
The Commonwealth Bank of Australia

Scenario Analysis Workshop

Bank of Japan

18 July 2006

Commonwealth Bank



Commonwealth Bank Of Australia

- The Commonwealth Bank is one of Australia's leading financial institutions with businesses in New Zealand, Asia and the United Kingdom. We are positioned for future growth, and aim to provide accessible banking and financial services for all Australians; fair, safe, challenging and rewarding employment for staff and to reward all shareholders through dividends and capital growth.
- **Profile**
We're one of Australia's leading providers of integrated financial services including retail, premium, business and institutional banking, funds management, superannuation, general and life insurance, broking services and finance company activities.
- **Strategy**
To be Australia's finest financial services organisation through excelling in customer service.
- **Structure**
We combine product development and service delivery with customer segment requirements, bringing us closer to our customers and helping us to meet customers' needs.
- **Our Leaders**
It's our team of leaders who ensure the business works together to support staff and grow the business.
- **Our People**
Our staff are committed to helping our customers manage and build wealth. With more than 35,000 staff, we're one of Australia's largest employers and we support our staff through a range of benefits and services.
- **Funding**
We raise and maintain the Bank's wholesale debt and capital in both the domestic and international capital markets in a cost efficient manner.
- **Facts and figures**
With over 130,000 distribution points across the country and businesses overseas, we're a diverse organisation with a long history in the Australian banking industry.
- **History**
The Commonwealth Bank was founded under the Commonwealth Bank Act in 1911 and commenced operations in 1912. The Bank was empowered to conduct both savings and general banking business. Today, we've grown to a business with over 700,000 shareholders, offering a full range of financial services to help every Australian build and manage wealth.



Agenda

- Operational Risk Framework

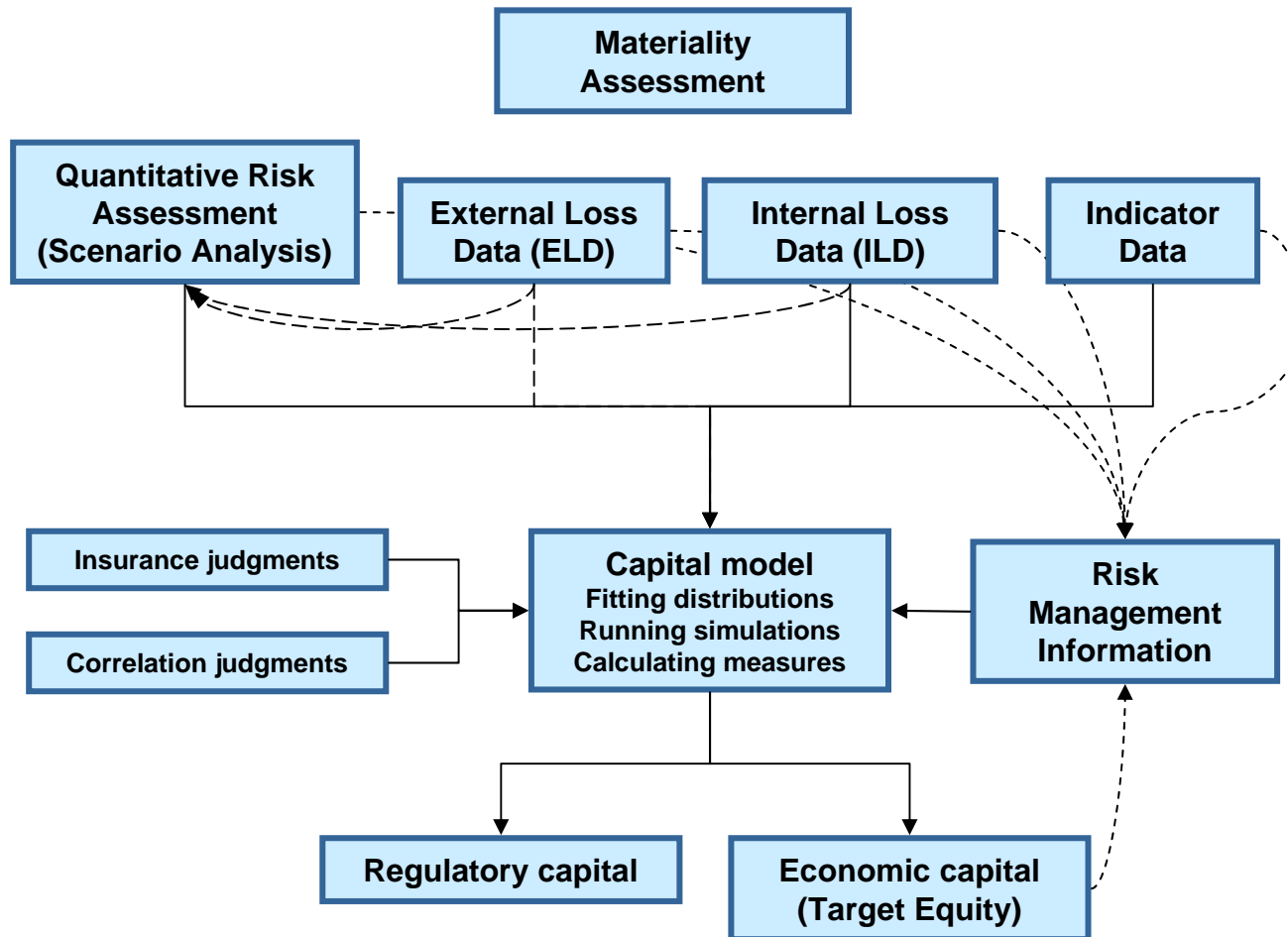
- Scenario Analysis – Quantitative Risk Assessments (QRA)
 - Advantages and Challenges
 - Preparation, Assessment & Validation
 - A practical example
- Technical Issues
 - QRA Exposure Aggregation
 - Portfolio Review Metrics



The Bank's Operational Risk & Control Process



Operational Risk – AMA Data Flows



AMA Granularity

The Bank applies a Business / Risk Type (“BuRT”) level dimension to Materiality Assessment; Scenario Analysis and Internal Loss Data collection

The Risk Type hierarchy is aligned to Basel II risk hierarchy

The Business hierarchy is based on 60 business divisions with the Bank’s Business Units:

- Premium Business Services
- Retail Banking Services
- Wealth Management
- International Financial Services (including ASB)
- Enterprise IT
- Finance & Risk Management
- People Services
- Office of the CEO



Level 1 Risk Type	Level 2 Risk Type
Personnel Malpractice	Unauthorised Activity
	Theft & Fraud
External Fraud	Theft & Fraud
	Systems Security
Employment Practices & workplace Safety	Employee Relations
	Diversity & Discrimination
	Safe Environment
Damage to Physical Assets	Disasters and Other Events
Business Disruption & Systems Failure	Systems/ IT Infrastructure Failure
Execution Delivery and Process Management	Transaction Capture, Execution and Maintenance
	Monitoring & Reporting
	Customer/client intake and Documentation
	Customer/client Account Management
	Trade Counterparties
	Vendors & Suppliers
Clients, Products and business Practices	Suitability, Disclosure and Fiduciary
	Improper Business or Market Practices
	Product Flaws
	Client Selection, Sponsorship and Exposure
	Advisory Activities



Agenda

- Operational Risk Framework

- Scenario Modelling – Quantitative Risk Assessments (QRA)

- Advantages and Challenges
- Preparation, Assessment & Validation
- A practical example

- Technical Issues

- QRA Exposure Aggregation
- Portfolio Review Metrics



Scenario Analysis (QRA) – Advantages & Challenges

Advantages

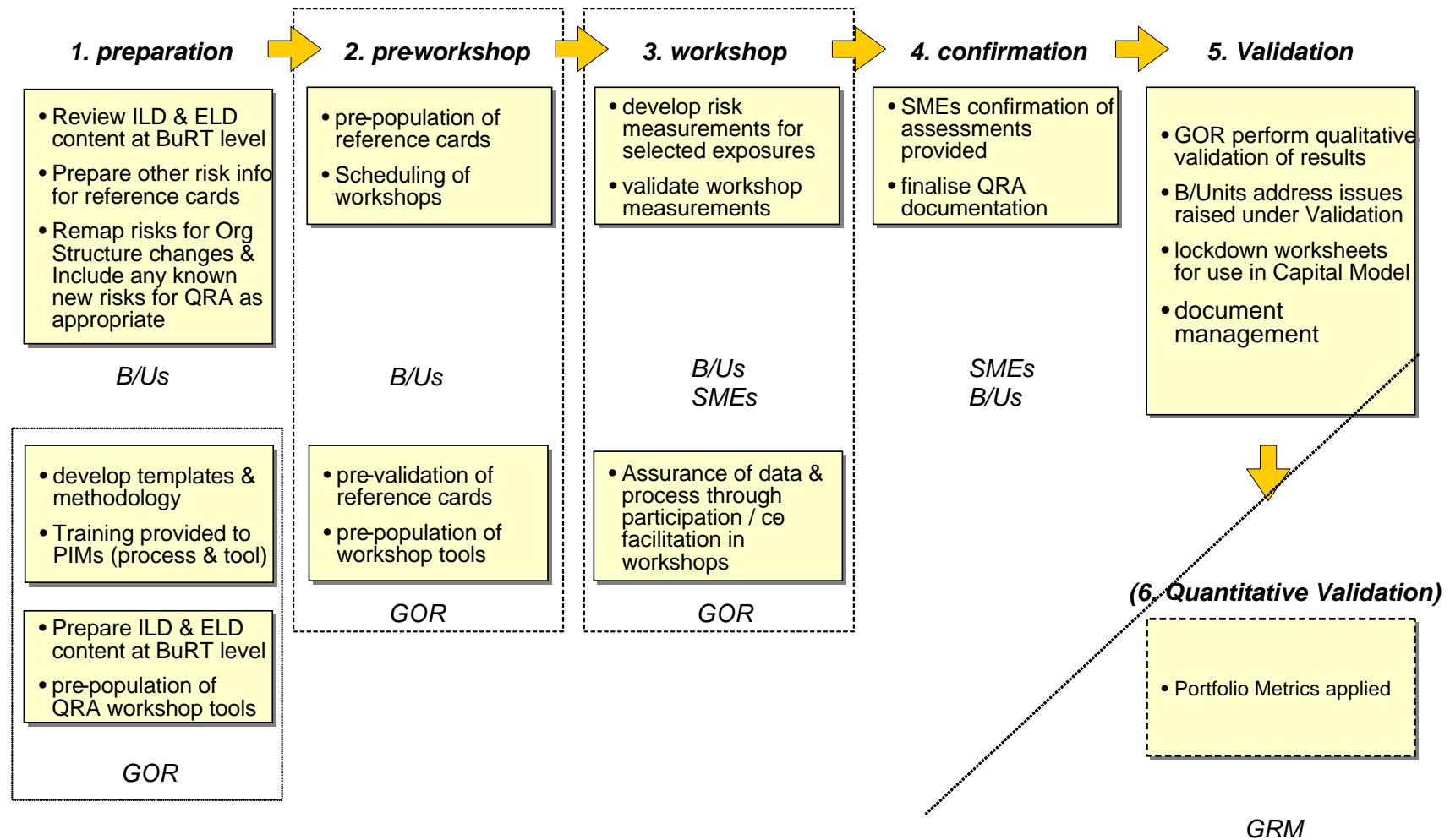
- **Granularity**
 - improves relevance to the business
 - provides structured thinking
- **Engagement**
 - A business discussion as much as a risk discussion
 - uses the language the business understands
 - Impact and frequency assessment playback
- **Completeness**
 - all relevant risk information used
 - Understanding risk drivers and refresh triggers

Challenges

- **Data availability**
 - availability and relevance of ILD & ELD
- **Consistency & Relativities**
 - Consistency in workshop delivery
 - Relativities in assessments
 - Write-up consistency
- **Keeping it simple**
 - Getting the right business representative
 - Keeping modelling discussions simple



QRA Process - Overview



Preparation: Collecting Risk Information

Previous QRA



Current Divisional Risk Profile

Risk Type – Level 1	Risk Type – Level 2	Potential Loss	Rating / trend (June 2006)	How are we performing?
Personnel malpractice	Unauthorised Activity	Low	G →	ILD – More / less incidents Control Weaknesses from Internal Losses, Audit, Controls Assurance, SOX, KRIs etc
	Theft & fraud	Medium	A ↑	ILD – More / less incidents Control Weaknesses from Internal Losses, Audit, Controls Assurance, SOX, KRIs etc
External fraud	Theft & fraud	Low	R ↓	ILD – More / less incidents Control Weaknesses from Internal Losses, Audit, Controls Assurance, SOX, KRIs etc
	System security	-	-	Not Applicable

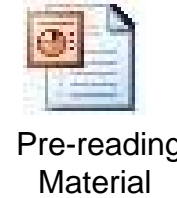
Review existing risk information contained in current risk profile. Is the profile 'current' or does it need to be updated (incrementally) for **new** risk data (i.e. ILD, Control Weaknesses from KRIs, Audit Issues, Compliance Issues, CSA/CAP or SOX testing etc) ?

External Loss Data



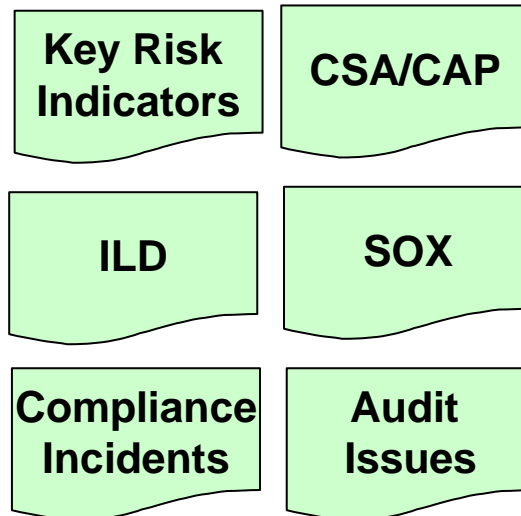
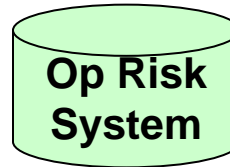
Review any ELD from last QRA. Review for any new ELD data points that are relevant to this BuRT ?

New Pre-reading Material



Preparation: Risk Information Sources

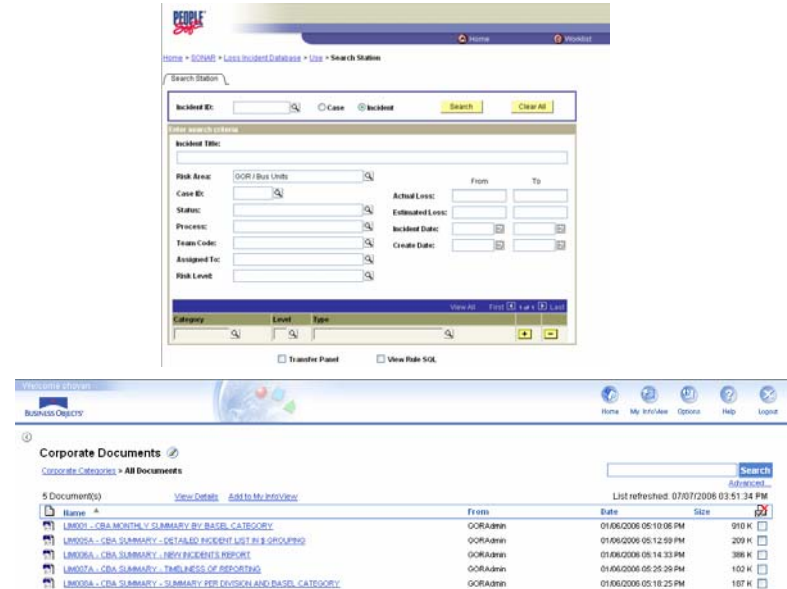
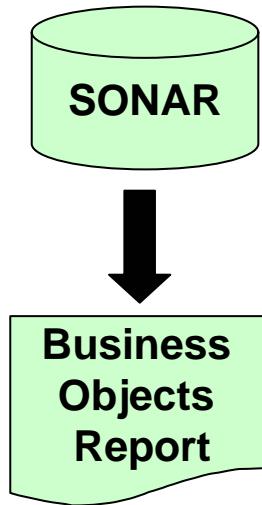
- Previous QRA assessment documentation
- Divisional Risk Profile



Risk Type – Level 1	Risk Type – Level 2	Potential Loss	Rating / trend (June 2006)	How are we performing?
Personnel malpractice	Unauthorised Activity	Low	G →	ILD – More / less incidents Control Weaknesses from Internal Losses, Audit, Controls Assurance, SOX, KRIs etc
	Theft & fraud	Medium	A ↑	ILD – More / less incidents Control Weaknesses from Internal Losses, Audit, Controls Assurance, SOX, KRIs etc
External fraud	Theft & fraud	Low	R ↓	ILD – More / less incidents Control Weaknesses from Internal Losses, Audit, Controls Assurance, SOX, KRIs etc
	System security	-	-	Not Applicable

Preparation: Risk Information Sources

- Internal Loss Data (ILD)



- External Loss data (ELD)



QRA – Assessment Workshop

Who's typically in a workshop

- Subject Matter / Business Experts (SMEs) with an appropriate level of experience in the business area and understanding of the risk type/ exposures
- Subject Matter / Business Experts from relevant Group Support function (e.g. from Technology Services in the case of Systems/IT Infrastructure Failure workshop)
- Business Unit Facilitator – cover all businesses within that Business Unit
- Independent Co-facilitator from Group Operational Risk

The key focus of the Workshop is based on:

Assessment of 'Frequency'

- How often do loss events occur

Assessment of 'Impact'

- How big are the losses when they do occur
 - what is the most likely impact (after controls and pre-insurance)
 - what would be the impact of the worst out of 10 loss incidents



QRA Assessment Workshop - Key Questions & Playbacks

Q2 Do you expect one or more loss events for this exposure each year?

Yes

Assessment should reflect the current risk and control environment. Anticipated changes should be captured via indicators, or via a refreshed QRA once the impact of the changes has been determined.

FREQUENCY - HOW OFTEN DO LOSS EVENTS OCCUR

Q3 What is the most likely number of loss events in a year? **50**

Q4 The following is a table and graph of predicted loss event frequencies based on your above judgement. Click on the buttons below or adjust your judgement above to best reflect your judgement.

Periods of 1 year	Events per period
	39
	43
	45
	47
	49
	51
	53
	55
	57
	62

This represents a sample of frequencies for this exposure over 10 Periods of 1 year

Buttons:

IMPACT - HOW BIG ARE THE LOSSES WHEN THEY DO OCCUR (in \$'000s)

Loss includes all direct losses and also identifiable impacts on margin/business volumes, but excludes cost of control improvements, ongoing recurring margin/business volume impacts beyond one year, and generalised reputational impacts on the bank as a whole.

Q5 When a loss incident does occur, what is the most likely impact (after controls, pre insurance)? **(in \$'000s)**
40

Q6 What would you judge to be the impact of the worst out of 10 loss incidents? (This does not represent the maximum loss that can occur for this exposure) **164**

Q7 The following is a table and graph of predicted loss impacts based on your above judgements. Click on the buttons below or adjust your judgements above to best reflect your judgement.

Impact per Incident
12
26
39
51
64
78
95
115
143
197

This represents impacts for a sample of 10 loss incidents for this exposure

Buttons:

Based on these judgments, there is a **74%** likelihood of losing more than **\$40**, a **5%** likelihood of losing more than **\$80**, and a **0%** likelihood of losing more than **\$200**.

There is a likelihood of losing more than **\$83**.

The calculated average loss impact is **\$83**.

likelihood of losing more than **\$40** **\$80** **\$200** **\$400**

QRA – Approach to Validation

How is the validation performed

- Independent role performed by Group Operational Risk function ahead of assessment data being cleared for use by Capital Model Team
- Group Operational Risk also play a co-facilitation role in the Workshops and provide a weekly delivery forum meeting to share & discuss ideas/issues/concerns and program progress

What do we look for in validation

The basic principles established to support the effective validation process are:

- Appropriate pre-reading material was provided to stakeholder (SME) participants
- Confirm appropriate stakeholder participation and involvement
- Validate use of available information
- Document all judgements and discussions
- Confirmation of Assessments by SMEs
- Follow a consistent process
- Support periodic review of the measurement processes



QRA – Approach to Validation

Key Areas of Validation focus:

- Application of the Risk Information provided in the pre-reading material
- Workshop Write-up document provides sufficient insight and description of the rationale for the assessments to satisfy a removed party and to facilitate future use
- Reasonableness of assessments for Frequency and Impact based on the Risk Information provided in the pre-reading materials
- Accuracy and completeness of information provided

The Validation process is qualitative – and based on reviewing the individual exposures within a given BuRT. In this regard it is a forerunner to a more quantitative review based on a series of portfolio metrics (*refer later discussion on this point*).

It is anticipated that standardisation of some scenarios & parameters in the industry over the next 2-4 years will provide further benchmarking metrics which will further strengthen the overall validation process.



Agenda

- Operational Risk Framework
- Scenario Modelling – Quantitative Risk Assessments
 - Advantages and Challenges
 - Preparation, Assessment & Validation
 - A practical example

- Technical Issues
 - QRA Exposure Aggregation
 - Portfolio Review Metrics



Technical Issues – Scenario Analysis

- The Bank’s modelling approach is very granular – with some 85 businesses each considered against the 20 Basel risk types. This is driven both to model risk and the tail event potential accurately and to link closely with where the business manages their risk.
- To continue this and capture the best business judgments in the QRA process the Bank allows businesses to assess their key risks risk at the exposure level with separate frequency and severity judgements.
- These exposure level judgements are simulated to provide an annual loss distribution for the exposure that is shown to the business subject matter experts to ensure we have captured their judgements appropriately. These exposure annual loss distributions are aggregated to the Business / Risk Type (“BuRT”) level, resulting in an annual loss distribution for the BuRT.
- However separate frequency & severity distributions are required at the BuRT levels to:
 - Combine with other information sources (eg. ILD)
 - Model insurance mitigation
 - Incorporate frequency or severity dependence modelling
- Challenge: How to “convert” the BuRT annual loss distribution to “equivalent” frequency and severity distributions?



Technical Issues – Scenario Analysis

- Approach:
 - Calculate characteristics (e.g. variance) of BuRT annual loss distribution
 - Calculate parameters using the Method of Moments technique for all possible frequency (Poisson, Binomial and Negative Binomial) and severity distribution (Lognormal, Weibull and Gamma) pairs
 - For each distribution pair that returns valid parameters, simulate the annual loss distribution
 - Use a statistical based business rule to determine the best fit distribution pair



Technical Issues – Portfolio Review Metrics

- Assessment approach is bottom-up or granular
- We use tailored top-down checkpoints on the portfolio
- Four established Portfolio Review Metrics:
 1. Existence of Internal Loss Data vs Materiality Assessment judgment
 2. Bank Operational Risk Regulatory Capital vs Basel Standardised Measure
 3. Business Unit OR Regulatory Capital vs Basel Standardised Measure
 4. Modelled Expected Loss vs Budgeted Loss (for relevant businesses)
- There are defined processes for responding to issues raised by these comparisons
- The Bank is also working on three additional Portfolio Review Metrics for diagnostic purposes:
 5. Scenario Analysis Expected Loss vs Average Internal Loss Data
 6. Scenario Analysis Unexpected Loss % by Risk Type vs External Loss Data (Fitch)
 7. Tail Ratio (UL/EL) for particular risks vs same ratio for peer banks
- Also interested in other benchmarking initiatives



Questions & Contact Details

- **Questions**

- **Contact Details**

- Denis Taylor, General Manager, Group Operational Risk, denis.taylor@cba.com.au
- Mark Shelton, Executive Manager, Operational Risk Solutions, sheltoma@cba.com.au
- David Farmer, Capital Modelling Team Leader, Basel II Operational Risk Project, david.farmer@cba.com.au



Abbreviations used in the presentation:

- QRA: Quantitative Risk Assessment – scenario analysis process used across the Bank
- ILD: Internal Loss Data
- ELD: External Loss Data
- CSA/CAP: Controls Assurance program (qualitative risk and control assessment looking at inherent and residual risk)
- SME: Subject Matter Expert or business expert
- BuRT: Business / Risk Type level,
- B/U: Business &Unit
- GOR: Group Operational Risk
- GRM: Group Risk Management
- SONAR: The Bank's Loss Incident Management system of record (for capturing ILD)
- First Database: External loss event database records sourced from Fitch

