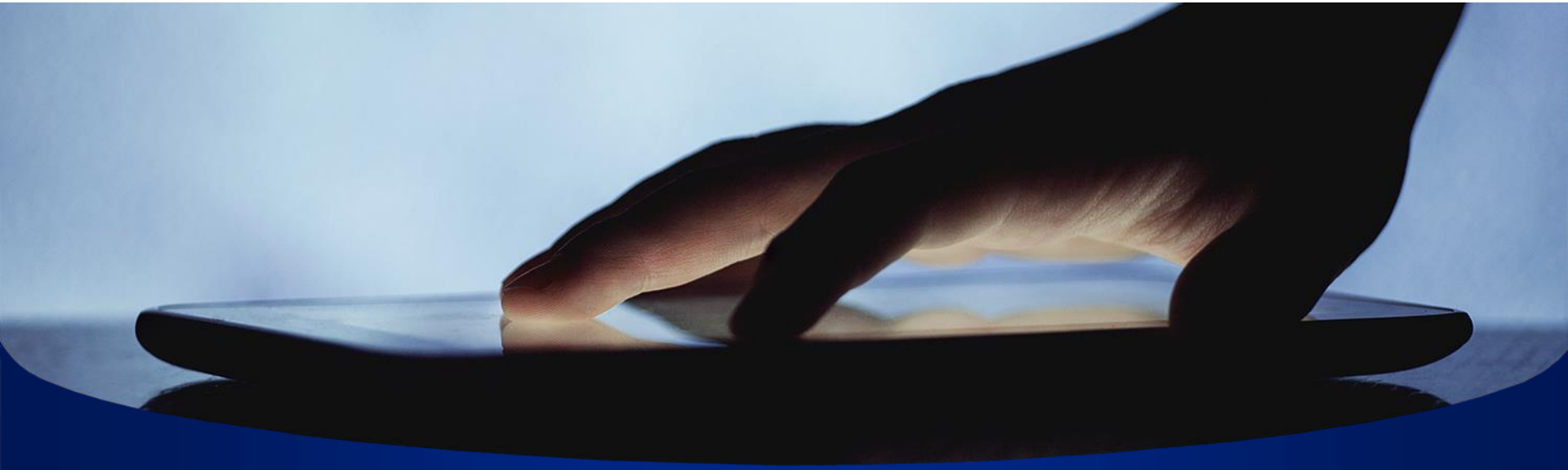
Operational Risk what is it? How does BCM Fit?

Karen Kemp, Director Operational Risk Management RBC

May 2017 BCAW



Technology & Operations

Agenda

1. What is Operational Risk
2. RBC Worldwide
3. Technology and Operations
4. T&O Operational Risk Program
5. Q&A

What is Operational Risk?

- The generic term ‘operations risk’ was officially coined in 1991 (COSO 1991) but was not widespread until the mid to late 1990s when Basel 2 proposals were developed and published in June 1999

- Operational Risk is not a new risk… However, the idea that operational risk management is a discipline with its own management structure, tools and processes… is new. (British Bankers Associate website, accessed 26.08.02)

- Three pillars of Basel II
  - Pillar 1 – Minimum Capital Requirement TOTAL RISK, Credit, Market & Operational
  - Pillar 2 – Supervisory Review Process
  - Pillar 3 – Market Discipline

- So how does this affect me?

Strategic Goals

- In Canada, to be the undisputed leader in financial services.
- Globally to be a leading provider of capital markets, investor and wealth management solutions.
- In targeted markets to be the leading provider of select financial services.

- Operates in ***44 countries***
- ***80,000+*** full and part time employees
- More than ***16 million*** clients worldwide

5 Business Segments

- Personal and Commercial Banking
- Wealth Management
- Insurance
- Capital Markets
- Investor and Treasury Services

Technology is anchored within T&O, which operates a complex technology environment and delivers critical capabilities for the business

Complex array of technology assets and physical infrastructure	Resilient and secure "engine" for business activities	Culture of performance, delivery excellence, regulatory compliance
2,600 applications	$42 trillion payments processed annually	1,700 active projects in 2013
25,000 servers	380 million client transactions completed daily	3,300 change requests delivered per month
19 data centres	4 million online banking clients	60,000 calls a month into the Enterprise Service Desk
50,000 devices send security events to the Security Operations Centre	1 million mobile banking clients	

All numbers are approximate

A number of forces of change are enabling significant shifts in traditional business models

Regulation

- New regulation
- Regulator scrutiny

Maturing technologies

- Mobile — Anywhere / anytime
- Big data and Analytics — Deep insight, volume and velocity
- AI / Cognitive Computing — Adaptive, self learning
- Cloud — Fast deployment, on demand, lower barriers of entry
- Social Media — Instant feedback to millions / constant connectedness

MAJOR BUSINESS SHIFTS

Business Models

- Investing heavily — Traditional competitors
- Superior client experience — Niche players
- Speed and agility, continuous relationship — Digital giants

Security threats

- Cyber
- Fraud

With growth and change comes risk..

and T&O is in a constant state of change…

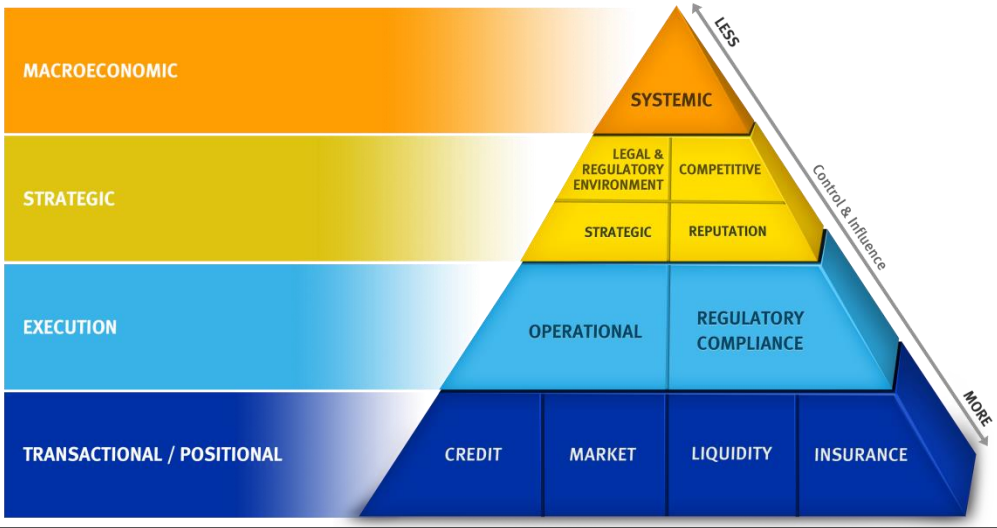
- ***Project Risk*** - Where the business wants it now – mobile, competition
- ***Information Technology Risk*** - Cloud – how do you risk assess something new and leading edge?
- ***People Risk*** – supporting legacy systems when the programming language is no longer taught in schools
- ***Privacy Risk*** – protecting our customers, employees and company
- ***Processing and execution risk*** – executing change management risk the first time.

RBCs Operational Risk Management Approach

- **RBC definition of Operational Risk**
  - **The risk of loss or harm resulting from inadequate or failed internal processes, people and systems or from external events.**

- BASEL definition
  - Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.

Operational Risk Categories



Operational Risk: The risk of loss or harm resulting from inadequate or failed internal processes, people and systems or from internal events

2nd LOD – Enterprise Operational Risk provides oversight & challenge for all 18 categories

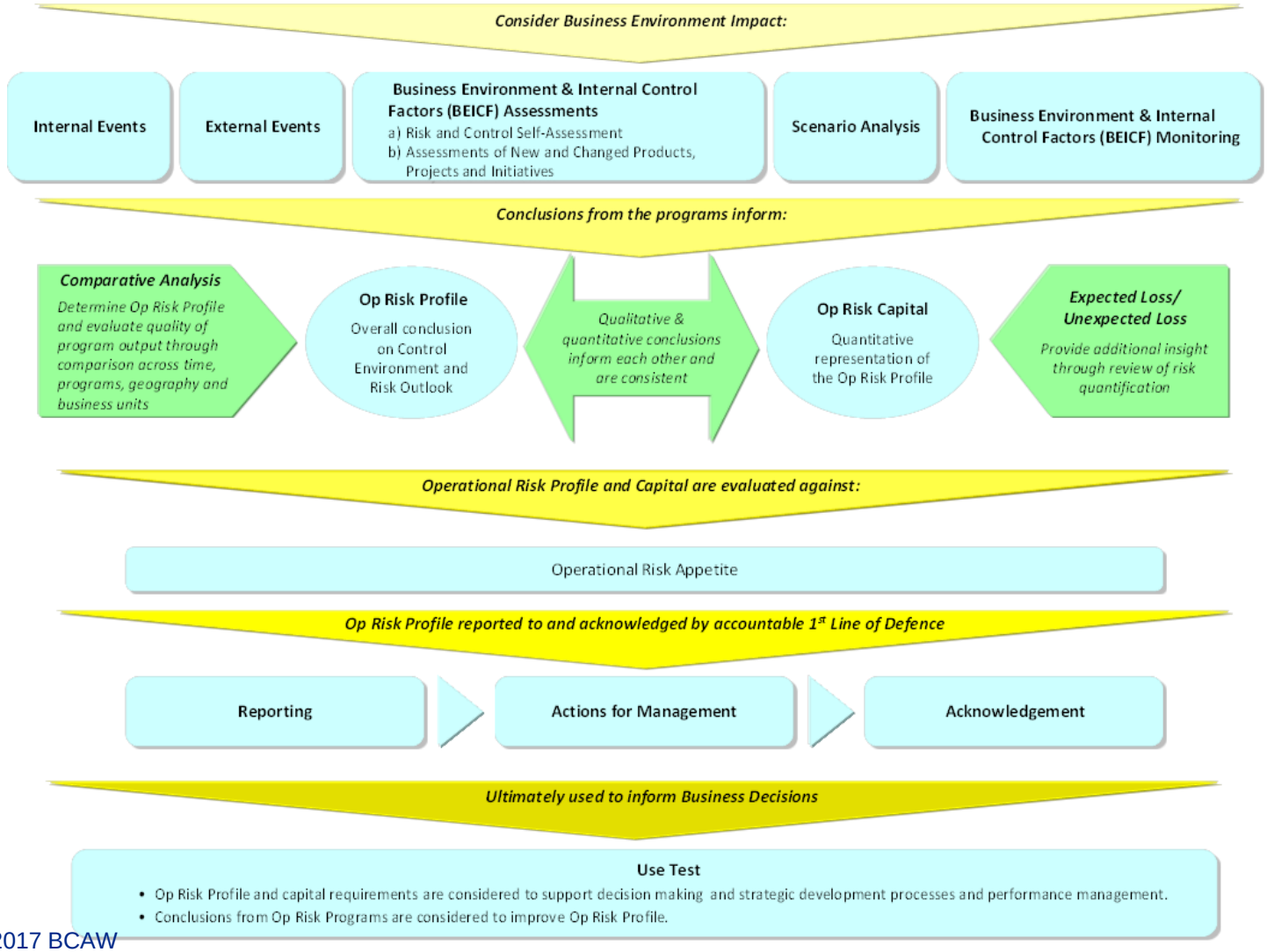
2nd LOD Centre of Governance provides support, oversight & challenge in their area of expertise

Finance Risk	Legal/ Fiduciary Risk	BCM/ Resilience Risk	Safety and Security Risk	Project Risk	Privacy Risk	Money Laundering	People Risk	Product Risk	Third Party Risk	Model Risk	Info. Mgt. Risk	IT Risk	Tax Risk	Suitability Risk	Fraud Risk	Regulatory Compliance Risk	Processing and Execution Risk

1st LOD - T&O BUORM Assesses risk for all 18 Operational Risk Categories

BUORM takes E2E *Horizontal* view, while CoGs leverage in depth knowledge for a deep *Vertical* view resulting in an *Integrated Risk Assessment for RBC.*

Enterprise Op Risk Program Elements



Operational Risk Management Processes

Risk & Control Assessments

- Cover many aspects Enterprise, Unit, Process, Trigger are all various types of assessments.
- All assessments must consider all 18 areas of Operational Risk
- Findings are treated the same as audit findings and tracked, and reported.

Risk Appetite and KRIs

- Risk appetite is the amount and type of risk one is willing to accept
- Risk appetite helps protect organization from an unacceptable loss or an undesirable outcome with respect to earning volatitly, capital adequacy or liquidity, while supporting and enabling the overall business

Business Environmental Factors and Internal Control Factors

- Risk parameters used in the management and measurement of operational risk Reflect the assessment of the Operational Risk Profile, both for a specific business and across RBC
- Consist of external/market factors and internal/business factors that are considered as part of the Enterprise-Level Risk and Control Self-Assessment
- Involves a qualitative assessment of the following factors:
  - 6 to 18-month risk outlook assessment determined during Risk and Control Self-Assessments from underlying Business Units and quarterly updates of significant changes to the Operational Risk Profile
  - Input from CoGs for specific Operational Risk Categories
- Ongoing monitoring of industry or internal developments

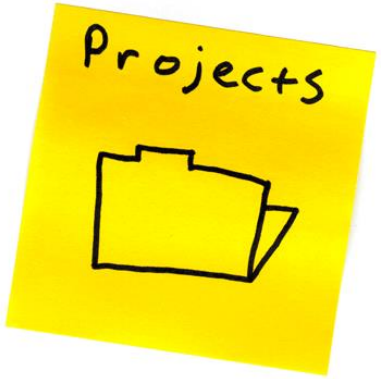
Internal Events/External Events/Projects

Internal Events

- An operational risk event is a specific incident where operational risk leads to, or could have led to, an unintended, identifiable impact
- Operational risk events can be further divided into two groups: Internal Events and External Events
  - *Internal Events* are those that affected RBC, or one or more of its subsidiaries or Business Units
- *External Events* are those that affected institutions other than RBC

IRP (Integrated Risk Profile)

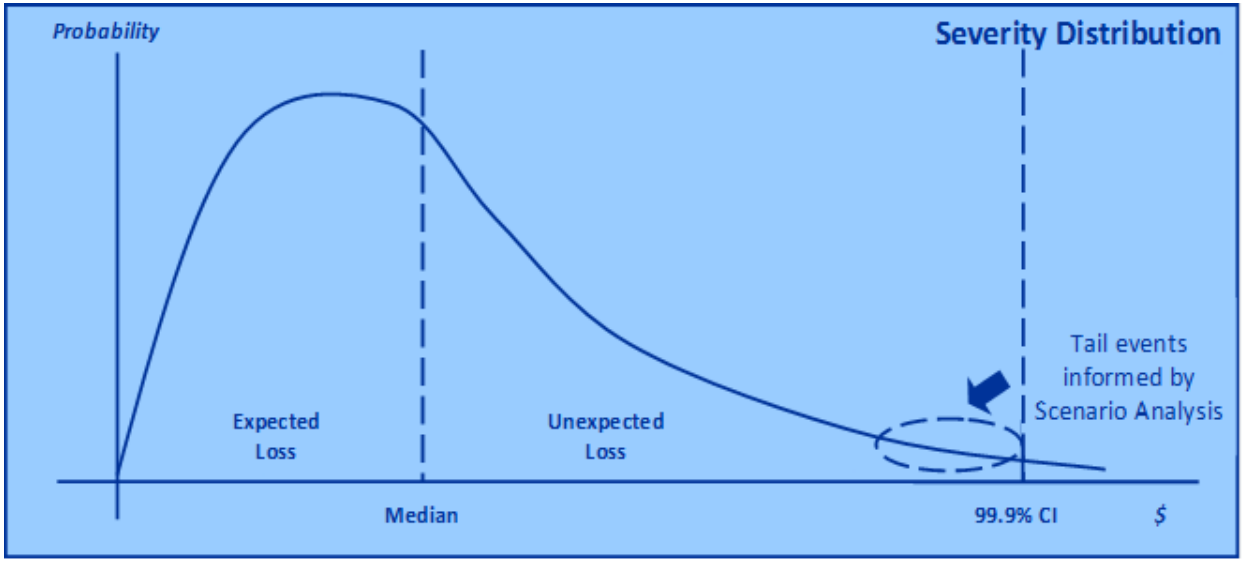
- Policy change now requires IRP to be completed for all projects prior to funding approval
- Project Managers must ensure the IRP is completed. The IRP is to be approved by the Project Sponsor or Sponsor delegate. Furthermore; the Project Manager must ensure that the Business Segment Operational Risk Management Team and relevant Centres of Governance are engaged in its review and provide approval and concurrence respectively.
- The IRP should be refreshed where there are material changes to the Project during its lifecycle to ensure that new or changed risks are identified and action plans re-evaluated and documented.



Scenario Analysis

Definition: A structured and disciplined process for making reasonable and plausible assessments of significant operational risk events, including catastrophic risk events; taking into account the expert opinions of business managers, risk managers and subject matter experts in specific areas of risk.

A set of circumstances that combine to create infrequent, yet plausible, severe operational risk events (also known as ‘Tail Events’).



Comparative Analysis

Decision making at various levels of any organization will benefit from more complete and interactive information. Operational risk management frameworks and tools are designed to permit the collection of information in specific areas across business lines on an enterprise wide basis.

The Risk & Control Self Assessment (RSCA) already incorporates comparative analysis into its requirements. Any unit that executes the RCSA requirements articulated in our ORM standard would have performed comparative analysis in the process to leverage, where possible, all and any ORM program outputs as illustrated.

In this analysis, we have taken these ORM program outputs and associated data, such as loss events, scenarios taken place, audit findings, KRI data points, and trends into consideration to form conclusions and recommendations to improve and enhance our risk management procedures and practices.

Recap

- Operational Risk is inherent in everything
- The goal is to establish a ‘risk aware’ culture
- Operational Risk outputs inform business decision making
- Operational Risk principles can be used in all organizations

Questions?