Enhancing Risk Management and Governance in the Region's Banking System to Implement Basel II and to Meet Contemporary Risks and Challenges Arising from the Global Banking System

Training Program ~ 8 – 12 December 2008
SHANGHAI, CHINA

Session 6.4

Australian Banking Perspective on Managing Operational Risk

Mr Bruce Lebransky
National Australia Bank

One of the distinguishing characteristics of the Basel II Framework from Basel I is its separate recognition and explicit measurement of operational risk - although regulators have had longstanding prudential requirements covering operational risk issues such as outsourcing and business continuity management.

<u>(i) The Issue of Regulatory Approval</u>

In Australia, APRA's implementation of the Basel II framework has required that for it to approve use of the IRB approach to credit risk measurement an authorised deposit taking institution (ADI) must also seek approval to use an AMA approach to operational risk plus approval to use an internal model for estimating interest rate risk in the banking book.

This regulatory requirement has contributed to ADIs having a focus on developing similar levels of "sophisticated" risk measurement and management capability and so be less likely to approach risk issues on a differentiated basis including with respect to issues of governance and use & experience. Integrated risk identification and management was highlighted in the Report of the Senior Supervisors Group (March 2008) as a characteristic of those firms dealing more successfully with current market challenges.

Amongst APRA's use and experience requirements for ensuring the integration of operational risk management (ORM) into day to day risk management are that:

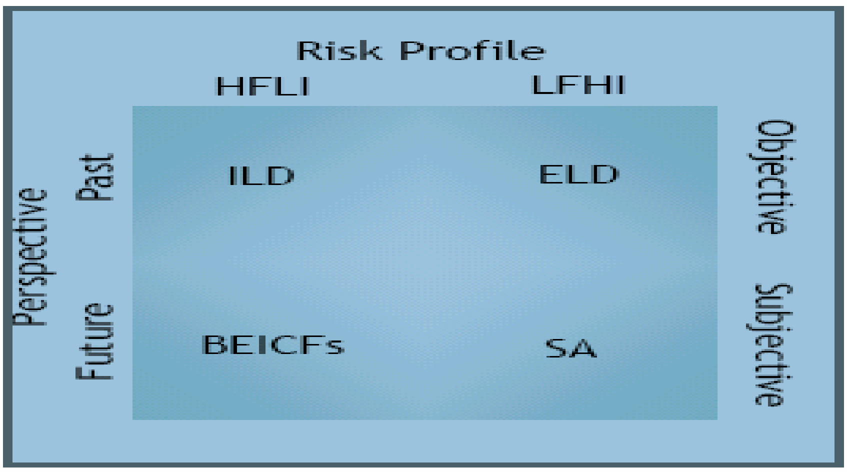
- Management decision making considers both inputs and outputs of the ORM system and can provide evidence of where this has occurred.
- Business unit heads/ staff are able to explain the drivers of their operational risk profile.

<u>(ii) The Characteristics of Operational Risk Data</u>

The process of risk estimation is the essential first step to effective risk management.

All Australian banks with AMA accreditation have included the four data elements identified under the Basel II Accord in their risk measurement approach and the derivation of their aggregate loss distribution.

The following highlights the different characteristics of these data elements:



<u>(iii) Internal Loss Data (ILD)</u>

ILD contributes approximately 50% of NAB's total measurement of operational risk.

At NAB, internal loss events of greater than $10,000 per event are the mandated capture threshold across the group for internal modelling. The largest event-type component categories are the classifications of: "internal fraud" and "execution, delivery and process management".

Senior management and the Board are informed of significant losses through escalation policies. For NAB the reportable events threshold at group level is $500,000 and its foreign currency equivalent throughout the group.

The NAB group event management policy states events must be (initially) captured within 5 working days of the event having been discovered. This is consistent with APRA requirements. Formal data integrity policies require the business unit to record the loss and for management to approve this with the separation of risk management acting to ensure the validity of loss events as recorded.

As data capture has expanded so has the ability to conduct more granular risk analysis particularly in identifying common issues across different business activities and regions. This is clearly helpful to BEICF analysis.

APRA's Prudential Standard *APS115: Capital Adequacy – Advanced Measurement Approaches to Operational Risk*, prescribes a method for the classification of credit and market risk related operational losses within this data collection:

- ➢ Credit related operational losses must be treated as credit risk, with the exception of fraud by parties other than the borrower (e.g. credit card fraud);
- ➢ Market related operational losses must be treated as operational risk.

<u>(iv) External Loss Data (ELD)</u>

External loss data (ELD) contributes to building information on low-frequency – high impact events. It also helps as a reference point for discussions in scenario analysis workshops.

NAB subscribes to external loss data from 3 sources:

- publicly available information (Algo First)
- as a member of a consortium (ORX)
- insurance information (previously from AON-Op base but no longer collected)

There is significant reporting bias in all three sources of ELD for analytical purposes so ELD is more useful for qualitative assessments of risk:

- Public data: the probability that a loss is reported by the media tends to increase with the severity of the loss. Consequently the proportion of large losses tends to be overstated.
- Insurance data: biases will arise from policy terms and conditions.

- Consortium data: the data thresholds used by individual banks may differ from the threshold used by the consortium. Nevertheless NAB considers this data to be increasingly robust as its time of collection has increased and the level of institutional participation has increased.

NAB does not employ a scaling of ELD. It considers there to be limited correlation between the size of an entity and the size of any recorded event. However, entity size is considered to impact the likelihood of an event occurring so that there is important qualitative information with ELD as well as information for better estimating the shape of the distribution tail.

(v) Scenario Analysis

The process for developing scenarios is common across the group. It is a requirement that meaningful challenge processes be incorporated in the scenario construction process.

Different scenarios can and are constructed to reflect regional and business differences. It is a regulatory requirement that documentation be provided on the assumptions used and rationale for this in the making of scenarios in workshops.

(vi) BEICFs – (business environment and internal control factors)

BEICFs are incorporated into the NAB's scenario analysis through qualitative overlay to the operational risk assessment and calculation. The BEICF processes are important learning and decision tools for the business about is operational risks and risk mitigation actions.

- Business Environment factors are the characteristics of a bank's internal and external operating environment that create operational risk exposures.
- Internal Control factors reflect those parts of the bank's internal control system that are used to mitigate these risk exposures.

(vii) Risk Mitigation Recognition in the Calculation of Operational Risk Capital Requirements

At this time APRA does not recognise insurance as a risk mitigation tool. It is possible that this position may alter. NAB has insurance arrangements in place with limits on the permissible size of excesses at both group and subsidiary bank level.

NAB also calculates expected operational risk loss but this too is not recognised for purposes of calculating regulatory operational risk capital.

During the current financial turmoil, NAB has not sought to change its insurance arrangements or experienced material fluctuation to its expected operational risk loss. However there seems to have emerged some reluctance in direct insurance markets to accept higher risk categories of insurance and the bank has sought to obtain more direct access to the re-insurance markets.

(viii) Operational risk tolerances:

These include the following:

- Qualitative tolerance: the tolerance for exposure which without appropriate mitigation has the potential for unacceptable levels of financial loss or damage to reputation.
- Profit and loss tolerance: the maximum tolerance for the P&L impact of operational risk losses each year.
- Insurance self-retention level: the degree to which individual regions are willing to accept the losses arising from insurable operational risk events.
- Economic capital tolerance: the maximum tolerance for operational risk in e-cap terms.
- Financial volatility tolerance: which are expressed in terms of financial outcomes under 1 in 5 year and 1 in 20 year events.

Operational risk is allocated to the subsidiary banks of the group by way of the construction of a separate operational risk model and outcomes for each legal entity - a bottom-up approach.

National Australia Bank

MAFC / APEC / AFDC Shanghai Conference: Session 6.4: Operational Risk

8 – 12 December 2008
Bruce Le Bransky

nab Clydesdale Bank Yorkshire Bank Bank of New Zealand nabCapital MLC

Key points to be covered

- Operational Risk Management is Important
- Operational Risk of Australia's largest banks
- Operational Risk Data Elements
- NAB Operational Risk Measurement
- Operational Risk Framework (ORF)
- Operational Risk Principles at NAB:

  - Business as First Line of Defence
  - Independent Risk Management as Second Line of Defence

- Policy & Standards - NAB's Group Events Management Policy
- Event escalation and reporting to GORS
- BEICF – Establishing Operational Risk Profile
- ORECS – Tool for ILD collection
  Integrity of ILD capture
- Appendix A ORECS - loss data collection system and process
  Appendix B ORECS - risk event capture

Operational Risk Management is Important

- Effective Operational Risk Management Minimises:

  - Financial losses

  - Disruption to business processes

  - Non-financial impacts including regulatory, reputation & customer impacts.

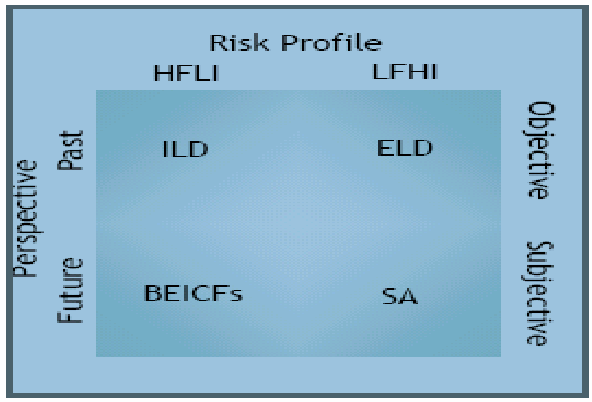
- Not actively sought as with credit or market risk. Inherent part of business and so is “different”.

Operational Risk of Australia’s Largest Banks

Name of Bank	AMA Operational RWA as a % of total reported Pillar 1 RWAs (includes IRRBB)
Westpac	7%
NAB	6.9%
ANZ	6.6%
CBA	6.6%

National Australia Bank

Operational Risk Data Elements



ILD accounts for nearly 50% of NAB's operational risk measurement

SA and ELD comprise the balance. Impacts the risk tail.

BEICFs are inputs into the scenario analysis - reflect current risk profile

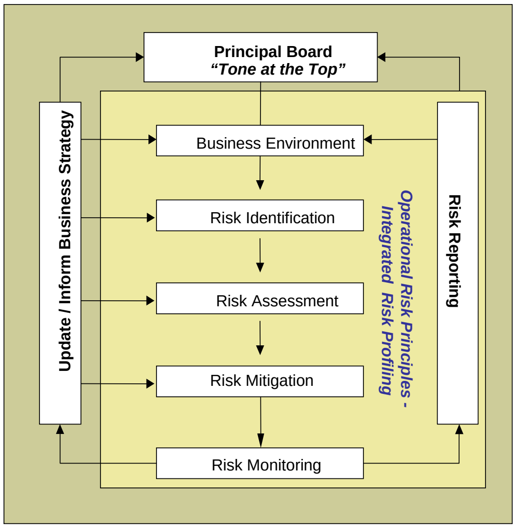
National Australia Bank

NAB Operational Risk Measurement

- AMA regulatory capital calculation is determined separately for each jurisdiction / entity and summed to reach Group level figure.
- Regulatory capital measurement does not include any adjustment for insurance.
- Group determines insurance coverage and limits.
  Regions have input into self-retention / excess decisions.
- Regulatory capital measurement covers both expected and unexpected loss unlike credit risk.

National Australia Bank

Operational Risk Framework (ORF)



- The Operational Risk Framework outlines the principles by which NAB manages operational risk as part of BAU.

Operational Risk Principles at NAB – Business as First Line of Defence

- Accountable for the management of risk – acceptance, avoidance and mitigation.
- Identify and assess business operating environment and risk profile (BEICFs outcomes).
- Responsible for accurate reporting of events and their impacts. Escalate as necessary.
- Accountable for implementation and monitoring of controls. Appropriate training – embed risk management within business.

Operational Risk Principles at NAB – Independent Risk Management as Second Line of Defence

- Group Operational Risk and Security (GORS) –
  Establish & operate the Group Events Management Policy (next slide)
- Design supports for ORF - policies, tools, processes and training. Includes scenario analysis.
- Monitor implementation and review effectiveness. Review event capture, timeliness and completeness.
- Review outcomes for common trends across group
- Review risk mitigation actions of the business
- General Manager part of Group Risk Leadership Team. Risks types are not considered in isolation.

National Australia Bank

Policy & Standards - NAB's Group Events Management Policy

This Policy aims to make NAB Operational Risk Framework effective.

- **Objective** - transparent and verifiable processes for complete and accurate internal event reporting.
- **Timing** – event recording is 5 business days (APRA expectation)
- **Data Collection Threshold** - events with a gross financial impact exceeding $10,000.
- **Reporting Escalation** (next slide)
- **Policy Renewal** - Annual Review
- **Application** - all employees and business lines

National Australia Bank

Event escalation and reporting to GORS

- Covers “reportable” operational risk events:
  - Regulatory impacts:
    significant breach of regulatory compliance obligation
    formal regulatory enquiry / investigation / fine
  - Reputational impacts:
    widespread adverse media coverage
    potential for significant litigation if not adequately addressed
  - Customer impacts:
  - Financial impacts: AUD 500,000 (initial regional escalation threshold is $100,000)

BEICF - Establishing Operational Risk Profile

Business Environment	Objectives – What is the Business Model Products and services offered) Systems) Are changes occurring?
Risk Identification	Risks / uncertainties facing business Event experience and actual trends. Scenarios and extreme event risks
Risk Assessment	Three buckets: Expected, Exceptional, Extreme Assessment of risk mitigation and controls External events and scenarios – potential impact on business Latest internal audit reports – ratings and responses
Risk Mitigation	Identification. Plans for improving control environment. Tolerance for risk acceptance eg excess on insurance coverage. Acceptance of calculated capital – hurdle rates of return.
Risk Reporting	How is this structured: content / frequency / to whom. Escalation

National Australia Bank

ORECS – Tool for internal loss data collection

ORECS provides:

- Detailed description of what happened including process being undertaken
- Risk that materialised
- Controls that failed or were not performed
- Causes
- Cost and impact
- Escalation and notification functions

- Operational risk related credit risk losses also captured.

ORECS - Integrity of internal loss data capture

Requirement - Events identified / captured / approved / verified. Appropriate independence of duties.

- **Business identifier** – Gathers event information and records in ORECS.
- **Business approver** – Review and approve the event within ORECS. Accountable for the completeness and accuracy of the event record. To be completed within 10 days of event being submitted.
- **Operational risk reviewer** – Ensure record is complete, accurate and comparable with other ORECS entries.
- **Operational risk portfolio analyst**

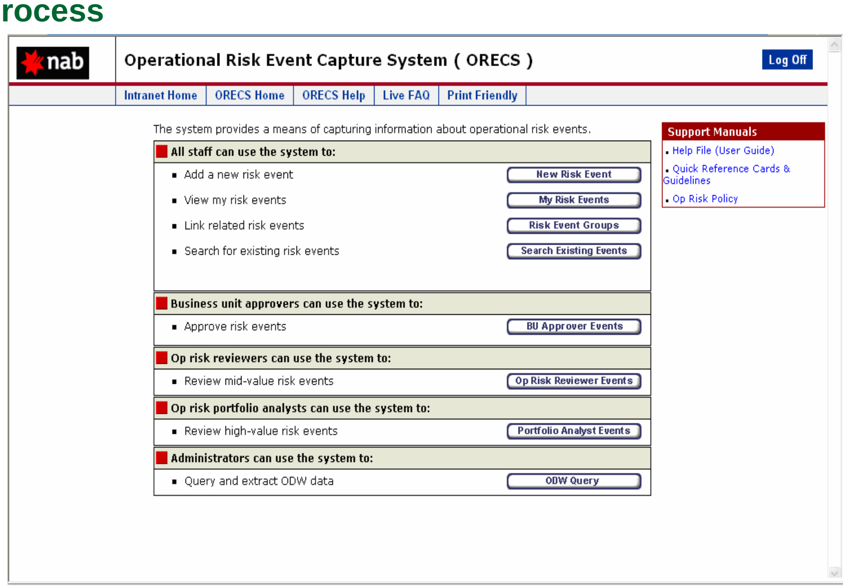
Independence - Risk staff report to the regional head of operational risk. Clear separation of reporting lines and duties from the business.

Key points covered

- Operational Risk Management is Important
- Operational Risk of Australia's largest banks
- Operational Risk Data Elements
- NAB Operational Risk Measurement
- Operational Risk Framework (ORF)
- Operational Risk Principles at NAB:

  - Business as First Line of Defence
  - Independent Risk Management as Second Line of Defence
- Policy & Standards - NAB's Group Events Management Policy
- Event escalation and reporting to GORS
- BEICF – Establishing Operational Risk Profile
- ORECS – Tool for ILD collection
  Integrity of ILD capture

Appendix A: ORECS – Loss Data Collection Systems and Process



Appendix B: ORECS – Risk Event Capture