

Risk and Control Self Assessment (RCSA)



Session 1

Presented by Phyllis Segal
RMA Faculty—Operational Risk
phyllis@segal.org



Today's Instructor

Phyllis Segal



phyllis@segal.org

RMA Faculty –
Operational Risk



Course Topics

Session 1

1. Setting the Context of RCSA
2. Why do a RCSA?
3. Organizational Issues
4. Resources Required
5. Frequency and Granularity

Course Topics

Session 2

- 6. RCSA Components and Steps
- 7. Step by Step - How to conduct a RCSA

1. Setting the Context

- A. What is a RCSA?
- B. RCSA and Operational Risk toolbox
- C. Operational Risk in the context of Risk Management
- D. What is Operational Risk?
- E. Operational Risk and Basel II
- F. Inherent vs. Residual Risk

A. What is RCSA?

Formal documented process used to proactively identify, assess, manage and report operational risks and controls

A. What is RCSA?

Risk

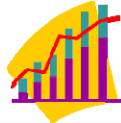
- Anything that could jeopardize the achievement of an objective.
- Examples include: inaccurate records or information, fraud or employees not following process due to lack of skill.

Control

- Methods, procedures, equipment or other things that provide additional assurance that relevant business objectives will be met.
- Types of Controls include: Preventative, Detective, Compensating controls

B. RCSA and Operational Risk Toolbox

- Key Risk Indicators
- Loss Reporting and Analysis
- Operational Risk Dashboard



DASHBOARD

ABC Bank Limited Processing Risks Summary As at 09/30/02
Foreign Exchange Business

Overall Risk Rating - Moderate

Losses Processing Risk - Q3 Loss Report
Detailed Report: FX

	Q3 02	Q2 02	Q1 02	YTD 02	Q3 01	Q2 01	Q1 01	YTD 01	Q3 00	Q2 00	Q1 00	YTD 00
Execution Losses - HF	15	18	8	41	15	88	115	218	15	15	15	45
Execution Losses - non-HF	21	23	14	58	61	85	147	295	15	15	15	45
Settlement Losses - HF	15	22	24	61	66	78	212	456	15	15	15	45
Non	62	69	68	199	63	74	147	304	15	15	15	45
TOTAL	113	142	114	361	315	406	874	1,018	60	60	60	180
Q3/02 YTD	113	142	114	361	315	406	874	1,018	60	60	60	180

Key Risk Indicators (KRIs)

Commentary
Numbers of outstanding confirmations increased significantly in Sept, taking them just into the high risk band. Hedge funds account for the majority of the increase. Payment mismatches remain moderate with little impact felt from the IT changes.

Approval Business Mgmt Risk Mgmt

Action Item Alert

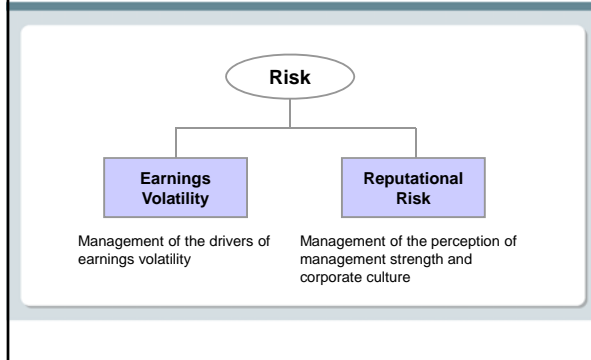
Open FX High Risk Action Items

- FX Management committed to automate the capture of hedge fund payment instructions. Status: Overdue and Open
- FX Management to monitor the impact of HF client take on rate on processing infrastructure with a view to moderate/rise if risk levels rise further. Status: Current and Open

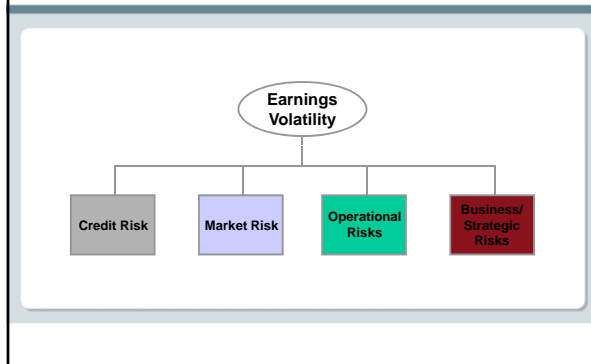
Environmental Factors (EFs)

Commentary
Market EP's continue to show pressure building on the infrastructure. HF take on is ahead of plan and looks set to continue. Client satisfaction continues to weaken. The technology environment is stable with hedge fund enhancements anticipated in Q4. Rework within Operations has increased on settlement problems, overtime is increasing but the risk is under control.

C. Operational Risk in the Context of Risk Management



C. Operational Risk in the Context of Risk Management



D. What is Operational Risk?

"... the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. The definition includes legal risk but excludes strategic and reputational risk."



E. Operational Risk - Basel II

- 3 methods for calculating operational risk capital charges (Basic, Standard, Advanced Measurement Approach)
- 11 principles for the sound management of operational risk relate to:
 - Role of the Board and Senior Management in developing and maintaining an appropriate risk management framework and environment
 - Risk Management: Identification, Assessment, Monitoring and Mitigation/Control including New Product Approvals, and Business Continuity
 - Role of Disclosure

www.bis.org

F. Inherent vs Residual Risk

- **Inherent/gross** risk is the amount of risk that exists, without taking into account the existence of controls
- **Residual/net** risk is the amount of risk that exists, taking into account the existence of controls

2. Why do a RCSA?

- Consistent management of operational risks across the organization
- Reduce losses, higher profitability
- Improve audit results
- Regulatory requirement
- Management takes responsibility for their own risks
- Improved processes, teamwork and role clarity
- Greater efficiency and effectiveness

3. Organizational Issues

- A. Centralized vs. Decentralized
- B. Role of the Board
- C. Role of Senior Management and Businesses
- D. Role of Audit
- E. Ownership and Accountability

A. Centralized vs. Decentralized

- Who conducts the RCSA?
 - Methodology
 - Identification
 - Assessment
 - Monitoring
 - Reporting
- Benefits of each approach

B. Role of the Board

- **Take the lead** in establishing a strong risk management culture.
- **Approve and periodically review** the bank's operational risk management framework. Framework should provide a firm-wide definition of Operational Risk and lay down the principles of how operational risk is to be identified, assessed, monitored and controlled/ mitigated
- **Approve and review** a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

C. Role of Senior Management and Businesses

- Senior Management
 - Implementing the operational risk framework approved by the board of directors
 - Developing policies, process and procedures for managing operational risk in all of the bank's material products, activities, processes and systems
- Businesses
 - Manage/own risks in their businesses

D. Role of Audit

- NOT directly responsible for Operational Risk management
- Conduct an independent check on all management processes, including Operational Risk management, and RCSA
- RCSA ratings should be a consideration for Audit business reviews
- Ensure that risks were identified and assessed properly, that progress is being made on RCSA Action Plans

E. Ownership and Accountability

- **Responsibilities** for risks have been formalized
- **Awareness** of risks by business heads has increased and that THEY own the risk
- Some of these risk categories were **managed before** (with varying degrees of success)

4. Resources Required

- A. People
- B. Time
- C. Technology



Some RCSA Software*

Name of Vendor	Web Address	Product name	GRC?
Centerprise	centerprise.com/products/eopriskcenter.html	Enterprise OpRisk Center	No
Sword Achiever	www.sword-achiever.com/	Achiever Plus	Yes
Methodware	www.methodware.com/kairos/	Kairos	Yes
OpenPages	www-01.ibm.com/software/analytical/openpages/	GRC Platform	Yes
Protiviti	www.protiviti.com/grc-software/Pages/Risk-Management.aspx	Governance Portal for Risk Management	Yes
SAS	www.sas.com/software/governance-risk-compliance/index.html	Governance Risk and Compliance	Yes
Thomson Reuters	accelus.thomsonreuters.com/solutions/enterprise-grc	Enterprise GRC Solutions	Yes

* Not an endorsement for any particular software

5. Frequency & Granularity

- A. Frequency
 - As often is required to manage the risk
 - Annually, on a tiered basis
 - Quarterly
- B. Granularity
 - Scoping the enterprise

See you next session!

- RCSA Components: Objectives, Risks, Controls, Action Plans
- RCSA Steps: Identify, Assess, Act, Report
- Step by Step - How to conduct a RCSA