ORA considered in the following business activities?

Categories: Optimised, Maturing, Ad Hoc, Foundation, Unsure / Don't know

Business activities: Vendor/M&A due diligence, Project management activities, Procurement processes and tenders, Outsourcing of systems & processes, New Product Approval process, Escalation of internal breaches, Business case development, Business As Usual process, Budgeting and planning process, Other

To what extent is ORA considered in the following risk management processes?

Categories: Optimised, Embedded, Somewhat embedded, Not embedded

Risk management processes: Referred to in risk policies and procedures, Incorporated in Internal Audit methods, Used in breach reporting & escalation, Included in Committee Chartors, Setting of Key Risk Indicators, Risk ID, assessment & measurement
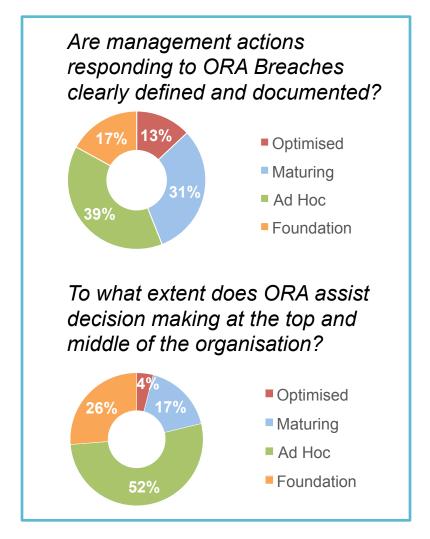
Escalation and Reporting

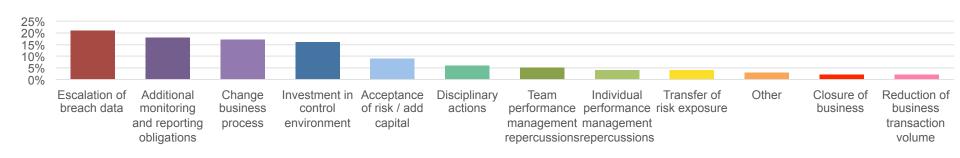Sound practice for embedding ORA data into escalation and reporting activity

- Make the reporting as practical as possible

- Inject related business data into existing monitoring reports

- Gear your ORA framework towards a culture that encourages reporting, rather than focusing on a "error avoidance" culture
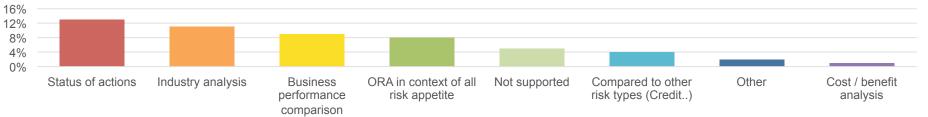
Are management actions responding to ORA Breaches clearly defined and documented?

- Optimised 13%
- Maturing 31%
- Ad Hoc 39%
- Foundation 17%

To what extent does ORA assist decision making at the top and middle of the organisation?

- Optimised 4%
- Maturing 17%
- Ad Hoc 52%
- Foundation 26%

Escalation and Reporting

What are the management activities most typically deployed in response to breaches?

Is Board Risk appetite reporting supplemented with other actions?

Sound practice for accelerating reporting effectiveness:

- Standardise reporting approaches, language, definitions and formats such as dashboards
- Provide more advanced analysis, such as analysis that support cost / benefit discussions
- Additional investments in IT infrastructure to support the OR function's data collection
- Leverage regulatory expectations for internal and external reporting.

Summary of Top 10 sound practices

1. Identify and allocate accountability to the risk takers that manage the risk

2. Underpin and align ORA to a consistent risk taxonomy and align to other risk frameworks

3. Gear your ORA framework to encourage desired behaviours and drive cultural change

4. Capitalise on the regulatory agenda but avoid approaching ORA as a tick-box exercise

5. Avoid operational risk management jargon, instead, place the discussion of operational risk in a strategic context

6. Ensure Operational Risk has a seat at the table at the beginning of the planning process

7. Keep it practical and leverage what the business does already and strive for consistency

8. Make it forward-looking – get creative with KRIs by using them as a management tool

9. Link measurement of risk to management of risk but be wary of using capital

10. Be prepared to make changes as you tailor your ORA framework to your organisation's business priorities and objectives – and update it as your organisation matures