CAFRAL

June 27, 2013

Operational Risk Management Framework- Qualitative requirements

ERNST & YOUNG

Quality In Everything We Do

Introduction of speakers

1. Pavan Kaushal, Partner, Financial services, Risk advisory

2. Kailash Prabhu, Manager, Financial services, Risk advisory

Context Setting

Qualitative requirements is an imperative ingredient for successful risk management – 'Comply, invest and grow differently'

- Around 70% of Basel requirements of TSA is around qualitative requirements
- Around 90% of qualifying requirements of TSA is around qualitative requirements
- Around 20% of AMA requirements is around qualitative requirements
- Around 30% of AMA quantitative requirements is around loss data
- BEICF, one of four mandatory elements in AMA can not be established with sound implementation of qualitative requirements

What top performers* are doing right:

- Communication is transparent and timely, providing stakeholders with the relevant information that conveys the decisions and values of the organization
- The board or management committee plays a leading role in defining risk management objectives
- A common risk framework has been adopted and implemented across the organization

** EY Global Survey released in 2011*

Table of contents

- Introduction

1. RCSA- Elements, value realization and design principles
2. Selecting KRIs- Elements, benefits and design principles
3. Incident and Loss data- Management process and PoV
4. Insurance- Requirements and considerations
5. Interplay between RCSA, KRI and Incident data
6. Turning risk to results- EY insights

Risk management should precede risk quantification
Lesson from crisis

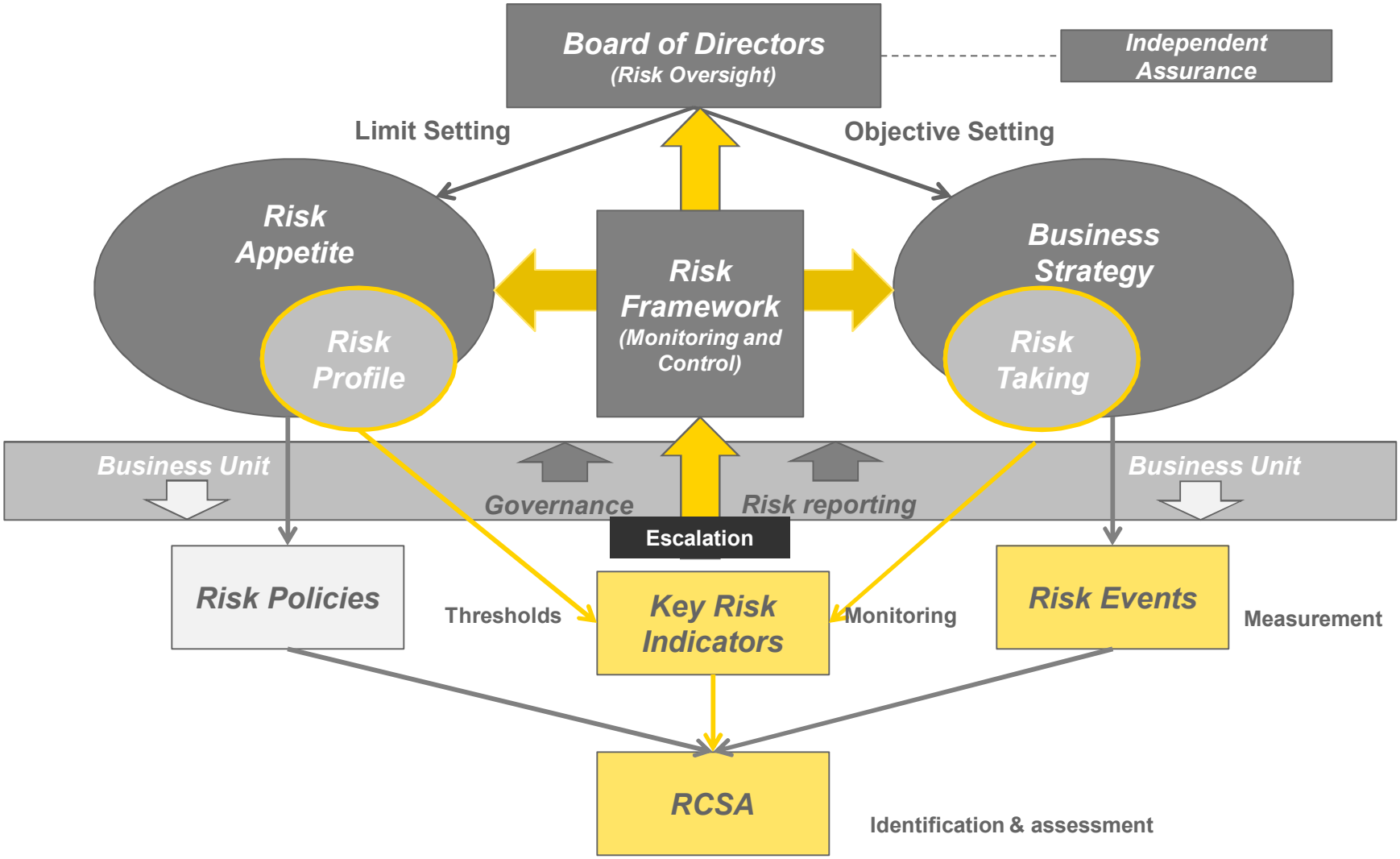
- An institution (wishing to migrate to TSA)has to hold supporting documentation related to the observance of the TSA qualifying criteria. CEBS

- It is prudent to establish and roll out frameworks for risk identification& assessments, risk monitoring and risk measurement before looking to migrate to TSA / AMA (Qualifying criteria compliance)

- There is no risk management in Gross income computation and loss simulation

- Deploy specific tools for the above but provide consolidated risk information with conclusion and management action plan to Senior management & board

Operational Risk Framework
The key elements



Supervisory guidance

- In the past, banks relied almost exclusively upon internal control mechanisms within business lines, supplemented by the audit function, to manage operational risk. While these remain important, there is need to adopt specific structures and processes aimed at managing operational isk. Several recent cases demonstrate that inadequate internal controls can lead to significant losses for banks
- In addition to identifying the risk events, banks should assess their vulnerability to these risk events. Effective risk assessment allows a bank to better understand its risk profile and most effectively target risk management resources. Amongst the possible tools that may be used by banks for assessing operational risk are:
  - Self assessments, Risk mapping and KRIs

-RBI Guidnace note in management of OR (Oct 14, 2005)

- Risk identification and assessment are fundamental characteristics of an effective operational risk management system. Effective risk identification considers both internal and external factors. Sound risk assessment allows the bank to better understand its risk profile and target risk management resources and strategies most effectively.

-BCBS Sound Practices for the Management and Supervision of Operational Risk (June 2011), pg 10

- a bank s firm-wide risk assessment methodology must capture key BEICF that change its operational risk profile. These factors will make the risk assessments:
  - More forward-looking
  - Reflect the quality of the bank s control and operating environment
  - Recognize improvements and deterioration.

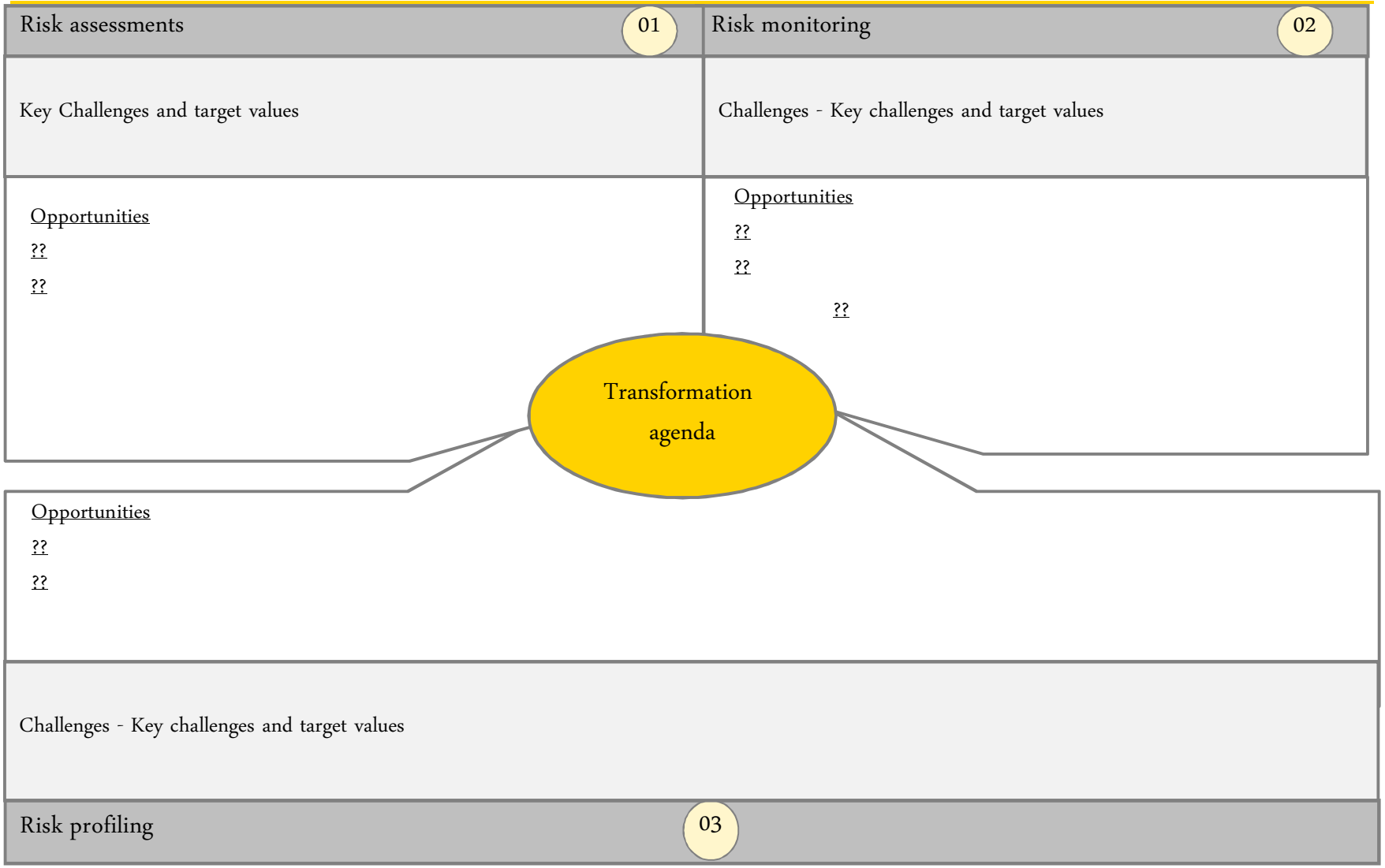
-BCBS International Convergence of Capital Measurement and Capital Standards: A Revised Framework ("Basel II") (June 2004), p. 137

- BEICFs are indicators of a bank s operational risk profile that reflect a current and forward-looking assessment of the bank s underlying business-risk factors and internal control environment.

-Interagency Guidance on the Advanced Measurement Approaches for Operational Risk (June 2011), p. 9

Challenges & Opportunities

Is your program delivering the required value



1 RCSA- Risk identification and assessments
Overview

What is a Risk and Control Assessment (RCA)?

It is a process whereby a business assesses its risks (i.e. strategy, objectives, products, and activities) and the effectiveness of the controls in a structured and comprehensive manner.

- The term RCSA merely defines who does the risk and control assessment

Role of RCA in an operational risk framework

- Provides a **consistent** way to evaluate risks and controls across the organization
- Provides **transparency** around risk and control deficiencies
- Helps **prioritize** remediation actions
- Promotes **BU ownership** of risks and controls
- Supports **risk profile** generation and satisfies regulatory expectations regarding BEICF[1]
- Supports **knowledge transfer** and **training**

Common RCSA Attributes:

Business/ Process	Risk Identification	Control Identification	Control Evaluation	Control Ownership	Risk Rating & grading	Action Plans/Acceptance

[1]BEICF: Business environment and internal control factors

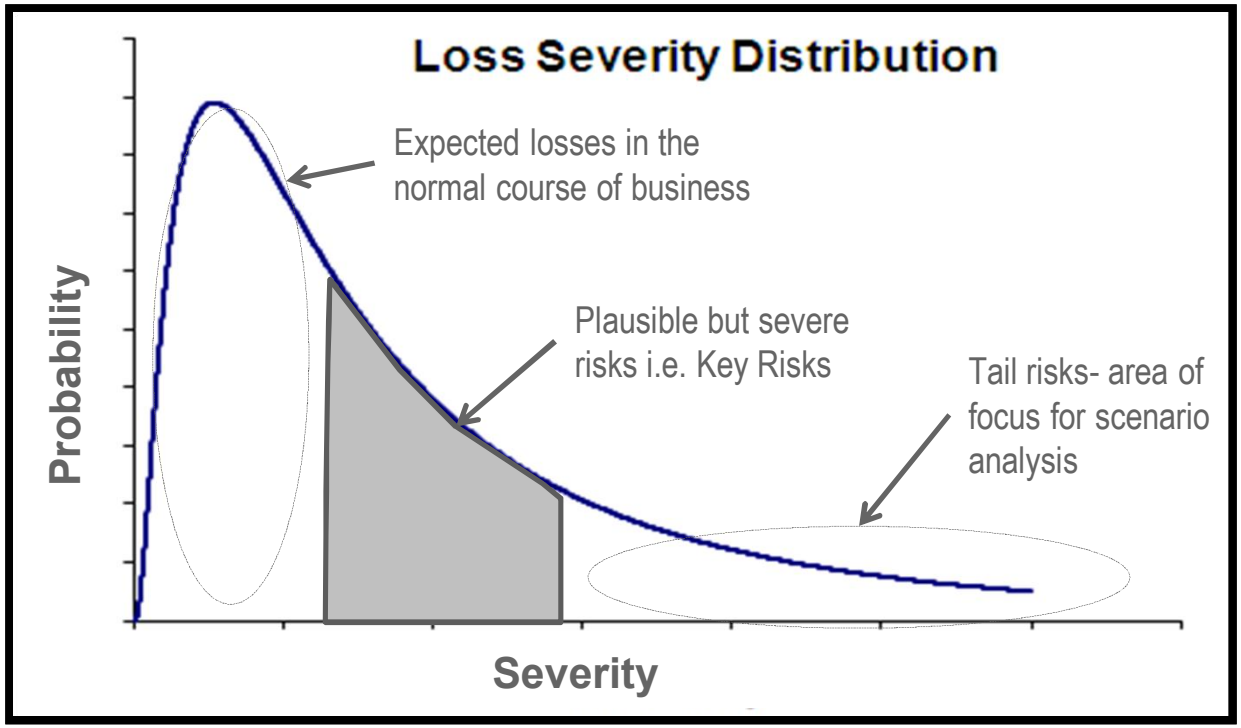
Impediments to value realization

- Lack of defined focus
  - Granular vs. key
  - Risk vs. control
  - One size fits all
  - Refresh
- Overlap and redundancy in assessments
- Lack of meaningful reporting and therefore limited utility
  - Inability aggregate- inconsistent data structure/taxonomy
  - Not focused on key risks and themes
  - Inadequate/inconsistent measurement and analysis
  - Not linked to risk appetite (e.g., exception driven reporting)
- Lack of engagement between risk management and business (due to skill sets, roles & responsibilities, etc.)- assessments not driven by 1st line of defense

RCSA designed in a manner that is not "fit-for-purpose" is a major contributor to these challenges.

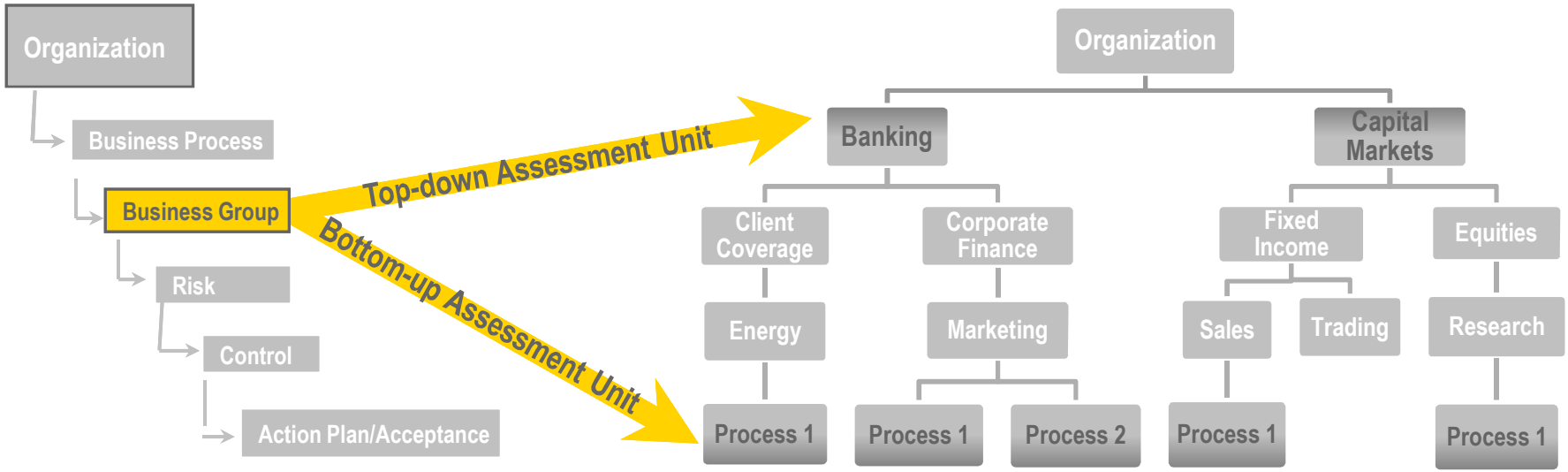
Key Design Principles
Focus of RCSA

- The focus of risk and control assessments is one of the most significant challenges:
  - Once-in-a-lifetime events
  - Commonly occurring events
  - Somewhere in between?



Key Design Principles
Organizational level of RCSA

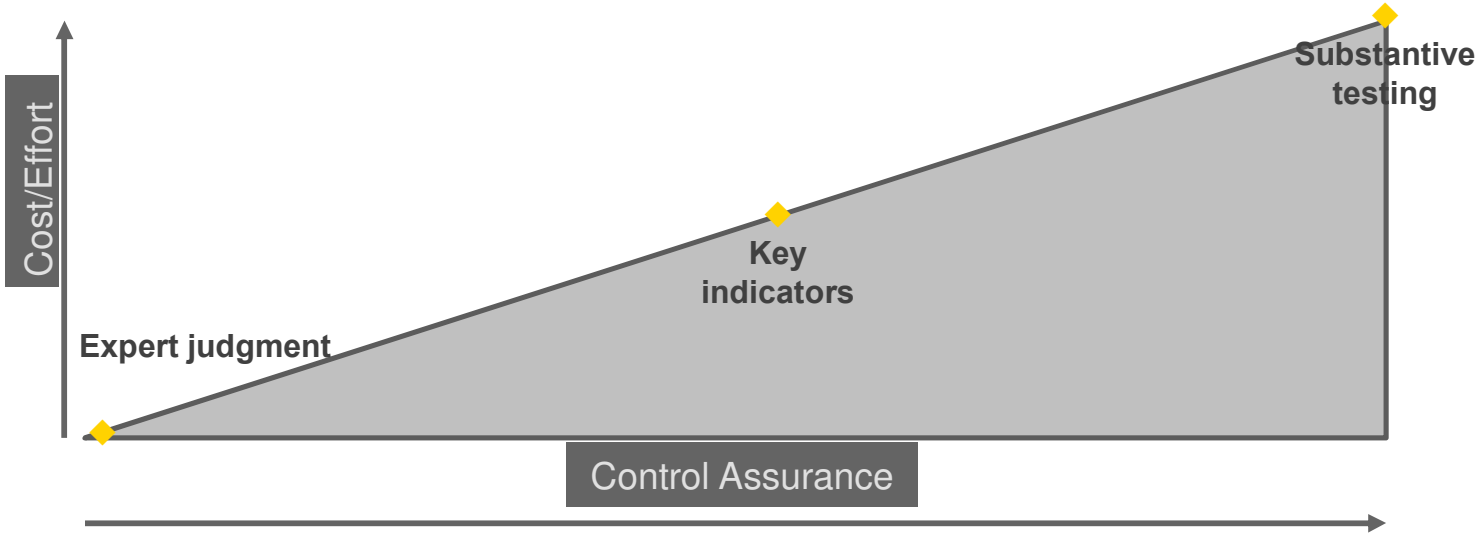
- Top-down vs. Bottom-up
  - Trade-off between resource intensiveness as well as challenges in risk data aggregation versus the need for greater degree of assurance.



Top-down assessments
- Fewer assessment units
- Front-to-back assessments
- Focus on key risk themes

Bottom-up assessments
- Granular level of detail
- Process focused, highly structured
- Tends to be control oriented

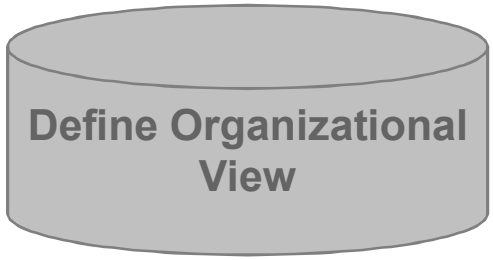
Key Design Principles
Level of control assurance



Key considerations for RCSA testing:

- Testing roles and responsibilities (e.g., skills, training)
- Test design
- Test execution
- Interpretation of results/reporting

Key Design Principles
Common RCSA data structure



- Common hierarchy allows for analysis and comparison

- Promotes the use and acceptance of a common risk and control language to minimize confusion and ambiguity
- Should be flexible - allow for business line customization and organizational roll-up

- Facilitates prioritization of risk controls and issues
- Should be flexible - allow for business line customization and organizational roll-up

Data structure should be common across all framework elements, and to the extent possible, across other risk and control activities.

Key Design Principles
Leverage existing assessments and other data

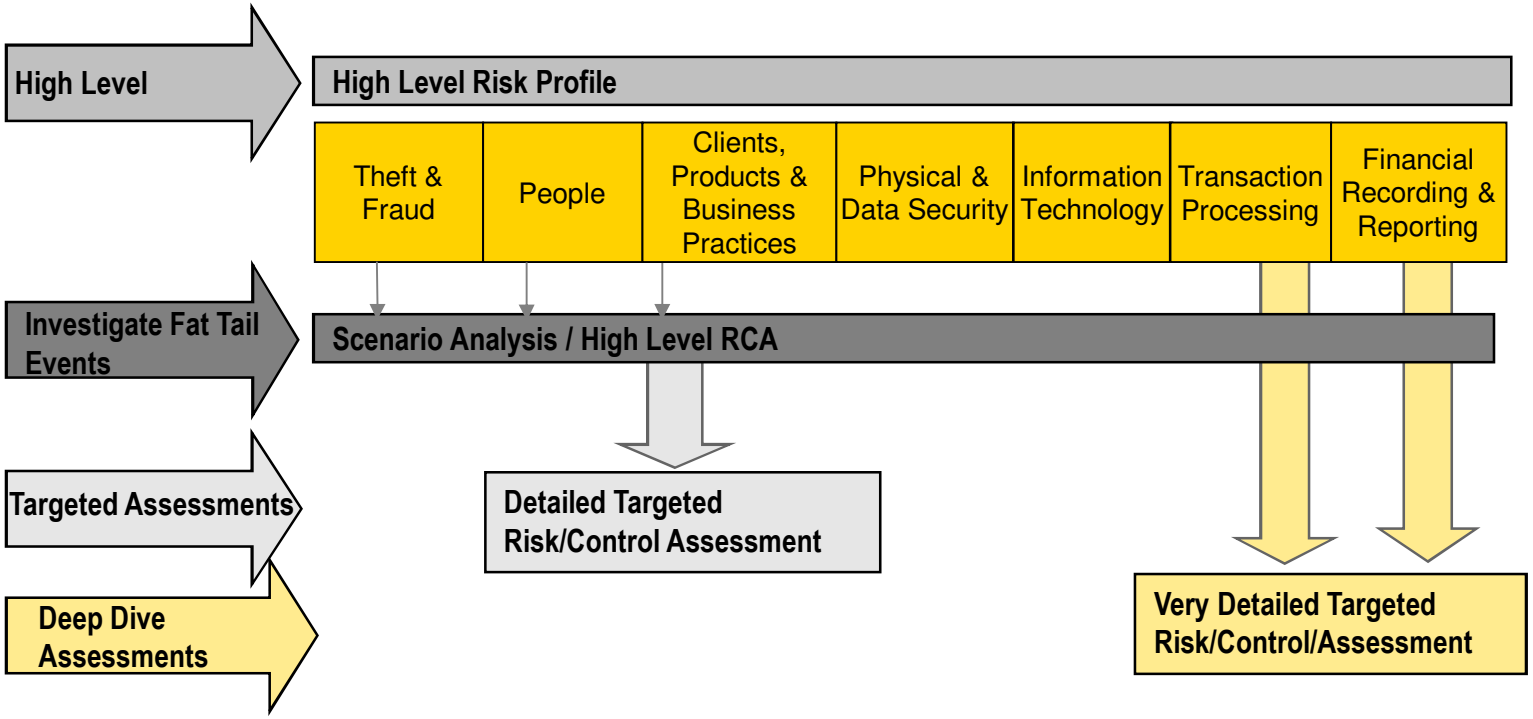
Potential data sources:

- Business plans
- Operational risk incidents
- Regulatory findings/emerging regulatory changes
- External incidents
- Internal/external audit findings

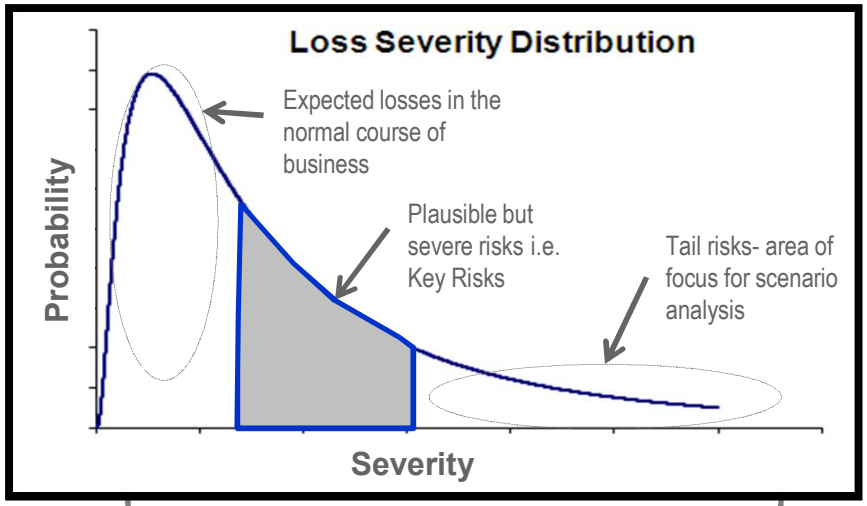
RCAs should leverage information from other assessments and data sources to minimize duplication and overlap.

Key Design Principles
Defined targeted model

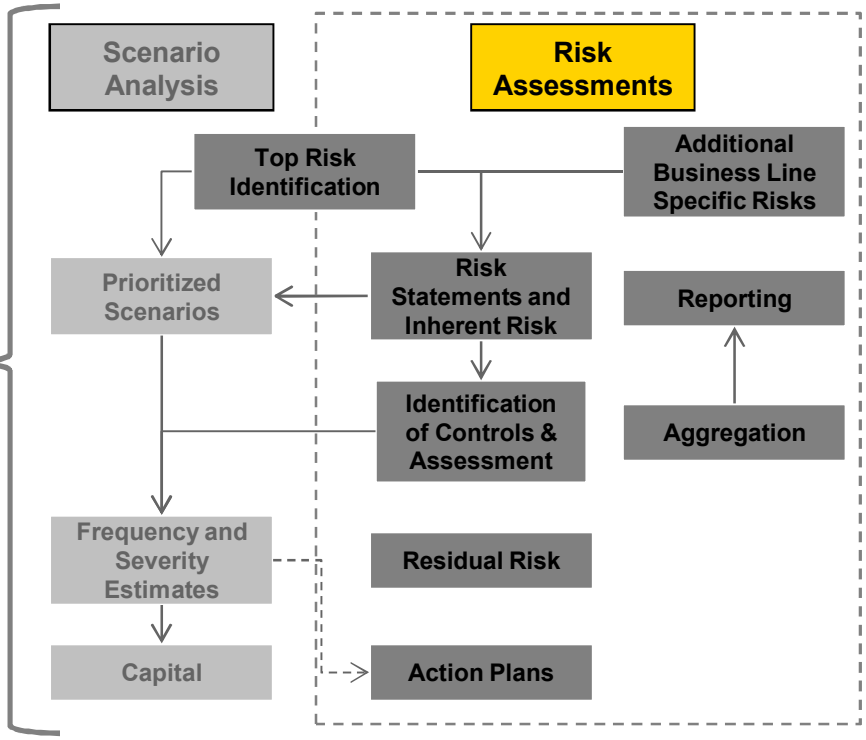
- Combines top down and bottom up approaches
- Recognizes limitations of "one size fits all" approaches
- Leverages other data; detailed assessments are performed as needed



Key Design Principles
Integrating with scenarios



- Scenario Analysis targets infrequent, high severity risks/losses.



- A well designed RCA process can be expanded to accommodate a Scenario Analysis process in order to obtain better exposure estimates.

Key Success factors
What works

- Manage RCSAs like a process design exercise with clear objectives, structure and focus
- Determine how the RCSA will be used and adjust level of control assurance accordingly
- Reduce the burden leverage other assessments/data
- Define roles and responsibilities for RCSA design and execution

Key "people" considerations for the risk management function:

- Strong understanding of the business
- Ability to facilitate the process and analyze RCA results
- Authority to engage with and challenge the business
- Alignment of roles/responsibilities with skill sets

2 Key Risk Indicators (KRIs)
What are they?

- A **risk** is something that has the potential to stop a business from meeting its objectives. A risk is something that has not materialized; it is not an event or a loss, rather a risk is the potential for future events or losses.

- **Risk indicators** are implemented as early warning signals to indicate the likely or impending occurrence of a risk materializing into an event with potential consequent financial losses or impact to brand / reputation.

Key Risk Indicators (KRIs) are predictive measurements implemented to assist management in identifying both changes and possible changes to an organization's risk profile. KRIs are metrics that indicate risk exposure; they do not measure impact.

For example, an increase in customer complaints may be indicative of an increase in the rate of error in product design or development, either of which can increase the risk of loss or reputational damage

KRI Reporting, Monitoring, and Escalation
KRI Database

- A database of KRIs can be maintained which includes the following data fields:

KRI Description	KRI Owner	Frequency	Threshold	Unit of Measure	Historic Data
A detailed description/definition of the KRI and its metric.	The name of KRI owner.	How often the KRI are collected and reviewed.	The boundary on acceptable value of KRI metric as defined by management.	A %, ratio, or amount.	Data for the KRI metric, used for trending.

KRI Benefits

- **A predictive tool for risk management** – All risk management tools should enable identification of risks to prevent them from materializing. However, tools such as Risk and Control Self Assessment (RCSA) and event data collection are backward looking. KRIs provides early warning of potential risk events that may prevent the business from achieving its objectives.

- **Reinforce risk and control ownership and accountability** – Risk takers can monitor their risk profile more frequently rather than just using (often annual) RCSA and therefore can take more immediate action to reduce risk and mitigate potential losses.

- **Recognition of which risks are key at a particular time** – KRIs bring greater awareness of which risks are important to the organization at a given time and facilitates more effective and efficient risk management. KRIs embedded as a management tool will improve risk awareness in the business, reduce losses, and improve profitability.

KRI Benefits (continued)

- **Better understanding of the RCSA** - KRIs enhance a business's understanding of risks and controls and can give tangible evidence of current risk levels and any changes to the business's risk profile. KRIs can also be used to validate levels of the key risks documented in the organization's RCSA process.

- **Clearly set the institution's risk appetite** - KRIs are an important factor in articulating risk appetite. They provide insight into the risk profile at both the enterprise and line of business level. Clearly established KRIs provide the organization with more objective measures of risk levels by which boards of directors, senior management and the business units/control functions can monitor and assess their current risk profile against their established risk appetite.

KRI Design Principles
Leading vs. Lagging Indicators

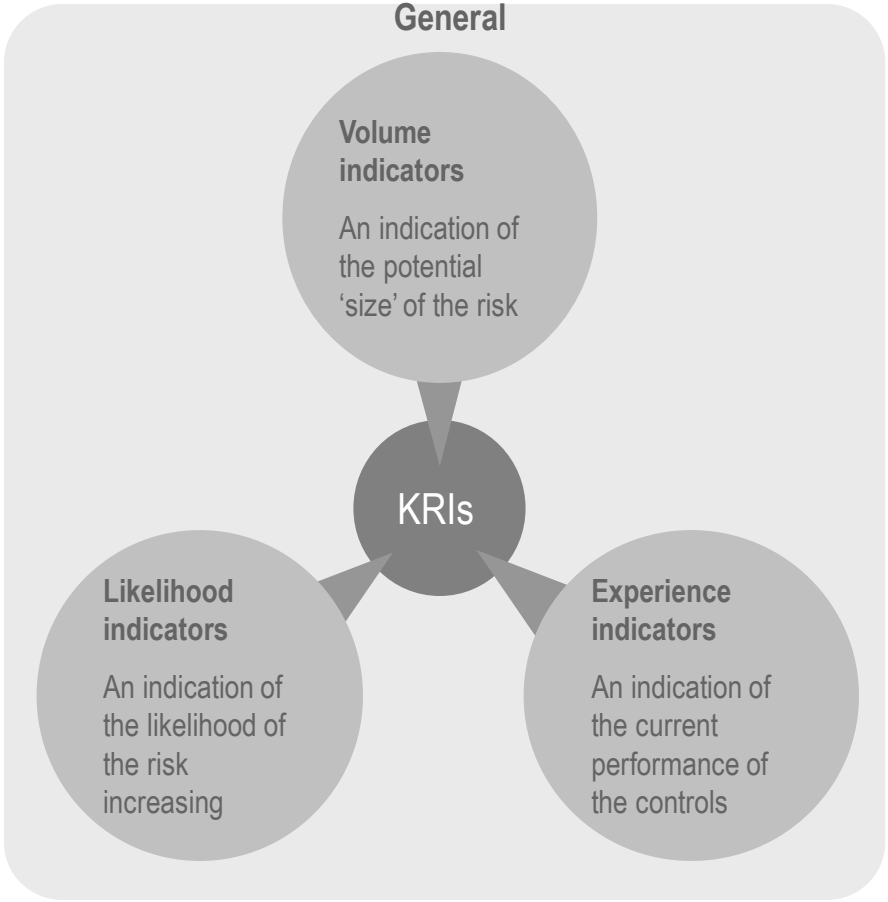
KRIs are either leading or lagging:

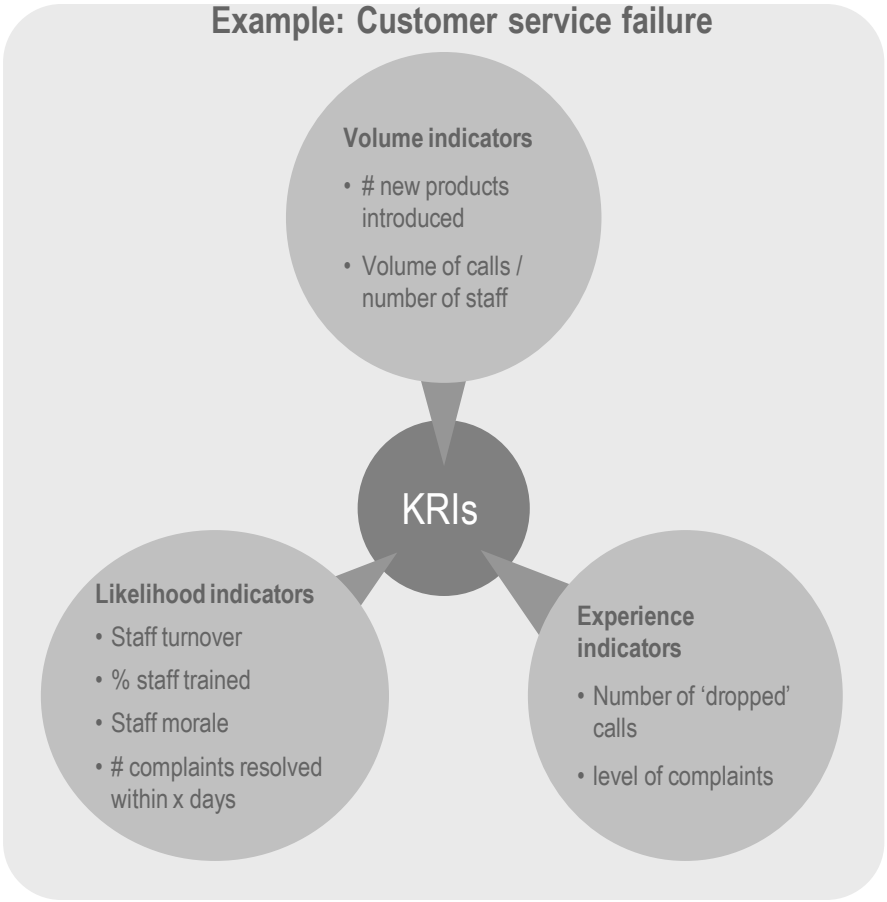
- **Leading indicators** are predictive in nature, i.e. if a predefined threshold is breached it points towards an issue occurring in the future.

- **Lagging indicators** are useful when they are reported frequently so that corrective action can be taken quickly if necessary. Lagging indicators can also be **predictive** when reported over time, thus enabling trending and indicating whether exposures are increasing to an extent that may breach threshold.

KRI Design Principles
Forming a Balanced View

A helpful method for considering the inclusion of indicators. NB. Experience indicators (defined below) may commonly be lagging indicators, volume and likelihood indicators will commonly be leading indicators.





KRI Design Principles
Choosing The Best Risk Indicators

1. **Confirm to key risks –** KRIs should be linked / restrictedto the largest potential risk exposures
2. **Break key risks into risk components –** risks are often comprised of a number of components which have different causes and impacts
3. **Consider the rationale for picking indicators of the risk –** document what is likely to cause a risk and how it is likely to manifest itself
4. **KRI selection –** a mixture of high-quality leading and lagging indicators
5. **Threshold calibration –** Leverage FTR / error rates and other management approved metrics for threshold calibration and objective back testing

Tracking all possible KRIs and re reporting of certain metrics is a major contributor to these challenges.

KRI Setting

- **KRI Setting Examples**

Key Risk	Risk Component	Rationale for indicator	Key risk Indicator
Ineffective business processes, fragmented systems, and decentralized technology infrastructure results in inconsistent financial, business, and risk management data and inconsistent, inaccurate reporting.	1) Ineffective business processes	**Leading:** - Processes are not documented **Lagging:** - Process errors	- Example 1: percentage of up-to-date procedure documents that are in place for key processes - Example 1: Errors as a percentage of processing transactions

KRI Setting

Key Risk	Risk Component	Rationale for KRI	Key risk Indicator
Default Risk of financial loss due to an issuer, counterparty, or borrower failing to fulfill its obligations.	**Borrower Credit Profile** The ability of a borrower to repay a loan, including debt to income, cash flows, and collateral.	**Leading:** New loans are issued based on the credit profiles of the borrowers, including credit rating which is predictive of the ability to repay. **Lagging:** Defaults can be predicted as loans enter delinquency. While some delinquent loans are paid current, an increase in delinquency rate or dollars may indicate future defaults.	**Example 1:** Weighted Average Credit Rating of New Loan Originations **Example 3:** 12-month rolling average flow rate (new $ delinquent 1-30 days)

KRI Leading Practices
Attributes of a Good KRI

- Key Risk Indicators are either ***indicators* for *key* risks (direct linkage) or *key* (good) *indicators* of risks**; the best KRIs are both.

- It is good practice to **document the rationale for linking KRIs to the risks**, indicating what types of data are likely to be a leading indicator, and what types lagging.

- To make an indicator better, a **percentage or ratio** will enable comparability between periods, departments, regions, and business units.

- **Filtering out noise** in KRI data can increase the correlation of the indicator to the risk. As KRIs are **indicators of a change** in exposure to risks, they do not need to be as complete as they would if they were performance metrics.

- **More volatile KRIs** should be constantly monitored for spikes, so that action can be taken immediately. KRIs should not just be reported in line with reporting timeframes but used by the business to actively manage risk.

KRI Ownership, Monitoring, Reporting, and Escalation

Reporting

- Established on a frequency consistent with the velocity of the risks being monitored, and the lag times between management action and a reduction in risk.
- Reported only for key risks. Too many KRIs will not provide a clear picture of how well risks are being managed.
- Reported in relation to the defined thresholds and with trending information to ascertain risk direction and volatility.
- Easy to understand and consistent. Commentary should be included to explain areas of exception, correlations, and interpretation of data presented.

Escalation

- Escalation protocols and timeframe requirements for escalation, must be clearly defined.

Monitoring

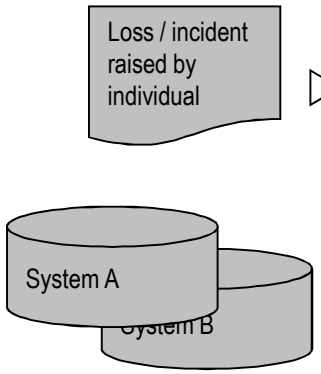
- Frequent or continuous monitoring by the business as needed.
- Formal reporting should be implemented to the Enterprise Risk Committee or other risk committee.

Ownership

- KRI owners should be established and responsible for reporting on KRI.
- KRI owners should be the risk-takers, as risk-takers are those individuals who will also be primarily responsible for taking action to reduce risk.
- Risk-takers owning KRIs and KRI reporting helps establish a strong risk culture.
- A risk monitoring and control function should review KRI reporting and assess it for validity and challenge the commentary, risk decisions, and actions of KRI owners.

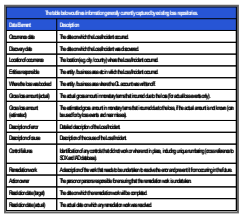
3 Incident and Loss data management
Key elements

Collation of Losses/incident



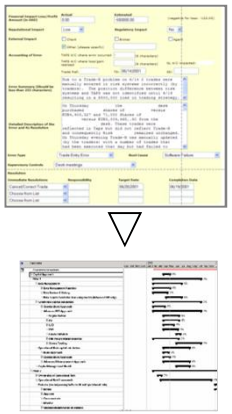
- Records of events in production systems are identified.
- Events not captured in production systems are discovered and raised.
- Ownership established.

Data Elements



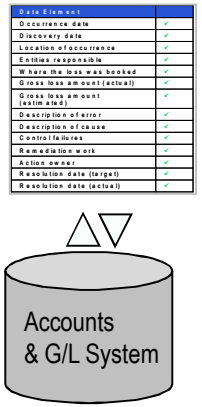
- Scope and collection standards agreed.
- Consistent data elements captured
- Field structure supports data collection.
- Data dictionary in place.
- Pick list options agreed.

Recording & Categorisation



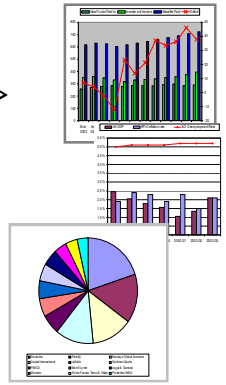
- Loss or incident events recorded in a data repository.
- Attributed to the correct GL code / cost centre.
- Risk category assigned.
- Remediation work planned.

Approval & Reconciliation



- Events approved by Business Area management.
- Events reconciled to the GL where possible.

Reporting



- Operational risk events reported to management within Business Area
- Provide loss/incident information as required by the Firm.

Data Considerations

	Data Element	Description
When	Occurrence date	The date on which the Loss/Incident occurred.
	Discovery date	The date on which the Loss/Incident was discovered.
	Resolution date (actual)	The actual date on which any remediation work was resolved.
	Recovery date	The date on which any recovery amount was realised.
	Date of write off	The date on which the Loss/Incident was written off.
Where	Location of occurrence	The location (e.g. city / country) where the Loss/Incident occurred.
	Entities	The entity / business area etc in which the Loss/Incident occurred. / Basel business line
	Where the loss was booked	The entity / business area / cost centre where the GL account was written off.
Why	Description of error and cause	Detailed description of the Loss/Incident including contributory causes
	Control failures	Identification of any controls that did not work or where not in place, including unique numbering (cross reference to RCSA / ICOFR and IAD database).
	Remediation work	A description of the work that needs to be undertaken to resolve the error and prevent it from occurring in the future.
	Market / Credit risk flag	Highlights that the Loss/Incident was the operational risk component of a credit or market risk loss or near miss.

Data Considerations (cont.)

	Data Element	Description
How much	Gross loss amount (actual)	The actual gross amount in monetary terms that incurred due to the loss (for actual loss events only).
	Gross loss amount (estimated)	The estimated gross amount in monetary terms that incurred due to the loss, if the actual amount is not known (can be used for by loss events and near misses).
	Recovery amount	The monetary amount that was recovered following discovery of the Loss/Incident. And Insurance classification
	Net Loss	The net loss after accounting for any and permissible recovery amount.
Which	Loss/Incident Type	This flag will identify whether the Loss/Incident that occurred was a loss, gain or near miss event and whether it was a cash outflow/inflow or an accounting adjustment.
	Account write off	The accounting entries for the write-off.
	Information source	This field will capture whether it was an internal Loss/Incident, information entered from a public source or competitor loss information.
	Basel II – Event type	The Basel II Level 1 risk category that can be attributed to the near miss or loss.
	Recovery type	The reason for recovery.
Who	Action owner	The person or persons responsible for ensuring that the remediation work is undertaken.

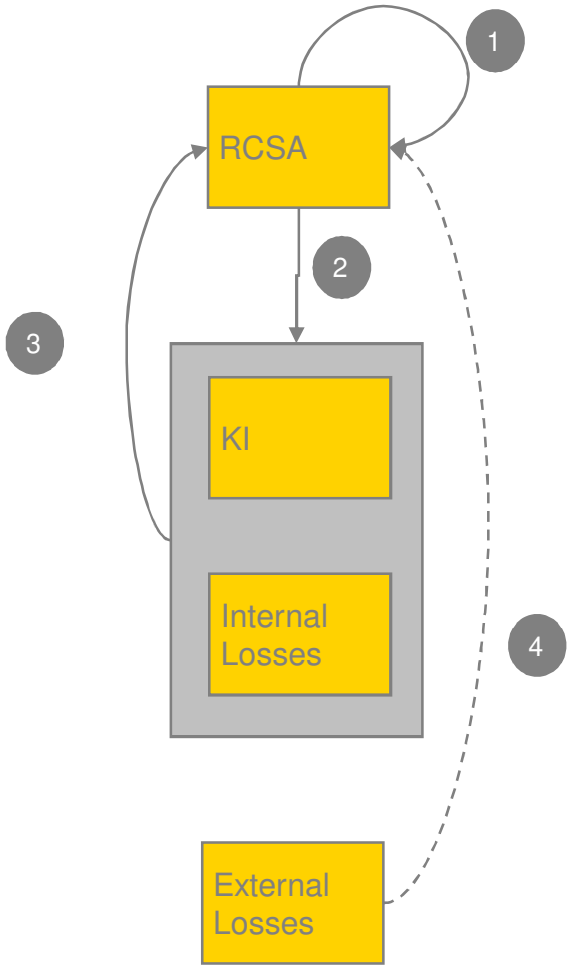
4 Insurance as risk mitigants

Requirements and considerations

Sno	Areas	Description
1	Rating of the provider	Minimum of A or equivalent
2	Recognition limitation	20% of OR capital
3	Term	Initial, residual and haircuts
4	Notice period	Cancellation of 90 days.
5	Stakeholders	Re insurance
6	Uncertainty	Time difference and contractual obligations
7	No leading practices- Not a common decision	Only 25% of AMA banks* reported insurance-related capital offsets of more than 4% of total operational risk capital
8	Resiiducal credit risk	The credit risk associated with the failure of the provider, to some extent is mitigated by A rating requirements but there is potential residual risk.

* *2009* Basel range of practice survey notes

5 Interplay between Key OR Elements in the Target Operating Model



In a well functioning operating model each of the key elements of operational risk plays an important role in continually re-enforcing the effectiveness and efficiency of a solid OR framework.

1 Periodic RCSA (including scenario analysis in a more advanced stage) helps identifying the effects of changes in the business model or changes in the environment on the range of meaningful risks and the effectiveness of controls.

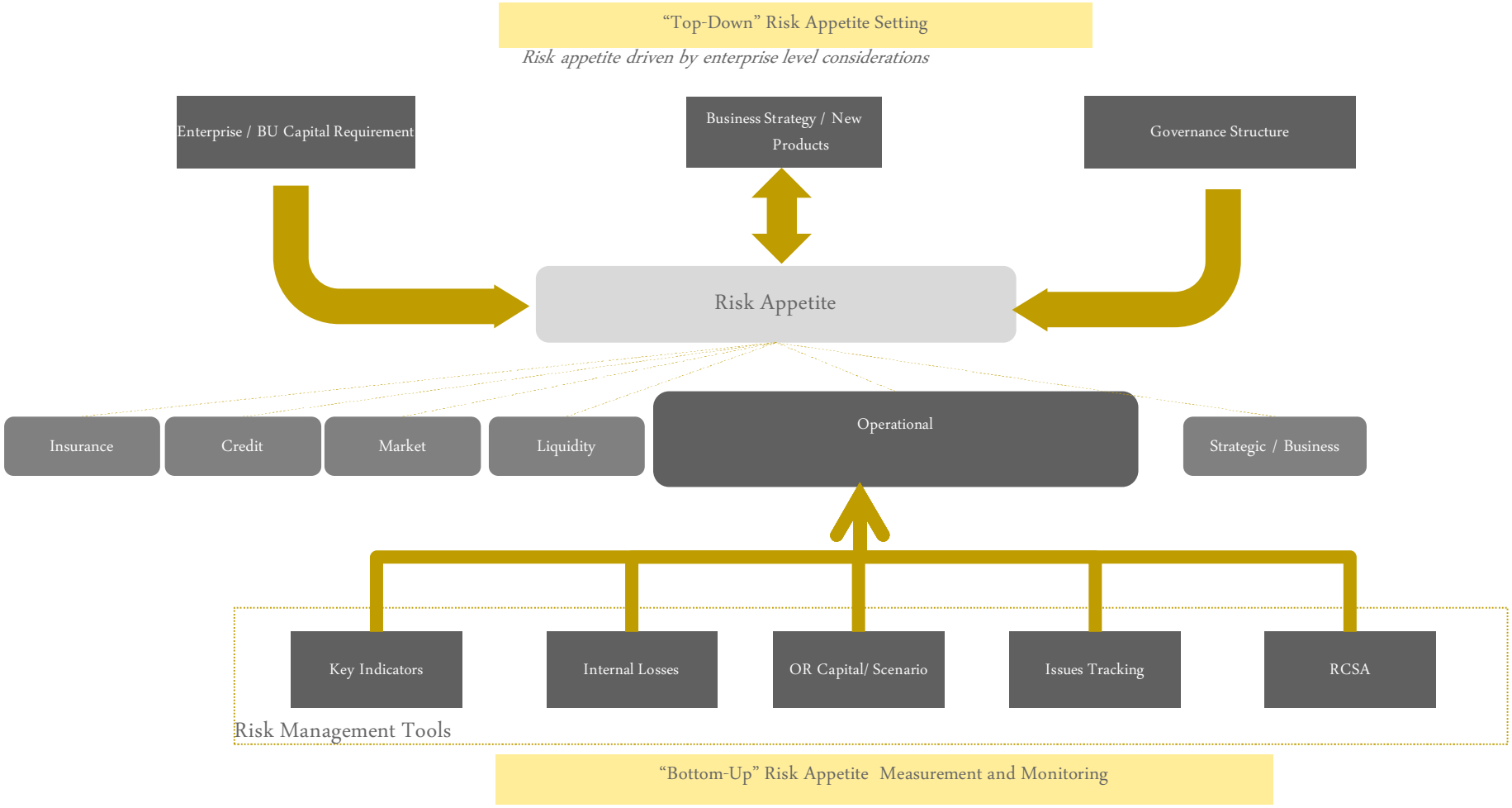
2 Through an RCSA the relevance of indicators and loss categories can be determined and improved which allows the organization to use KI and loss collections for continuous process and control improvements

3 Performance of KI's and loss experiences are not only used for monitoring purposes but can be fed back to verify and improve the RCSA process

4 External losses support advanced measurements of capital. They also can be used to challenge RCSA's (and scenarios) by questioning whether risks and controls sufficiently cover rare but possible cases.

OR Elements and Risk Appetite

Top down appetite setting and bottom up measurement



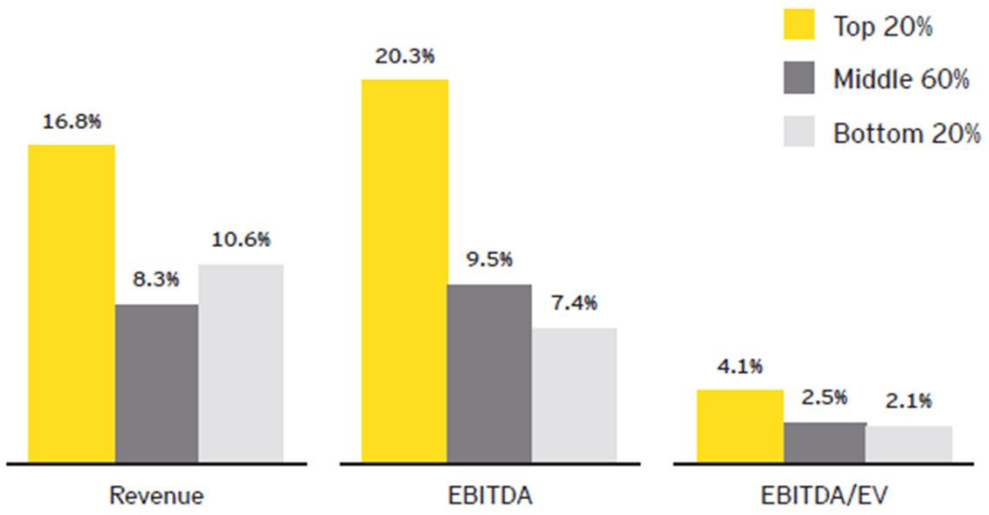
Operational Risk appetite is monitored and measured by various framework components including KRIs

5 Impact of successful risk management process

EY Global Survey – Insights and results*

- In our extensive experience with our clients, we see that companies with more mature risk management practices outperform their peers financially. Our research suggests this translates to competitive advantage: we found that companies with more mature risk management practices generated the highest growth in revenue and EBITDA

Compound annual growth rates 2004-11 by risk maturity level



* *EY Global Survey released in 2012*

Summary of key findings:

- *The top-performing companies (from a risk maturity perspective) implemented on an average twice as many of the key risk capabilities*
- *Financial performance is highly correlated with level of integration & coordination across risk, control and compliance functions*
- *Effectively harnessing technology to support risk management is the greatest weakness or opportunity for most organizations*

Where companies are looking to drive results

Companies achieve results in three interrelated ways

82%

of institutional investors are willing to pay a premium for effective risk management

(Source: Ernst & Young study)

Companies are overspending on risk and controls; most are overspending by approximately

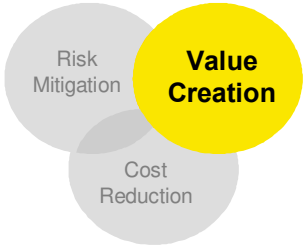
30%

3x

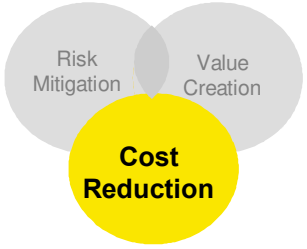
Companies in the top 20% of risk management maturity delivered three times the level of EBITDA than the bottom 20%.

(Source: Turning risk into results, Ernst & Young,)

- *Identifying and understanding the "risks that matter"*
- *Differentially investing in the risks that are "mission critical" to the organization*
- *Effectively assessing risks across the business and driving accountability and ownership*
- *Demonstrating the effectiveness of risk management to investors, analysts and regulators*



- *Achieving superior returns from risk investments*
- *Accepting and owning the right risks to achieve competitive advantage*
- *Using analytics to optimize the risk portfolio and improve decision-making*
- *Using risk management savings to fund strategic corporate initiatives*



- *Implementing a new risk operating model to materially improve the cost structure*
- *Reducing cost of control spend through improved use of automated controls*
- *Streamlining or eliminating duplicative risk activities*
- *Improving process efficiency through automated centers and continuous monitoring*

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young is a leader in serving the global financial services marketplace
Nearly 35,000 Ernst & Young financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, Ernst & Young is the only public accounting organization with a separate business unit dedicated to the financial services marketplace.

Ernst & Young professionals in our financial services practices worldwide align with key global industry groups, including Ernst & Young's Global Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, Ernst & Young's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

It's how Ernst & Young makes a difference.

Ranked as the Number 1 professional services brand in India — Global Brand Survey 2013, conducted by TNS
Ranked as Number 1 for OR services for four years running - Operational Risk & Regulation

ERNST & YOUNG
Quality In Everything We Do