# Risk Drivers and Controls Approaches:
## *Linking Operational Risk Measurement and Management*

**Risk Management Group's Conference on**
***Leading Edge Issues in Operational Risk Measurement***
**Federal Reserve Bank of New York**

**New York, 29 May 2003**

**Presentation by Scorecard Working Group**

# Risk Drivers and Controls Approaches:
## *Linking Operational Risk Measurement and Management*

## ***Agenda***

- Objective
- Definition: "Risk Drivers and Controls Approaches" (RDCAs)
- Key Features of RDCAs
- Examples from an RDCA Questionnaire
- Role of Internal and External data in RDCAs
- Determining Initial Operational Risk Capital
- Ongoing Capital Distribution in an RDCA
- Key Development Considerations for RDCAs
- Validation of RDC Approaches
- Lessons Learned

# Risk Drivers and Controls Approaches

## ***Working Group Participants:***

- *Chairman:* Mark Lawrence, Group Chief Risk Officer, Australia and New Zealand Banking Group
- Marie Gaudioso, Head of Operational Risk, Bank of New York
- Phil Severs, Head of Information Risk Management, Halifax Bank of Scotland
- John Mulgrew, Head of Operational Risk, Mellon Bank

*** The views expressed in this presentation do not necessarily reflect the overall view of each participating institution.**

# Objective

**To develop an operational risk measurement methodology which:**

- Directly connects risk measurement with the operational risk management process;
- Provides increased understanding and transparency of operational risk exposures;
- Provides a 'road map' for reducing risk; and
- Provides transparent incentives for banks to invest in internal controls.

# ***Definition:*** **Risk Drivers and Controls Approaches**

A "*Scorecard" methodology* refers to a class of diverse approaches to operational risk measurement and capital determination which all have at their core an assessment of specific operational risk drivers and controls.

These can also be called "**Risk Drivers and Controls Approaches**", or "**RDCAs**".

Such approaches are effectively expert systems, which assess:

- *the level of a bank's exposure to specified drivers of risk, and*
- *the scope and quality of a bank's internal control environment, key operational processes and risk mitigants,*

and directly link these assessments to risk capital.

- RDCAs should not be confused with dashboards, checklists or reports!!

# Key Features of RDCAs (I)

## Questionnaire-Based

- An RDC Approach incorporates the use of a questionnaire which consists of a series of weighted, risk-based questions. The questions are designed to focus on the principal drivers and controls of operational risk across a broad range of applicable operational risk categories, which may vary across banks.
- The questionnaire is designed to closely reflect the organization's unique operational risk profile by:
  - *designing organization-specific questions that probe for information about the level of material risk drivers and quality of controls;*
  - *calibrating possible responses through a range of "unacceptable" through "effective" to "leading practice";*
  - *applying customized question weightings and response scores aligned with the relative importance of individual risks to the organization. These can vary significantly between banks (due to business mix differences) and may also be customized along business lines within an organization. Note that scoring of response options will often not be linear.*
- The specific risk categories, customized suite of questions and weightings, and scored response options provide business managers with transparent priorities for risk management improvements.

# Examples from an RDCA Questionnaire

**The questionnaire is comprised of questions that that probe for information on the level of risk drivers and quality of controls within each risk category.**

Each business unit will use a questionnaire (customized in some cases) to self-assess its risk for a particular category

**Internal Fraud Questionnaire (sample)**

| | | Not Applicable | Unknown |
|---|---|---|---|
| • *What percentage of your Line of Business' FTEs are temporary employees or contract employees?* | 15% | ☐ | ☐ |
| • *Performance based remuneration (% total salary) - in the last year* | 20% | ☐ | ☐ |
| • *Non-management/ clerical overtime hours worked (% total hours) - in the last year* | 5% | ☐ | ☐ |

- *Degree of autonomy of majority of staff*
  - *Very High: Independent operation, off-site (e.g. mobile sales force)* ○
  - *High: Independent operation, on-site* ○
  - *Moderate: Close team-based working groups* ○
  - *Low: Flat management, close supervision* ○
  - *Very Low: Strong hierarchical management, very close supervision* ○

Questions are focussed on obtaining information about drivers and controls

The questions that are asked will prompt each business unit to think about its management of operational risks

Questions can be a variety of types using objective criteria to assess the level of risk drivers and the quality of controls. Answers can be quantitative or qualitative.

# Examples from an RDCA Questionnaire (cont.)

## The questions can be far more complex to deliver more exacting information:

### Internal Fraud Questionnaire (sample)

**Control Objectives: Physical security measures should be in place to prevent the theft/destruction of assets (e.g. negotiable instruments, PCs and other hardware, valuable documents, client/proprietary information etc.), as a result of inappropriate access by unauthorized individuals.**

**Best Practices: These should restrict and monitor access to premises and sensitive areas (e.g. data centers, workstations, vaults, storage areas for client/proprietary information, etc.).**

**These include:**

- **Sophisticated identification devices, (e.g. biometric identifiers, smart cards, etc.).**
- **General access controls, (e.g. security guards, surveillance rooms with video monitors, cameras, passwords, id cards, etc.) as a second layer of restriction.**
- **Access granted, changes made and security breach reports are formally approved and monitored by management the same day.**

**Mitigant Question**
**For your business, how do you accomplish the above objective to ensure adequate physical security measures are in place?**

| | Value | Weight | Score |
|---|---|---|---|
| • **Physical security measures restricting access to all premises and sensitive areas include all of the above attributes. The process is subject to independent review on an annual basis and a formal ongoing monitoring process of action plans is in place** | 1 | 0.15 | 0.15 |
| • **Physical security measures restricting access to all premises and sensitive areas include most of the above attributes. Management formally approves and monitors most access granted, changes and security breaches are approved and reviewed the same day. The process is subject to independent review on an annual basis and a formal ongoing monitoring process of action plans is in place** | 2 | 0.15 | |
| • **Some sophisticated identification devices and general access controls restrict all access to premises and sensitive areas. Management informally approves and monitors the majority of access granted, changes and security breaches are approved and reviewed less than daily. The process is subject to independent review on an annual basis and an informal monitoring process of action plans is in place** | 3 | 0.15 | |
| • **All access to premises and sensitive areas is restricted by the use of some general access controls. Management informally approves and monitors some access granted, changes and security breaches are approved and reviewed less than daily. The process is subject to independent review more than annually, and an informal monitoring process of action plans is in place** | 5 | 0.15 | |
| • **Physical security measures restricting access to all premises and sensitive areas include some general access controls. Management informally approves and monitors access granted. The process is subject to review on an ad-hoc basis** | 8 | 0.15 | |

# Key Features of RDCAs (II)

## Business Line Involvement

- RDCAs leverage the collective operational risk knowledge of the organization taken from the business units, key risk specialists and audit functions in their development and design.
- Business line involvement in the development of the RDCA framework underpins their ownership of the results.

## Forward-looking

- RDCAs attract capital when vulnerabilities & weaknesses are identified, i.e. when the probability of loss is high, not *after* a material loss, when as a result of management action (strengthening of controls) the probability of loss is likely to be greatly reduced.
- RDCAs provide an evaluation of the level of each business unit's risk drivers and the effectiveness of their controls in detecting and mitigating the material risks. This evaluation serves as an effective proxy for future risk.

## Behavioral Incentives for Improved Risk Management

- An RDCA's direct linkage to capital and management performance provides strong incentives throughout the bank for risk management improvements, focusing business unit effort and investment on improving risk mitigation and internal controls.

# Key Features of RDCAs (III)

## Transparency

- All risk assessments are explicit and transparent, especially to line managers, and are regularly subjected to managerial, audit and/or supervisory interrogation.
- The linkage to capital is formula-driven, transparent and risk sensitive, reflecting risk profile changes as manifested in the question responses.

## Responsive to change

- The real power in RDCAs lies in their ability to respond easily to changes in the risk profile resulting from changes to the business mix or new operational risks.
- In particular, RDCAs elicit and identify new risks resulting from changes in the institution or its core processes, and easily accommodate new operational risks as these arise, before losses are experienced (e.g. Information Technology Security risks), as specific questions can easily be added or adapted.

## Fully Integrated into the Operational Risk Management Process

- By their design, RDCA methodologies are fully aligned with the organization's operational risk management framework, thus directly linking the measurement and management of operational risk.

# Role of Internal and External Data in RDCAs

## Uses of Historical Internal and External Operational Data:

- Such data may be used in the process of determining the initial level of operational risk capital, depending upon the method used.
- Identifying the principal drivers and mitigants of risk for each operational risk category, thereby informing the development of specific questions and response options.
  - Internal events – evaluate past experience and lessons learned from prior control failures and near misses etc. (whether or not losses were sustained).
  - External losses – evaluate the causal factors contributing to other bank losses (where these are known) and assess vs. internal controls within the bank.
- Generating operational risk scenarios for high impact events.

## Uses of Future Internal/External Operational Data

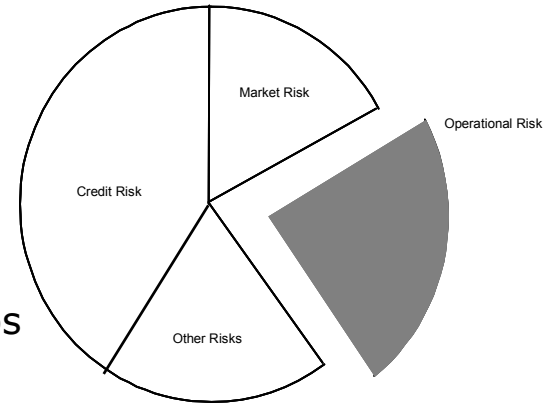
- Future *internal* operational data (including loss data) may be used to:
  - Cross-check the accuracy of questionnaire responses
  - Ensure completeness of the scope of material risks assessed
- Future *external* loss data provides an ongoing source of potential new or emerging risk drivers and scenarios.

# Determining Initial Operational Risk Capital

- **A variety of approaches should be used and compared for the purpose of determining an appropriate initial operational risk capital level**

Methods include:

- Benchmarking proportions of total capital (e.g. 20%),
- Benchmarking vs. other peer institutions,
- Benchmarking vs. capital for other risk types (internal),
- Loss Distribution Approach (LDA) at the bank level,
- Explicit consideration of low frequency, high severity loss scenarios
- Standardised Approach




- **The risk profile of the institution and its rate of change should influence the choice of the methods used.**

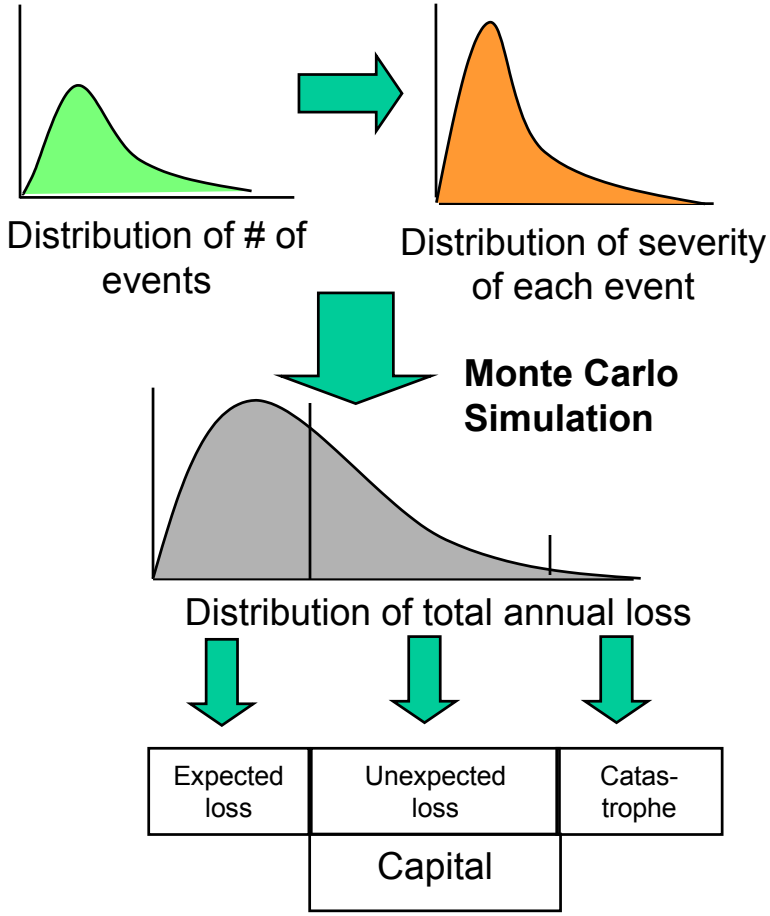
***Key Point :*** ***An aggregate Operational Risk capital level cannot be determined purely objectively.***

- **An essential prerequisite for such an Operational Risk capital level to be "right" for a particular Financial Institution is that it must be accepted and used by the Executive Management of that Financial Institution. This is an appropriate Executive accountability.**

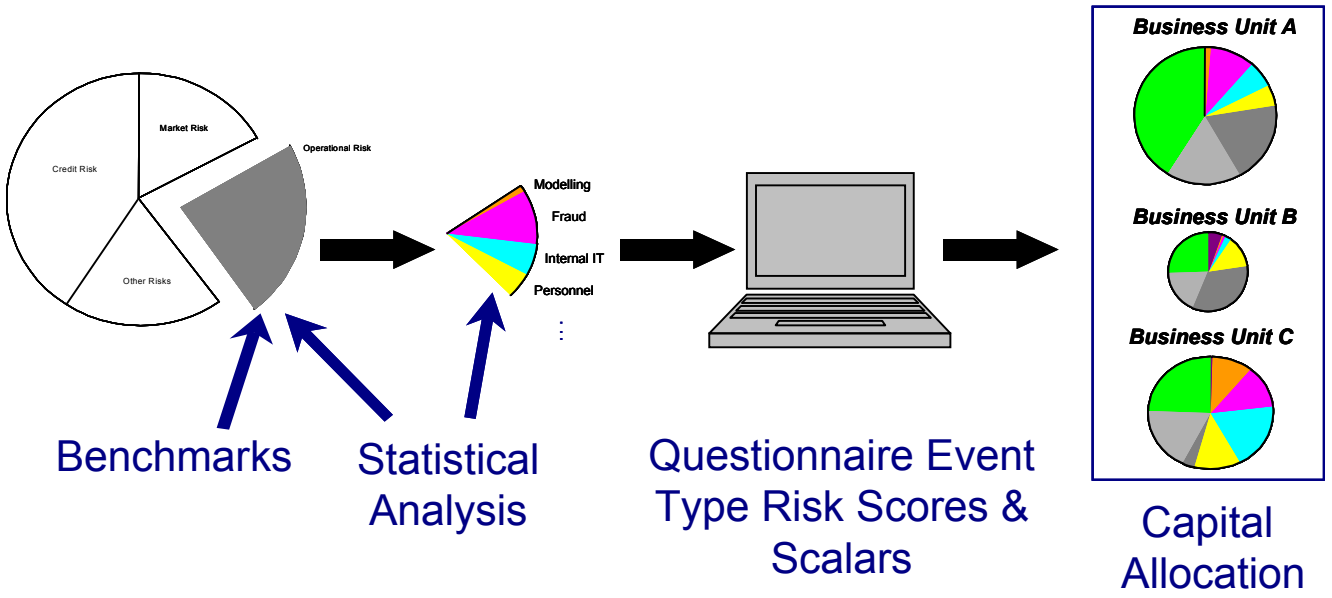
# Determining Initial Operational Risk Capital

## LDA Example: Losses are simulated by combining the likelihood and the severity of independent events

- This method uses internal and external loss data to set parameters for loss frequency and severity distributions.
- At each iteration of the Monte Carlo Simulation, one randomly generates the combination of loss events using the frequency distributions.
- The severity of each selected loss event is simulated using the applicable severity distribution.
- The total annual loss is the sum of the simulated losses.
- Many iterations of the simulation are performed to approximate the total annual loss distribution.
- After extracting expected loss and the largest annual loss anticipated at a given confidence level, the capital figure is determined.



# Initial Capital Distribution in an RDCA (Example)

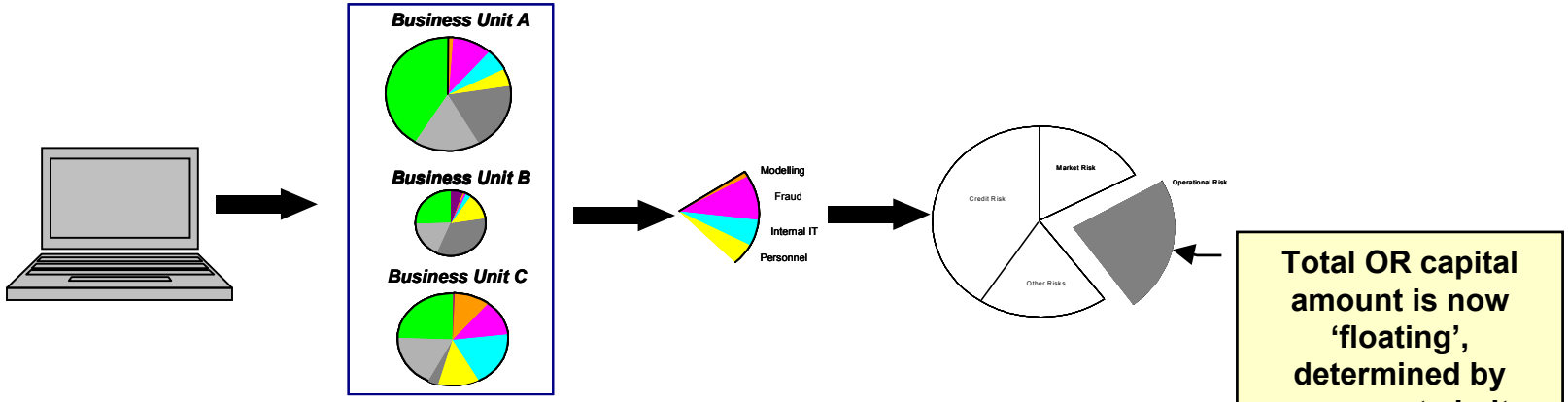



- Following establishment of an initial operational risk capital pool, this pool is proportionally allocated to the risk categories by a process which takes into consideration both historical operational data and the qualitative information from the risk drivers and controls from the RDCA questionnaire to form a forward looking view. The Executive Committee should endorse this allocation.
- Within each risk category, for each Business, the RDCA questionnaire assesses both the risk profile and the appropriate risk scalars for that risk. The combination of these elements form the basis for the downward distribution of capital to the individual business level.
- This initial distribution is a "top-down" process.



Refer Appendix C - worked example

# Ongoing Capital Distribution in an RDCA
## (Example Continued)




*Questionnaire:*
? Event -Type Risk Scores for each BU

? Capital Allocations for each BU

Risk Category Aggregations

Overall Capital Allocation

**Total OR capital amount is now 'floating', determined by movements in its component parts in a 'bottom up' manner**

- For each operational risk category, the new capital allocation for each Business Unit is determined as a direct result to changes in the corresponding *risk scores and scalars* for that unit. **This is the source of the direct behavioural incentive for line managers to reduce operational risk**
- For each Business Unit, the new total operational risk capital amount is the sum of the (changed) amount for each operational risk category, and the new operational risk capital level for the bank is the sum of the capital amount for each Business Unit. **Subsequent to the initial allocations, all ongoing distributions are therefore calculated on a "bottom-up" basis.**
- As a result, the total operational risk capital level for the bank (and the mix between risk categories) will change over time, driven by the changes in every Business Unit (just as for credit risk).



Refer Appendix C - worked example

# Key Development Considerations for RDCAs (I)

## Strategic support

- Engage and retain Executive support throughout the design process

## Design of capital determination/allocation methodology

- Decide definitions of precise operational risk categories to suit the organization
- Determine the organization's primary risk drivers in each category
- Create appropriate questions to assess the level of risk and quality of controls for each risk category:
  - Generic questionnaires and weightings, or customized by business line?
  - Evaluate causal factors which have contributed to previous operational failures, control breakdowns, or "near misses"
- Weight the questions using expert judgment informed by all available operational risk data and experience at your disposable
- Assign numerical values to the response alternatives, to be reflective of acceptable and unacceptable control outcomes
- Decide how to most effectively capture and reflect scale relationships in the model
- Integrate Key Risk Indicators within the model

# Key Development Considerations for RDCAs (II)

## Process implementation issues

- Leverage specialist operational risk expertise in the businesses within the methodology development process
- Source and integrate external specialist risk expertise, as needed
- Determine appropriate IT infrastructure to support the RDCA framework and execution

## Creating behavioral linkage and influence

- Establish a direct linkage between capital charges and management performance
  - *Example:* employ economic capital for operational risk in a RAROC or "Economic Value Added" (EVA) calculation, and use RAROC/EVA in risk-adjusted performance measurement

## Independent review

- Ensure the integrity of questionnaire responses
  - Consider the role of internal audit and other independent risk disciplines in the response validation process

# Validation of RDC Approaches

## Objective: Test the outputs of the RDCA model for reasonableness

### General considerations:

- Validation techniques should be tailored to the particular Advanced Measurement Approaches model selected.
- Purely statistical "validation" of operational risk capital measures will not be possible for many years (if ever)!
- Executive management and business managers should review and ratify the methodology and approve the specified capital level. This is an appropriate Executive accountability:
  - *"We understand and believe that the capital charges reflect the risks in our business"*
- "Use test" of the model as part of the day-to-day risk management process.

### Model validation:

- Assess the sensitivity of RDCA model choices and parameterization (question weightings, response scores, distribution assumptions as appropriate, etc.).
- Internal/external benchmarking for reasonableness of total operational risk capital by using different methods.
- Continually compare question responses with internal/external operational risk data (including losses) and consideration of stress scenarios, using expert judgment.

# Lessons Learned

## Executive  Management Direction and Support

- Ensure Executive management buy-in to the concept of assigning operational risk capital to the businesses up front
- Agree the composition and the role of the Project Steering Committee
- Regularly engage Executive management and the Board throughout the process

## Stakeholder Involvement & Buy-in

- Involve the businesses from the beginning
- Discuss and agree with all stakeholders the appropriate usage of internal & external data and scenario analysis in the RDCA framework design
- Strongly leverage relevant subject matter expertise

## RDCA Development Process

- Avoid over-emphasis on excessive precision in the risk measurement methodology
- Pilot the questionnaires with a small number of businesses and incorporate feedback
- Don’t “over-engineer” the process initially – focus on the essence and continuously evolve
- Ensure question responses can be independently validated and identify validation mechanisms, including the role of internal audit, in advance
- Appropriately involve supervisors in the development of the RDCA framework to facilitate understanding

# Lessons Learned (Cont.)

**Use <u>all</u> available information**

- External data can be very helpful in formulating scenarios, when detailed information is available regarding control breakdowns and other causal factors
- Use all internal data (not just loss data) to check the validity of questionnaire responses

**Use technology as an enabler to facilitate the process**

**Ongoing Considerations:**

- Ensure transparency in the ongoing capital methodology to:
  - optimize behavioral incentives to improve risk management;
  - optimize feedback from businesses; and
  - maintain credibility with the businesses
- As the environment, core processes and business mix change, periodically review questions, response choices and weightings to ensure:
  - emerging risks are appropriately captured;
  - optimal responses keep pace with leading practice; and
  - behavioral incentives remain appropriate for the institution
- Questionnaire results are often useful for identifying and/or refining key risk indicators and integrating these into the operational risk management process

# RDCA Refinement and Evolution

**How should the RDCA's performance be reviewed and how frequently?**

- Does the model output continue to be an accurate reflection of the operational risk profile?

**When should the aggregate operational risk capital pool size be reviewed? Factors to be considered:**

- The rate of change of the business mix
- The rate of growth
- The introduction of new products or business lines
- Internal structure changes

**How to manage integrating new risks and measures?**

- Trade-off: Stability and comparability from one period to the next, versus risk sensitivity

**Where is additional management focus on specific risks and mitigants warranted?**

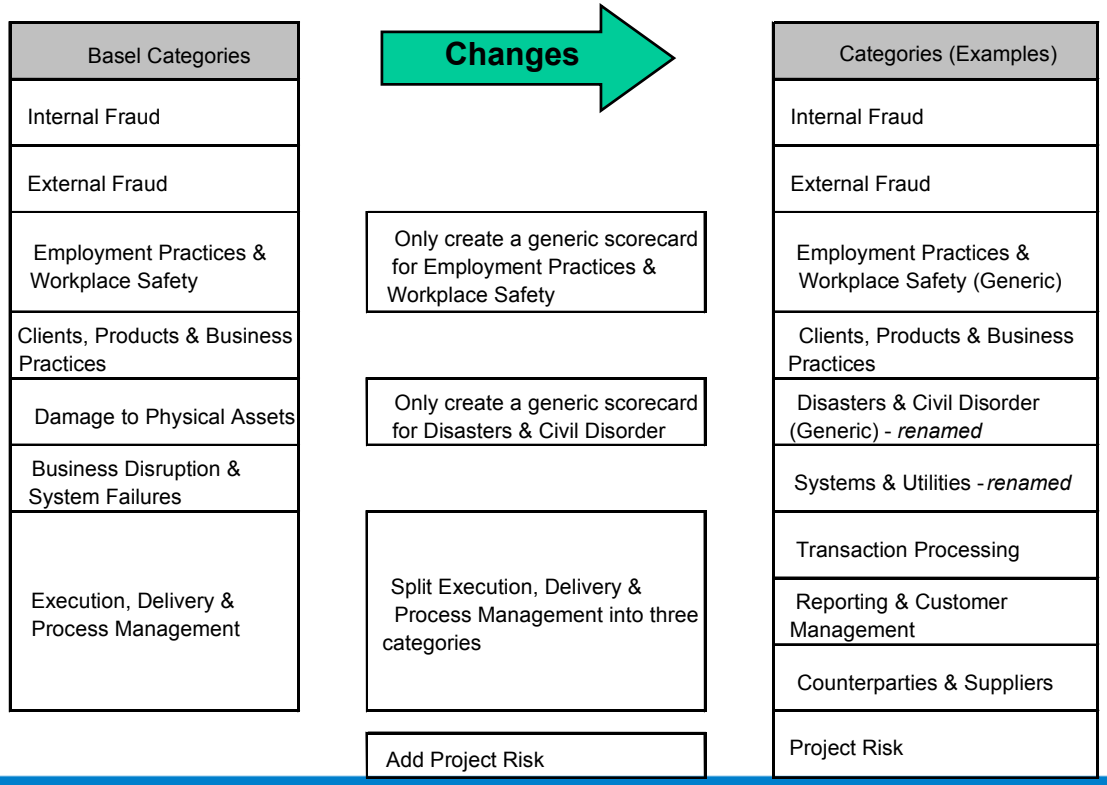
- Focus resources on new risks and high risk areas with poor control scores

# Appendices

# Appendix A - Example of Internal Risk Categories

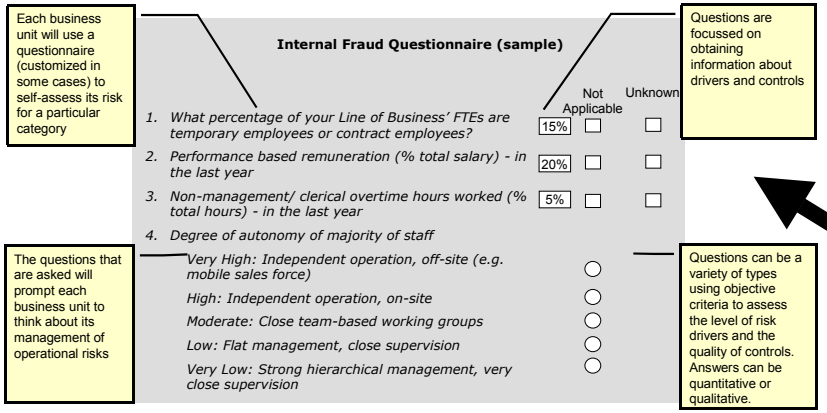
**RDCAs provide a risk assessment tool adapted to each of the differentiated types of Operational Risks (known as risk categories)**

- Risk events are best measured in categories
- Risk Categories have differentiated exposures and need to be weighted accordingly
- Measurement within each category is differentiated, this is recognised in the questionnaires
- It may be appropriate to tailor the Basel risk categories to reflect the needs of the institution



# Appendix B - Scoring components of RDCA Questionnaires

**A. Question Scoring:** Responses have preset calibrations for grading responses from suboptimal to optimal




In this example let us assume scoring ranges 1 (optimal) to 10 (suboptimal), weighting (for this example 15%)

For simplicity, let us also assume the following scoring bands:

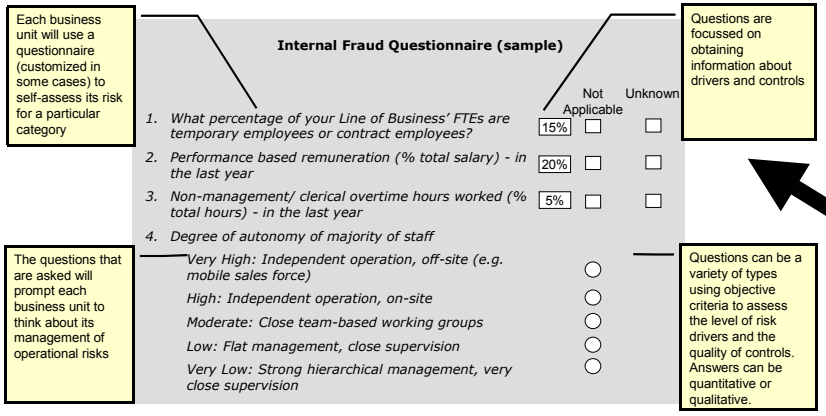
| | | |
|---|---|---|
| Very High | = | 10 |
| High | = | 7 |
| Moderate | = | 5 |
| Low | = | 3 |
| Very Low | = | 1 |

If the response selected was high, the score allocated would be 7 (towards the suboptimal condition for this risk driver).

All questions would have 'scores' derived in this manner, although the exact calculation mechanism would be tailored to the response type and the relationship could be simple bands, linear or much more sensitive.

# Appendix B - Scoring components of RDCA Questionnaires (cont.)

**B. Question Weighting:** All questions are weighted against each other to derive a 'relative importance factor' used in deriving the overall score.




In this example let us assume relative weighting is provided by apportioning the questions a % of the overall value i.e. the sum of the question weights in the questionnaire equals 100%.

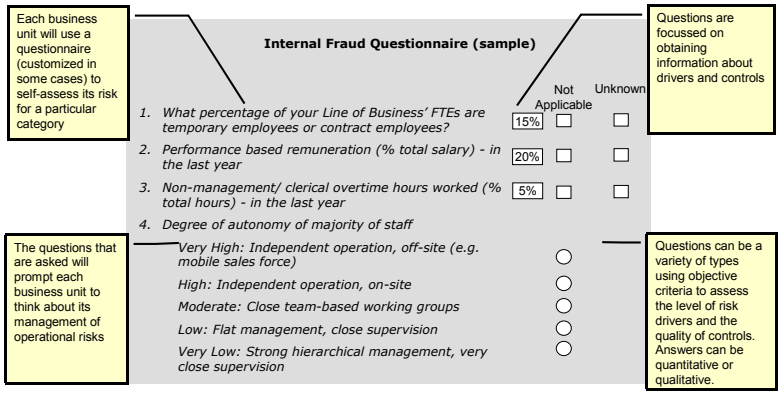
To follow the example through we assume the weight of this question is 10%.

Taking the question score derived on the previous page, 7, we can calculate the weighted score as 7*10% = 0.7

The total of **all** the weighted question scores therefore would give a score between 1 and 10 i.e. ten questions weighted at 10% each all receiving responses scores of 7 would each have a weighted score of 0.7. Totalling these, the questionnaire or Residual Risk Score (RRS) score for the category would equal a score of 7 within the examples scoring range of optimal at 1 and suboptimal at 10.

# Appendix B - Scoring components of RDCA Questionnaires (cont.)

**C. Risk Scaling:** The RDCA methodology includes a "size" mechanism through which the scale of risks is accounted for in the assessment. Sizing determinants may vary for different risk types and are customized within organisations to characteristics that have a relationship with the various risk categories.

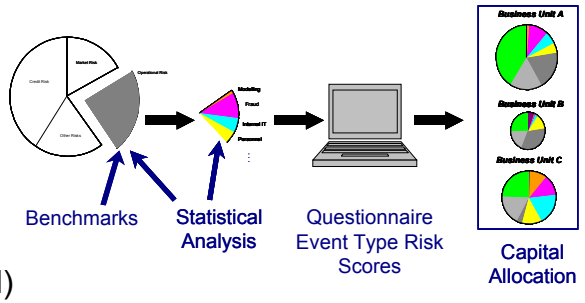



Sizing factors give a perspective on the scale of an operation in respect to the risk controls and drivers and hence its overall level of operational risk. This can be assessed as a related factor outside the questionnaire itself.

As an example, "Internal Fraud" could be "sized" by the number of staff in the operation being assessed (raw headcount or converted to Full Time Equivalent (FTE) staffing levels). This is utilised to allow for the calculation of different overall results for two operations with similar risk profiles that differ greatly in their scale, i.e. the actual amount of business conducted. A diversity of organisational characteristics are currently in use in RDC Approaches.

Note that multiple organisational characteristics may be used in determining a risk category's scale factor.

# Appendix C - Example of Initial allocation of capital




**Assumption 1:** Group Economic Capital calculated at $2b

**Assumption 2:** Risk Category: Internal Fraud, assessed at 10% of Group Capital ($200m)

**Assumption 3:** Scalar: Number of Staff (Full Time Equivalent basis) 10% weighting equating to $20m from the pool (Multiple scalars in this risk category making up 100% in total)

**Assumption 4 (questionnaire results):**

Business Unit A survey result 1.5, FTE scalar 1000

Business Unit B survey result 2.0, FTE scalar 500

Business Unit C survey result 1.0, FTE scalar 5000

**Calculation**:

Adjusted Risk Score = Risk Score * Scalar

Sum of Adjusted Risk Scores = 1.5*1000+2.0*500+1.0*5000 =1500+1000+5000=7500

Capital To Be Allocated per unit of Adjusted Risk Score, R = $20m / 7500 ~ 2667

Initial capital allocated for Internal Fraud risk category 1 = (Adjusted Risk Score for business unit X) * R

Initial capital A = 1.5 * 1000 * 2667 = $4m

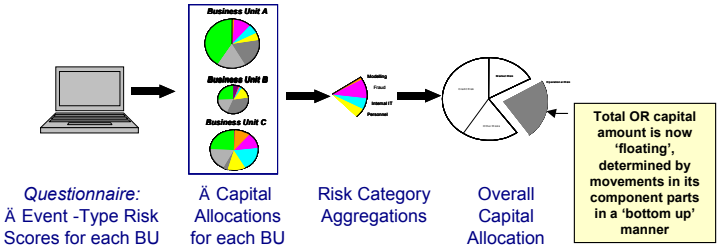
Initial capital B = 2.0 * 500 *2667 = $2.667m

Initial capital C = 1.0 * 5000 * 2667 = $13.333m



Back to slides

# Appendix C - Example of Ongoing Capital Calculation




**Assumption 1:** BU A has decreased Risk Score but FTE scalar is stable at the end of the first period

**Assumption 2:** BU B has not changed either Risk Score or FTE scalar

**Assumption 3:** BU C has decreased Risk Score but FTE scalar has increased

**Assumption 4 (specific questionnaire results at end of first period):**

Business Unit A: Risk Score 1.25, FTE scalar 1000

Business Unit B: Risk Score 2.0, FTE scalar 500

Business Unit C: Risk Score 0.8, FTE scalar 5500

**Calculation**:

New capital allocated for risk category 1 = (New Adjusted Risk Score for business unit X) * R

New capital A = 1.25 * 1000 * 2667 = $3.333m (from $4m)

New capital B = 2.0 * 500 * 2667 = $2.667 (no change)

New capital C = 0.8 * 5500 * 2667 = $11.733 (from $13.333m)

Note that R, the capital to be allocated per unit of Adjusted Risk Score, may be reset periodically. The period is shorter if risks are more dynamic and longer when they are more static. This method makes Business Unit allocation responsive to improvements/deteriorations in the business and control environment.



Back to slides