

# Applying the Best Practice of Operational Risk Management in Technology and Operations

By Dominic Wu,

Managing Director & Senior Risk Manager,  
Financial Markets and Treasury Services, APAC

The Bank of New York Mellon

## Agenda

- Current risk vulnerabilities in Technology and Operations Landscape
- Conduct effective Risk Control and Self Assessment
- Build up useful Key Risk/Performance Indicators
- Perform out-of-the box Risk Analysis
- Produce a Risk Heat map



*"Sexual Harassment is never pretty."*

*"Stop it, before it gets ugly."*

c. 2002 [www.ideasandtraining.com](http://www.ideasandtraining.com)



the recent spate of card-skimming cases involving DBS ATMs at Bugis Street.

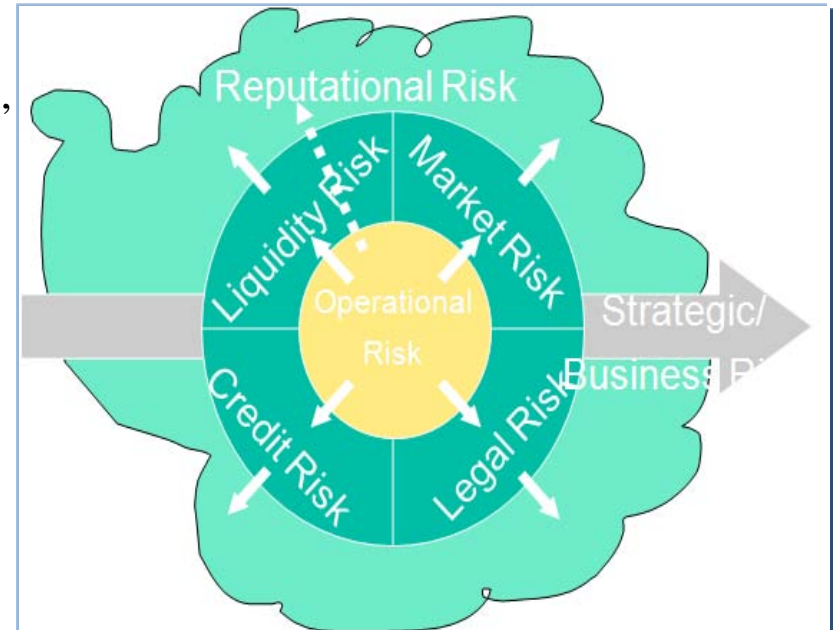
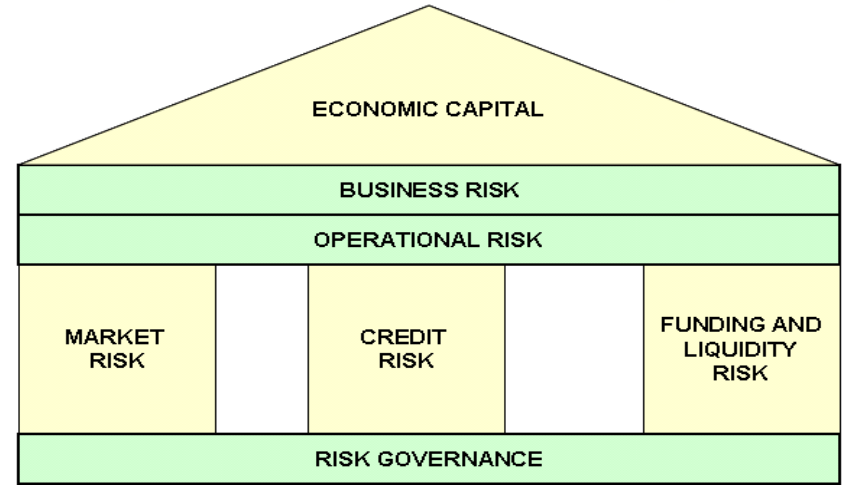


## What types of risk do we experience?



# Definition of operational risk

- “The risk of loss resulting from inadequate or failed internal processes, people and systems or external events”
- International Convergence of Capital Measurement and Capital Standards: A Revised Framework. BIS (2004)
- Everything that is not market risk or credit risk
- Lack of control over operational risk can lead to other risks
- ORM also practice in military, transportation, medical, industries have low tolerance of error



## What do these risk types mean?

### Operational Risk

- Is the risk of loss from inadequate or failed internal processes, people and systems, as well as from external events.

### Reputational Risk

- covers the risk to the firm's brand and relationships which do not arise out of any contractual obligation

### Technology Risk

- is the risk of business disruption due to systems failures

### Information Risk

- is the risk arising from the failure to uphold confidentiality of the client or the firm's information

## How would these risks materialise?

### Operational Risk

- Processing client instructions incorrectly
- Delivering securities to the wrong account
- Not completing reconciliations correctly

### Reputational Risk

- Failure to process a payment correctly leads to customer dissatisfaction

### Technology Risk

- A system failure means we are unable to process payments

### Information Risk

- Failure to follow a clear desk policy - confidential documents left lying on your desk.
- Sharing your password with another employee giving them access to information which they are not authorized to view.

## Basel Risk Event Categories

Risk Event Type (Level1)	Definition	Risk Event Type (Level 2)
<b>Internal Fraud</b>	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party.	<ol style="list-style-type: none"> <li>1. Theft And Fraud (Internal)</li> <li>2. System Security Breach (Internal)</li> <li>3. Unauthorised Activity</li> </ol>
<b>External Fraud</b>	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.	<ol style="list-style-type: none"> <li>4. Theft and Fraud (External)</li> <li>5. System Security Breach (External)</li> </ol>
<b>Employment Practices and Workplace Safety</b>	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/ discrimination events.	<ol style="list-style-type: none"> <li>6. Diversity and Discrimination</li> <li>7. Strained Employee Relations</li> <li>8. Unsafe Workplace Environment</li> </ol>
<b>Clients, Products &amp; Business Practices</b>	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	<ol style="list-style-type: none"> <li>9. Improper Advisory Activities</li> <li>10. Improper Customer Selection, Sponsorship &amp; Exposure</li> <li>11. Improper Business or Market Practices</li> <li>12. Product Flaws</li> <li>13. Suitability, Disclosure &amp; Fiduciary Breach</li> </ol>
<b>Damage to Physical Assets</b>	Losses arising from loss or damage to physical assets from natural disaster or other events.	<ol style="list-style-type: none"> <li>14. Disasters and Other Events</li> </ol>
<b>Business Disruption, System Failure</b>	Losses arising from disruption of business or system failure	<ol style="list-style-type: none"> <li>15. Infrastructure Failure</li> </ol>
<b>Execution, Delivery &amp; Process Management</b>	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.	<ol style="list-style-type: none"> <li>16. Inadequate Customer Documentation</li> <li>17. Failed Customer Account/Record Management</li> <li>18. Failed Transaction Processing</li> <li>19. Failed Regulatory Reporting</li> <li>20. Trade Counterparty Disputes</li> <li>21. Failed Vendor/ Supplier Management</li> </ol>



## Common Risk Casual Categories

Cause categories	Definition
<b>Processing</b>	The risk of losses from failed processing due to mistakes, negligence, accidents or fraud by directors, staff within the organization and external party.
<b>IT</b>	Inadequate IT strategy, IT policies or standards or shortcomings in the application of IT
<b>External disruption</b>	Unanticipated / uncontrollable factors external to the organisation, disrupting the bank's operational capability. In case insufficient or failing controls are the cause of the event, the cause should be classified as such
<b>Legal</b>	A description of the potential for loss arising from the uncertainty of potential and actual legal proceedings
<b>Compliance</b>	The risk of impairment to the organisation's business model, reputation and financial condition resulting from the failure to meet laws and regulations and internal standards and policies and expectation of key stakeholders
<b>People</b>	Insufficient management of human resources and/or poorly performing staff
<b>Information</b>	Inadequate information or inappropriate use of information
<b>Organisation</b>	An ambiguous or inadequate organisational setup, including the associated responsibility, accountability and governance structure

## What are the recent risk vulnerabilities?

- **Internal factors**
  - Inability to handle increasing volume with existing capacity
  - New business/product
  - Fat finger
  - Staff attrition
  - Lack of investment on controls
  - Retention of knowledge due to restructuring
  - Clearance of backlog especially on trade confirmations for OTC
  - Service/product misselling
  - Inadequate due diligence on counterparty – e.g. hedge fund
- **Internal governance**
  - Risk of going back to complacency and risk excessive taking
- **External factors**
  - Delay of discovery of rogue/unauthorised trading
  - Adjustment to new accounting standards
  - Change of regulation
  - Readiness for major market adjustment or W-shape adjustments
  - Retreat of quantitative easing
  - Prepare for next bubble burst (i.e. property, currency, commodity)
  - Business resilience

## Factors contributing to operational risk in the Financial Space

- **High frequency trading / Dark pool trading**
  - Incorrect trade execution
  - Market manipulation
  - Inadequate robustness and capacity of technology platform
- **OTC derivatives clearing**
  - Absence of ISDA and long form confirmation, tendency to go for market standardisation
  - Lack of internal pricing mechanism
  - Outstanding and unsigned confirmation
  - Inadequate and lack of standards in Straight-Through-Processing (STP) across markets
  - Inadequate and ineffective collateral management
  - Pressure to adhere to commitment on Fed letter and central clearing
- **Collateral and valuation**
  - Inaccurate calculation
  - Manual process
  - Inadequate forward looking capability on counterparty exposure
  - Majority of participants do not rehypothecate securities collateral
- **Bond trading**
  - Increasing cross border linkage leading to difficulties in contracts setting and clearing
  - Inadequate readiness of technology
- **Outsourcing**
  - Inadequate monitoring and lack of accountability
  - Inability to maintain the service level
- **Managing regulatory changes**
  - Increasing regulatory scrutiny, reporting and capital requirements
  - Increasing co-ordination and share of information among the Regulators/Exchange

## Samples of major prominent operational risk events

Global Market	Severity	Asset Management/Internal Hedge Fund	Severity
- Improper business practice	High	- Manager fraud	Tail
- Misselling of products and inadequate disclosure	High		
- Breach of fiduciary duties	Tail	Operations	Severity
- Incorrect trade execution	High	- Wrong settlement	High
- Incorrect trade booking	High	- Incorrect static data	High
- Incorrect model set-up	High	- Errors in collateral and margin payments	High
- Unauthorised trading	Tail	- Incorrect reporting to clients	High
Legal & Compliance	Severity	- Inadequate customer documentation	High
- Litigation	Tail	- Non-adherence to policies and procedures	High
- Fine and discipline actions by the government	Tail	Technology	Severity
- Breach of regulation	High	- Improper system design and inadequate system solution delivery	High
- Violation of internal policies	High	- System outages	High
- Client complaint	High	- Business disruption event	Tail
		- Information security incidents	High

## Samples of major prominent operational risk events

Human Resources		Severity	Risk Management	
-	Employment related issues	High	-	Incorrect parameter into risk model
-	Incorrect payroll	High	-	Incorrect model design
Controller		Severity	-	Breach of risk limits
-	Significant accounting adjustment	Tail	Corporate Services/Corporate Security	
-	Wrong payment of office expenses	High	-	Theft of and damage to physical assets
-	Pricing and valuation errors	Tail	-	Accidents and injury
-	Incorrect financial return to regulator and	High	-	Corporate security incidents
-	Client complaint	High		

# Operational risk drivers in trade life cycle

High		High		Medium		Medium	
High		High		High		High	
High		High		Medium		Medium	
1. Processing risk	2. System risk	3. Business disruption risk	4. Legal risk	5. Compliance risk	6. People risk	7. Information risk	8. Organisation risk
Product complexity	Inadequate system solutions and product support	Inadequate contingency plan for major system outage	Accumulation of backlog of confirmation	Inadequate KYC	Inability to retain talents	Inadequate control over archived data	Inadequate knowledge and ownership of the process and the risk by
Manual processing/confirmation/reconciliation				Stricter regulation	Inadequate staff resources and back up plan	Leakage of sensitive information	
Increasing client requirements							
Cross border trading and support							
Untimely response to market event							
Reconciliations are not robust							

## Agenda

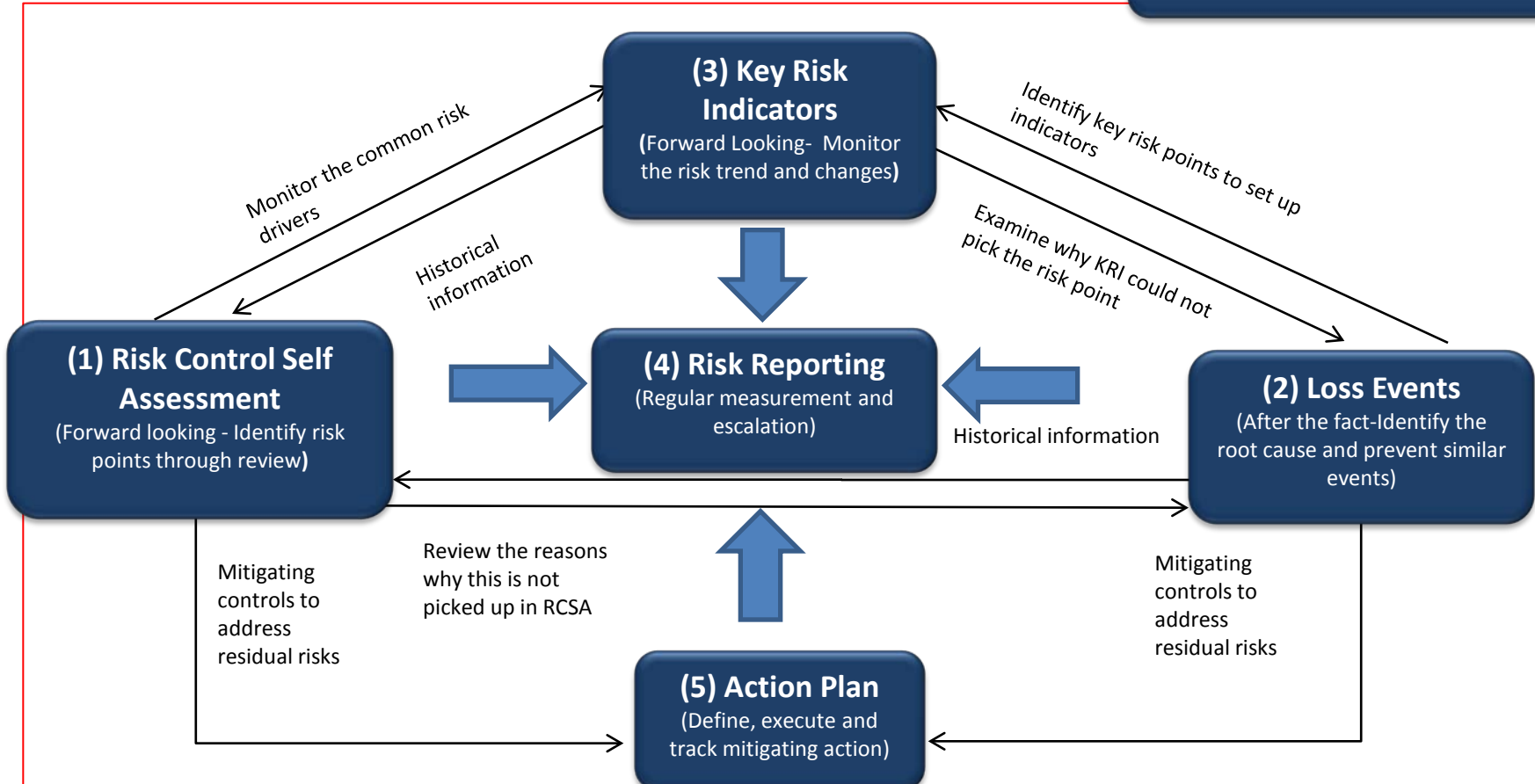
- Current risk vulnerabilities in Technology and Operations Landscape
- Conduct effective Risk Control and Self Assessment
- Build up useful Key Risk/Performance Indicators
- Perform out-of-the box Risk Analysis
- Produce a Risk Heat map

# Interaction between Risk Management Tools

Risk Governance Framework

Risk Appetite, Strategy, and Objectives

**(6) Scenario Analysis**  
(Thinking out of the box risk assessment)



Policy and Procedures

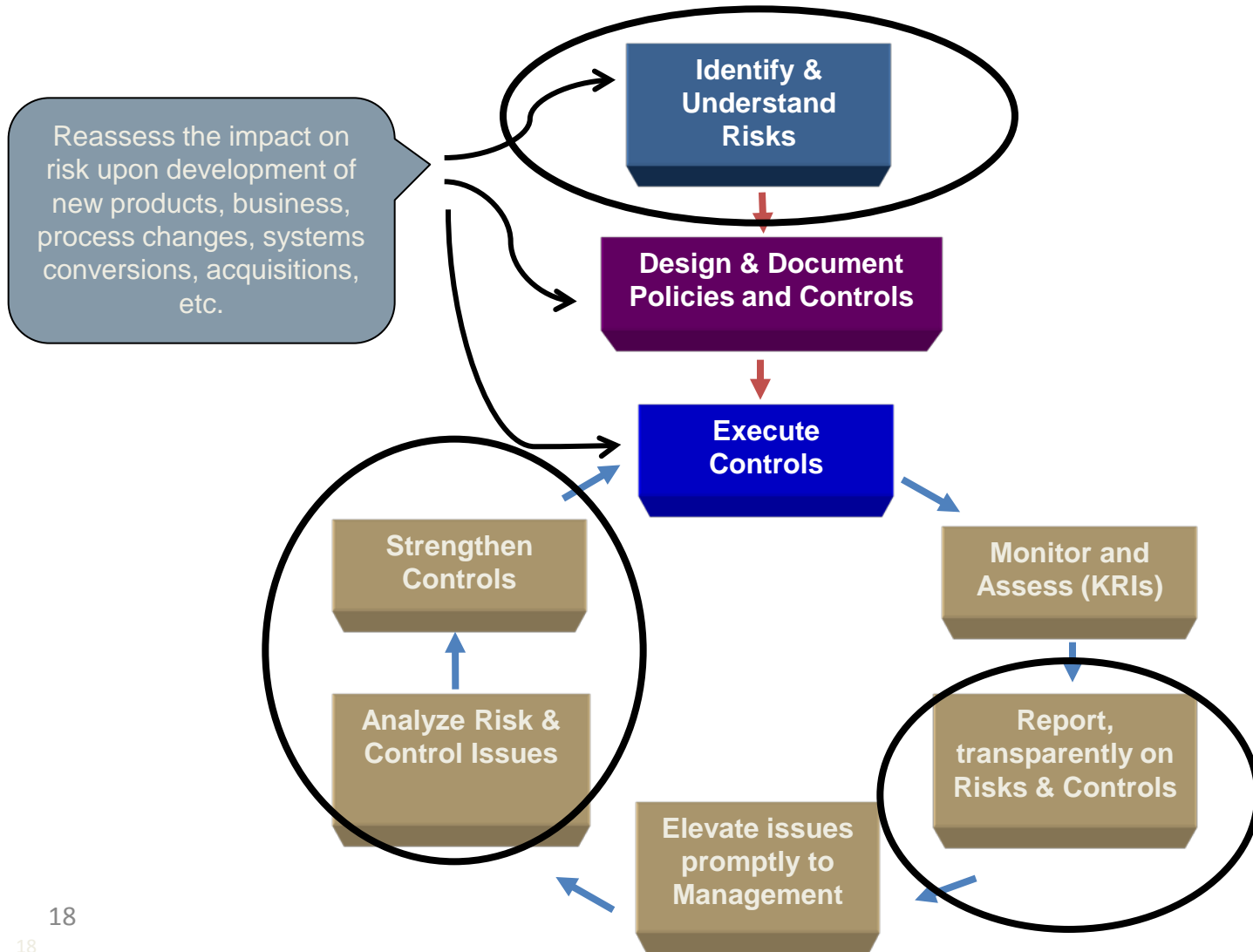
Corporate Governance and Organization



## Risk Control Self Assessment Overview

- It is a process to integrate and co-ordinate its risk identification and risk management efforts and generally to improve the understanding, control and oversight of risks
- Provides a systematic means of identifying control gaps that threaten the achievement of defined business or process objectives and monitoring what management is actually doing to close these gaps
- To formulate appropriate action plans to address identified control gaps, taking into account risk-reward (cost-benefit) considerations. With progress against these plans monitored as part of the overall risk management approach
- Promotes analysis and monitoring of factors that affect the level of risk exposure
- Acts as a complementary audit and management tool, as well as being the generally accepted means to satisfy corporate governance and regulatory requirements
- Key tool in sharing consistent and reliable risk information across the “Three Lines of Defense” i.e. Business, Risk and Audit so that a consistent risk profile could be derived
- Why is it important? RCSA can help the Firm and the Business to identify the risks and take remedial actions so as to
  - Protect reputation
  - Prevent losses
  - Minimize compliance and legal breaches
  - Improve the quality of service to clients

# Risk Management Framework Diagram



## Benefits

- It is a common language of risk information across the organization
- It enables better Enterprise Risk Management and aggregation of risk data
- It provides clear and specific ownership of action plans
- It enables open discussion of risk and control matters amongst staff and management, leading to better transparency and understanding of risk and its implications across the business
- It leads to cultural change, helping risk management to become embedded at all levels of the organization, with respect to both day to day activities and longer term business decision making
- It can demonstrate to Auditors and Regulators how risks are managed within the Business



## Roles and Responsibilities

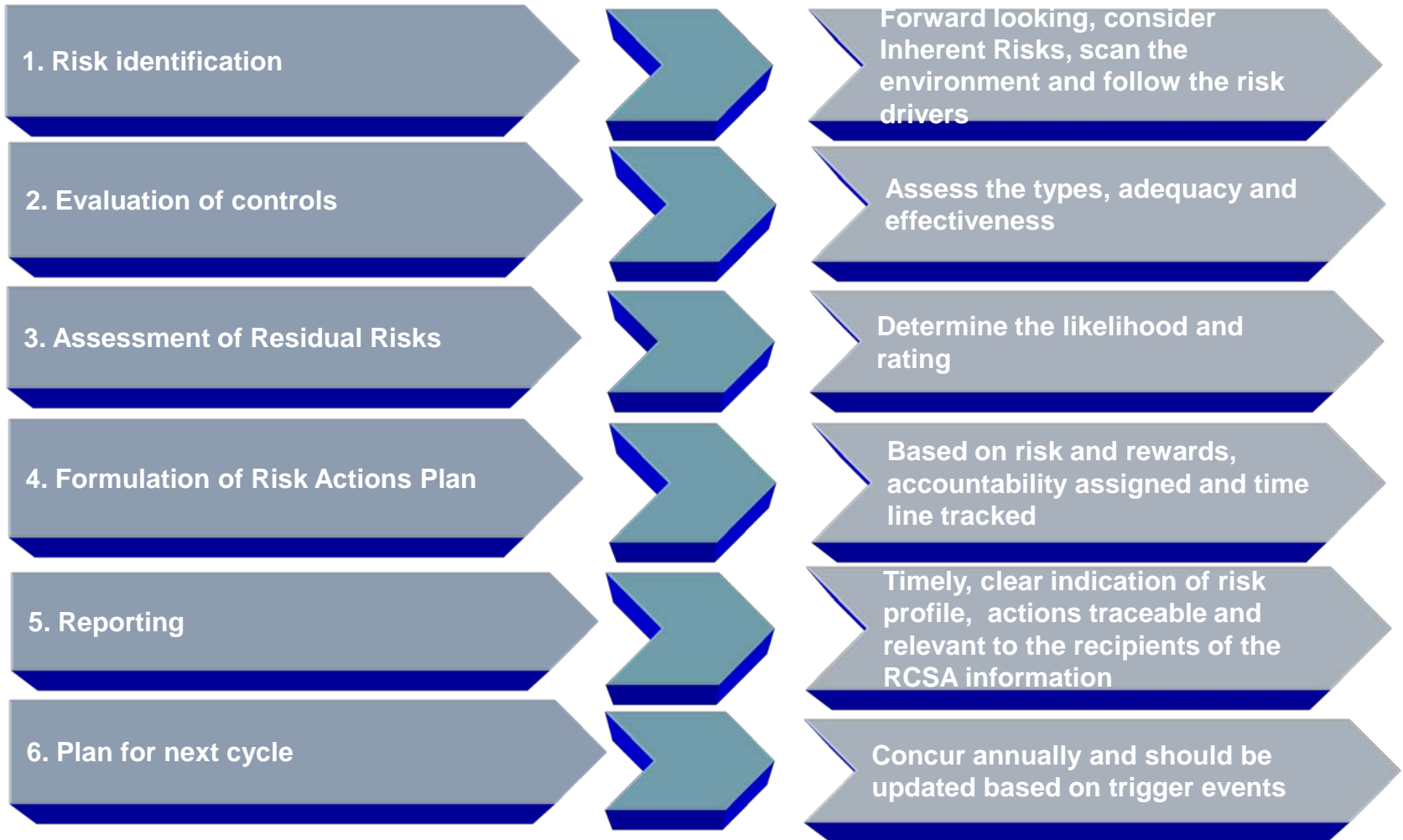
- **Business:**
  - Identifying and managing risk by implementing an effective control structure
  - Developing and maintaining an effective Risk and Control Self Assessment using the Risk Management Platform
  - Staff who is aware of risk issues should elevating to their Manager for input into RCSA
  - Ensure RCSA is updated on occurrence of a major loss event, new product or material change of process
- **Business Partner:**
  - Providing assistance and comments to facilitate the front-to-back assessment
- **Risk Management:**
  - Ensure that the Risk and Control Self Assessment accurately reflects the risk profile of the business and the content accuracy is concurred to by the Business or Business Partner Department Manager who owns the document on an annual basis.
  - Making sure the RCSA is updated by the process owner for process changes, poor audits, or major losses.
- **Regulators, Internal Audit and Control:**
  - Periodically review and test to validate adherence to policy
  - Leverage on the results of RCSA for planning and drawing conclusion on risk profile

## Components of RCSA

- The identification of business objectives, which can be defined either in terms of business targets or process delivery goals;
- The identification of risks that could threaten the achievement of those objectives and the activities and processes affected by the different risks identified;
- Identifying the controls in place intended to prevent the risks from crystallizing;
- Determining where responsibility for performing those controls lies; and
- An assessment of the effectiveness of the controls in operation and the level of residual risk remaining after control.
- Scope of RCSA can be defined in a way meeting the characteristics of the Firm and Business



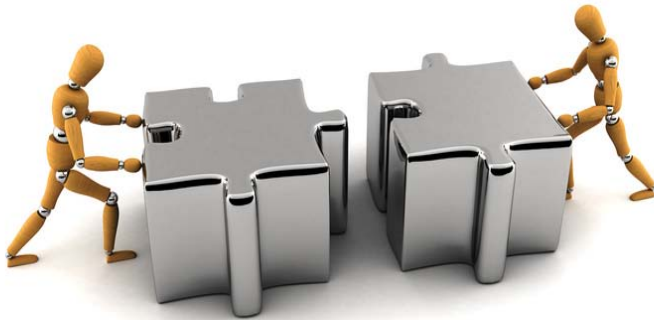
## How to Execute an RCSA



## Agenda

- Current risk vulnerabilities in Technology and Operations Landscape
- Conduct effective Risk Control and Self Assessment
- Build up useful Key Risk/Performance Indicators
- Perform out-of-the box Risk Analysis
- Produce a Risk Heat map

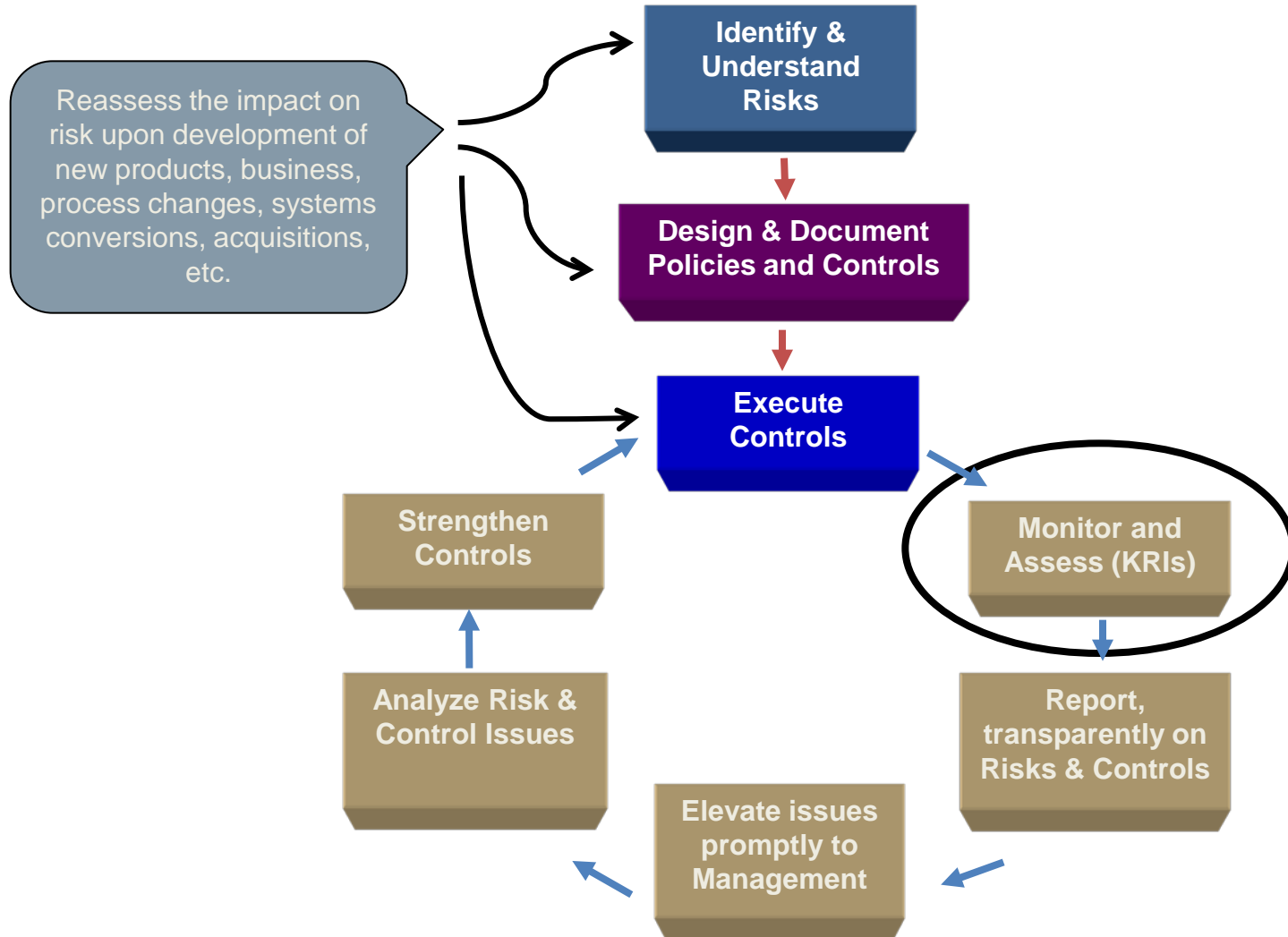
## Key Risk Indicators: Overview, Policy Requirements & Use



- KRI's are risk metrics used by the risk owner and Risk Management to monitor the health of the business and prevent financial loss, regulatory censure or client impact.
- KRI reporting can be implemented at all levels of the organisation, i.e. high level metrics tracking more material movements at the top of the house, or more granular, bottom up metrics useful for monitoring risks within a smaller functional unit.
- KRI's are owned and developed by the risk owner in conjunction with Risk Management. Metrics must be formally revalidated by the risk owner and Risk Management at least every 18 months.
- KRI reporting and monitoring must be performed on a monthly basis as a minimum. The risk owner is required to provide commentary describing the impact, the cause and the action plan for metrics that have breached the Red threshold.
- KRI results are reviewed with Senior Management at the Business Risk Committee and the Quarterly High Level Assessment Meetings.



# Risk Management Framework Diagram



## Roles and Responsibilities



- The Business are responsible for identifying their risks and developing Key Risk Indicators to monitor the effectiveness of controls and/or the level of residual risk.
- Risk management is a continuous process, KRI reporting and monitoring must be performed by The Business at least monthly and metrics revalidated at a maximum frequency of 18 months.
- Risk Management is responsible for the development of the KRI's in conjunction with Business Management and must concur that actions being taken to address red metrics are appropriate.
- Risk Management is responsible for ensuring that materially adverse conditions are reported and/or escalated to Senior Management.
- Regulators, Internal Audit and Control periodically review and test to validate adherence to policy.

## Effective Key Risk Indicators: Characteristics

- Most effective when used to generate exception reporting based on defined thresholds or tolerances, usually Red, Amber, Green rated (RAG).
- KRI thresholds/tolerances are a means of expressing risk appetite. Amber thresholds should be triggered when the metric is approaching a material level of risk, and red thresholds triggered when the metric has reached a material level of risk.
- Exceptions typically require additional commentary/explanation: Root Cause; Nature of Risk; Severity of Impact; Remedial Action and Target Resolution Date.
- Can be ‘Leading’ (measures risk drivers) or ‘Lagging’ (generally measures of crystallised risk).
- Useful in supporting, facilitating or driving business decisions.
- Quantitative/Quantifiable: \$, % or #.
- Can be benchmarked internally or externally.
- Timely (JIT) and practical.
- Measures cater for volume based spikes; relational measures.

## Spot The Difference: KRI's, KPI's and KCI's

### Performance Indicator

% of high risk tickler items closed within 15 days of due date

### Risk Indicator

Number of outstanding high risk tickler items >30 days

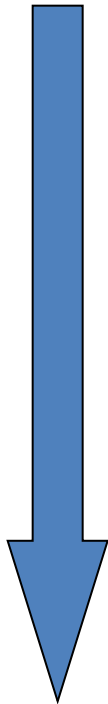
### Control Indicator

Number of missed tickler events identified after due date due to the absence of a tickler

- Often significant overlap, particularly where operational efficiencies also reduce risk or where business objectives are linked to the management of risk and control.
- Some metrics 'double up' as both performance and risk indicators (e.g. measures of STP, no. of audit recommendations past due date, value of operational losses).
- Where relevant the risk indicator is typically the inverse of the performance indicator in terms of what's being measured, e.g. % of Items within SLA vs % of Items outside of SLA.
- Important to remember that RAG thresholds for Risk Indicators should reflect risk appetite/tolerance, not BAU run rate or targeted performance level.
- Key Control Indicators (KCI's) are a subset of KRI's and measure the effectiveness of specific controls, e.g. Number of OFAC exceptions, not identified by the Firm and subsequently notified to the Firm by OFAC.

## KRI Examples: Leading vs Lagging

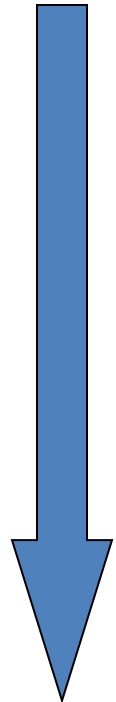
**Leading**



**Lagging**

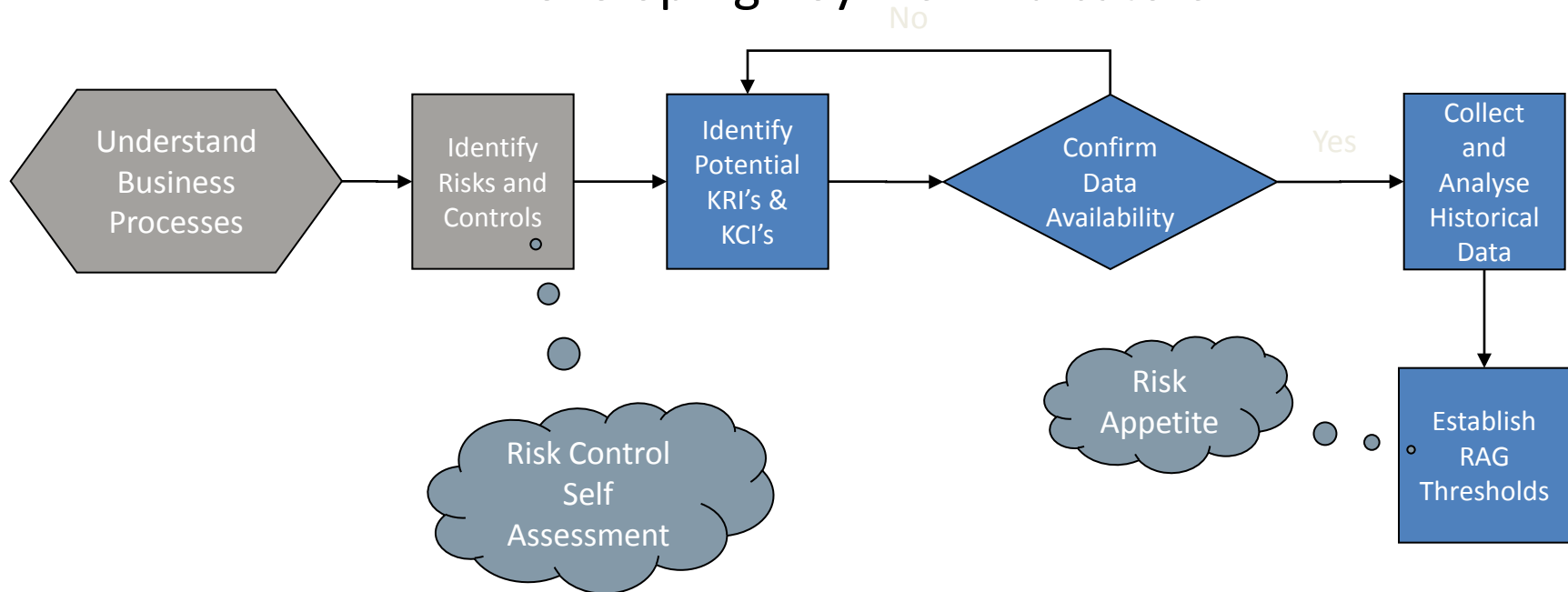
<b>Staff Turnover</b>	<b>Cash Payments</b>	<b>System Availability</b>
No. of Resignations in the month as a % of total FTE	Outgoing Cash Payments: % STP achieved (number of payments)	Inform system availability during committed service period (%)
No. of voluntary leavers in the month as a % of total FTE	Number of cash breaks as a % of rolling 4 week count of transactions	Average time taken to resolve high impact system outages in the month
Rolling 3 month count of all leavers as a % of total average month end FTE	Number of cash breaks >\$50,000 and >30 days old	Number of high impact system issues reported in the month
Rolling 12 month count of voluntary leavers as a % of total average month end FTE	Number of failed/late payments resulting in a cost to the Bank	Rolling 12 month count of high impact system issues

**Drivers of Risk**



**Crystallised Risk**

## Developing Key Risk Indicators

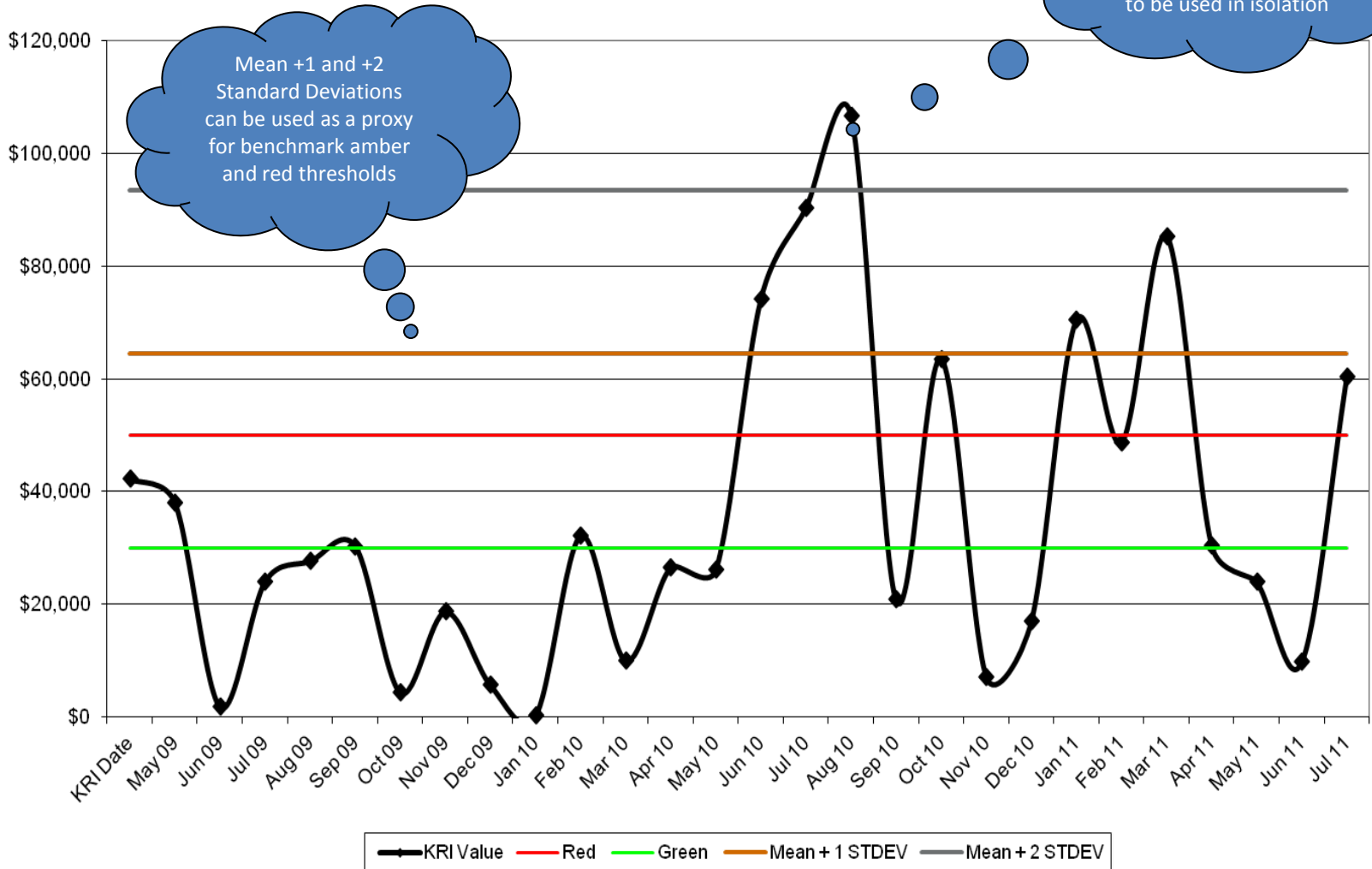


### Notes:

- Look to map metrics to key risks, but don't automatically exclude metrics that aren't captured in your RCSA.
- When setting RAG thresholds keep in mind your appetite/tolerance for risk, not what you want to see from a performance perspective.
- Effective exception reporting relies on amber and red thresholds only being triggered when there is a material exception.

# Setting Thresholds: Historical Data

\$ Value of Fee Receivables > 180 Days



## Agenda

- Current risk vulnerabilities in Technology and Operations Landscape
- Conduct effective Risk Control and Self Assessment
- Build up useful Key Risk/Performance Indicators
- Perform out-of-the box Risk Analysis
- Produce a Risk Heat map



## Definition and Objective

- Definition and background
  - A simulation technique used on asset and liability portfolios to determine their reactions to different financial situations. Stress tests are also used to gauge how certain stressors will affect a company or industry. They are usually computer-generated simulation models that test hypothetical scenarios (Investopia)
  - A stress test is commonly described as the evaluation of the financial position of a bank under a severe but plausible scenario to assist in decision making within the bank. The term “stress testing” is also used to refer not only to the mechanics of applying specific individual tests, but also to the wider environment within which the tests are developed, evaluated and used within the decision-making process (Basel)
  - Alerts bank management to adverse unexpected outcomes related to a variety of risks and provides an indication of how much capital might be needed to absorb losses should large shocks occur
  - Supplements other risk management approaches and measures
- Objective
  - To obtain forward looking assessments of risk;
  - To overcome the limitations of models and historical data (or the lack of it);
  - To support internal and external communication about potential future business states;
  - To feed into capital and liquidity planning initiatives;
  - To inform the setting of risk appetite and tolerance
  - To facilitate the development of risk mitigation or contingency plans across a range of possible areas and potential business states.

## Types

It can be split into simple sensitivity tests (SST) & scenario analysis (SA)

- SST explores changes to a portfolio's value following a change in one risk factor, for example interest rates. It is a very simple yet effective way of flagging up major deficiencies and weaknesses in a portfolio. The SST is frequently used by smaller banks and institutions as well as private investors. The drawback of this technique is that it is not plausible that just one variable should change—a massive increase in US interest rates, for example, would have a massive effect on exchange rates and equities
- SA takes into account a wide range of possible variables such as exchange rates, equity prices, and interest rates, and extrapolates possible outcomes and their probabilities. The process is not dissimilar to forecasting the weather—like the weather, a financial forecast is susceptible to change and must be repeated regularly

## Consideration

- Build them in conjunction with other techniques used in the business such as forecasting
- Data can be obtained from applying the developed stress tests to the firm's existing operational risk register, indicators and loss database. For example, by considering how the identified risks and controls will change in a given stress test a new stressed risk register is produced for that particular stress test. Consideration of the operational risk indicators and existing losses for the same stress test will yield a complete set of initial operational risk data for that test
- Check internal consistency within each stress test and comparability over the full set of tests
- The mathematical models used for generating stress test results can be the same as the models used for capital calculation. A range of values will be produced which will give an insight to the sensitivities of the firm to a variety of extreme operational risk events
- Consistent with the firm's business forecasts and that give valuable data to senior management to allow further and better understanding of the firm's operational risk profile. Given a perceived increase in the risk of disruption to the operation of firms from global pandemics, terrorist attacks or natural disasters it is vital that firms carry out stress tests involving their operational risks as well as their market and credit risks

## Consideration

- Stress test should be conducted at least quarterly. Able to capture new operational characteristics. Less frequent stress testing may be appropriate for operations with a low risk profile
- It should examine the effects and impact that different time horizons for measuring operational risk will have on business plans, strategic risks and future operating requirements.
- Various individuals such as Risk Managers, Finance and Business Management should be involved in designing and analysing the stress testing
- Understand the assumptions and make use the results for strategic planning and contingency planning

# Components

- Scenarios
  - What kind of Operational Risk would happen under “Economic Recession + Market Fluctuation + Existence of Credit Risk”
  - External typical events and internal historical data should be considered for scenario made of above assumption.
  - Independent scenario vs historical scenarios
  - Select some unrelated scenarios max 4 for each quarter
  - Business line affected
  - Subject
  - Act
  - Duration
- Reference and assumptions
  - State the reference both internal and external
  - Document the factors of consideration
  - Basis of computation
  - Quantify the impact
    - Financial
    - Regulation/Legal
    - Servicing to clients
    - Reputation
    - Staff safety
  - System tools
  - Capital modeling/ Monte Carlo Simulation
  - Simple analysis matrix
  - Results
  - Distribution of the result to division level
  - Impact on economic capital
  - Amendment to Operational risk appetite

## Overview of the current risk drivers

- Internal factors

- Inability to handle increasing volume with existing capacity
- New business/product
- Fat finger
- Staff attrition
- Lack of investment on controls
- Retention of knowledge due to restructuring
- Clearance of backlog especially on trade confirmations for OTC
- Service/product misselling
- Inadequate due diligence on counterparty – e.g. hedge fund
- Risk of going back to complacency and excessive risk taking

- External factors

- Delay of discovery of rogue/unauthorised trading
- Adjustment to new accounting standards
- Change of regulation
- Readiness for major market adjustment or W-shape recession
- Retreat of quantitative easing
- Prepare for next boom and burst (i.e. property, currency, commodity)
- Business resilience

## Common Scenarios

- Independent scenario
  - Counterparty fraud
  - Miselling of complex products
  - Rogue trading
  - Regulatory sanction on business
  - Collective employment litigation
  - Collective client litigation
  - Significant position mismarking
  - Massive leakage of sensitive firm/client information
  - Major business disruption
- Historical scenarios (from internal database)
  - Insider trading
  - Major system breakdown
  - Staff layoff
  - Company scandal

## Example 1

Event	Particulars	Remarks
<b>Type of scenario</b>	<b>Unauthorised trading</b>	Real independent event
<b>Scenario details</b>	Happen in Delta One trading in Equities	Real independent event
	By a Senior Trader without union who has good knowledge in the process and control	Real independent event
	Circumvent the control in middle and back office	Contributing factor
	Last for 6 months	Real independent event and judgement
<b>Reference</b>	(1) Fitch First Database (2) Trade volume and p/l flash	
<b>Assumption</b>	Process 1,000 trades each month	By the Business by referencing to average transaction handled by a trader
	Average nominal size is USD10MM	By the Business by referencing to average notional
	Lost 50% on each trade	By the Business and Risk Management
<b>Frequency</b>	Once a year	By Risk Management by referring to external database
<b>Estimated financial impact</b>	USD5,000M	Simple calculation by Finance
<b>Components of financial impact</b>	Direct and indirect loss in unwinding unauthorised trades	
<b>Other impact</b>	(a) Regulation / Legal: High (b) Servicing to client: Medium (c) Reputation: High (d) Staff safety: Low	
<b>Action</b>	(1) To conduct similar analysis for other lines of business (2) To review the internal control over trade cycle to minimise the occurrence and magnitude of impact (3) To arrive a common view of the deficiency of the capital in medium term	



## Example 2

Event	Particulars	Remarks
<b>Type of scenario</b>	<b>Investing counterparty fraud</b>	Real independent event
<b>Scenario details</b>	Happen in Merchant Banking	Real independent event
	A Senior Management had stolen the company monies, run away and results in liquidity problem	Real independent event
	Inadequate due diligence and monitoring	Contributing factor
	Last for 12 months	Real independent event with personal judgement
<b>Reference</b>	(1) Fitch First Database (2) Investment Portfolio	
<b>Assumption</b>	Private unlisted investments with conditions on reselling	By the Business by referencing to existing portfolio
	Investment nominal amount USD500M	By the Business by referencing to existing portfolio
	Lost 90%	By the Business and Risk Management
<b>Frequency</b>	Once a year	By Risk Management by referring to external database
<b>Estimated financial impact</b>	USD450M	Simple calculation by Finance
<b>Components of financial impact</b>	Direct and indirect loss in writing off the investment	
<b>Other impact</b>	(a) Regulation / Legal: High (b) Servicing to client: Low (c) Reputation: High (d) Staff safety: Low	
<b>Action</b>	(1) To conduct similar analysis for other portfolio of investment (2) To review the due diligence process to minimise the occurrence and magnitude of impact (3) To arrive a common view of the deficiency of the capital in medium term	

## Result

	USD'MM
<b>ORM Capital (based on AMA or TSA approach)</b>	3,000
<b>Total financial impact</b>	
Arising from stress testing	5,468
Expected losses	500
	5,968
<b>Shortfall</b>	<b>(2,968)</b>

- Formulate and document the management response and action
- Subject to validation

## Agenda

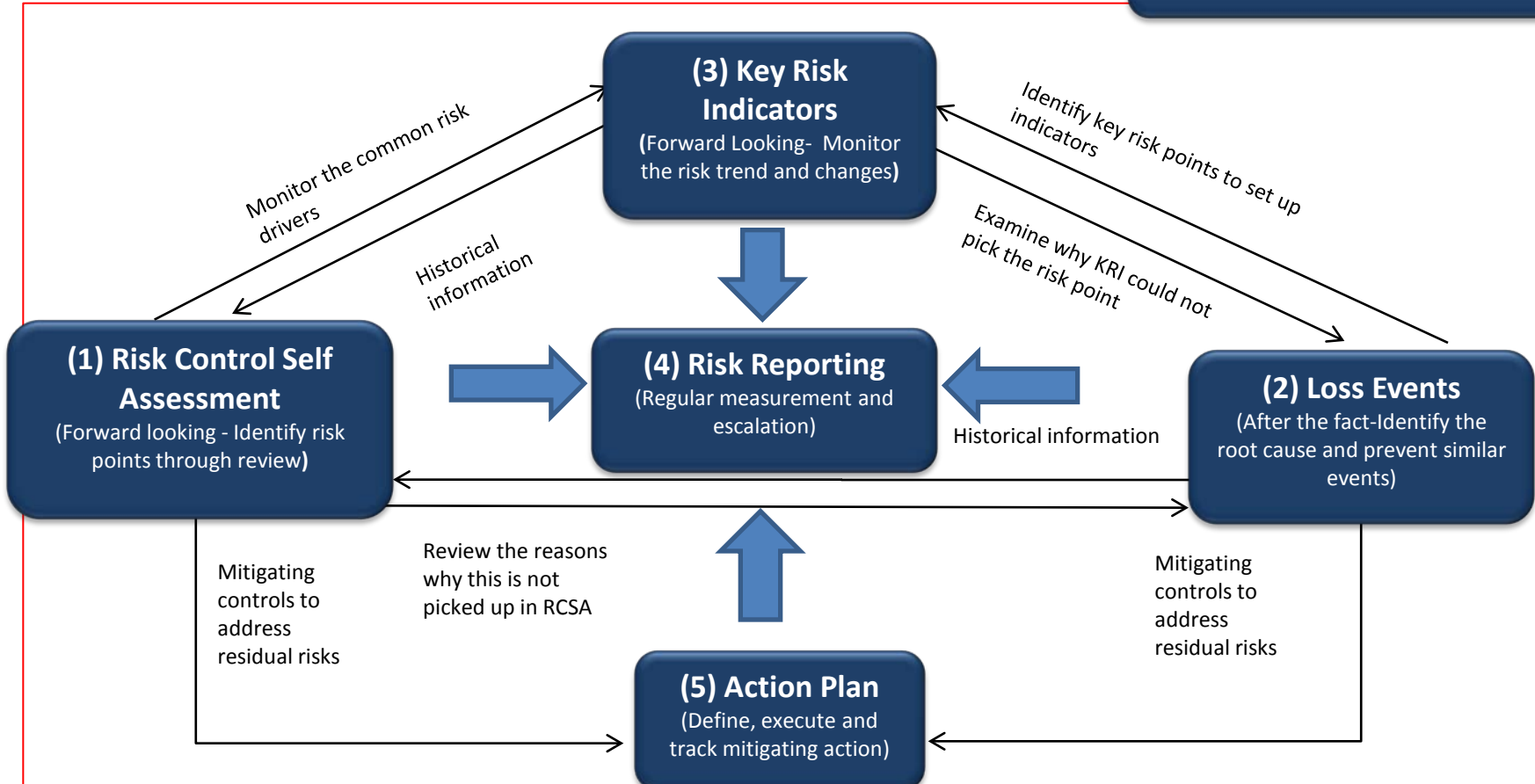
- Current risk vulnerabilities in Technology and Operations Landscape
- Conduct effective Risk Control and Self Assessment
- Build up useful Key Risk/Performance Indicators
- Perform out-of-the box Risk Analysis
- Produce a Risk Heat map

# Interaction between Risk Management Tools

Risk Governance Framework

Risk Appetite, Strategy, and Objectives

**(6) Scenario Analysis**  
(Thinking out of the box risk assessment)



Policy and Procedures

Corporate Governance and Organization

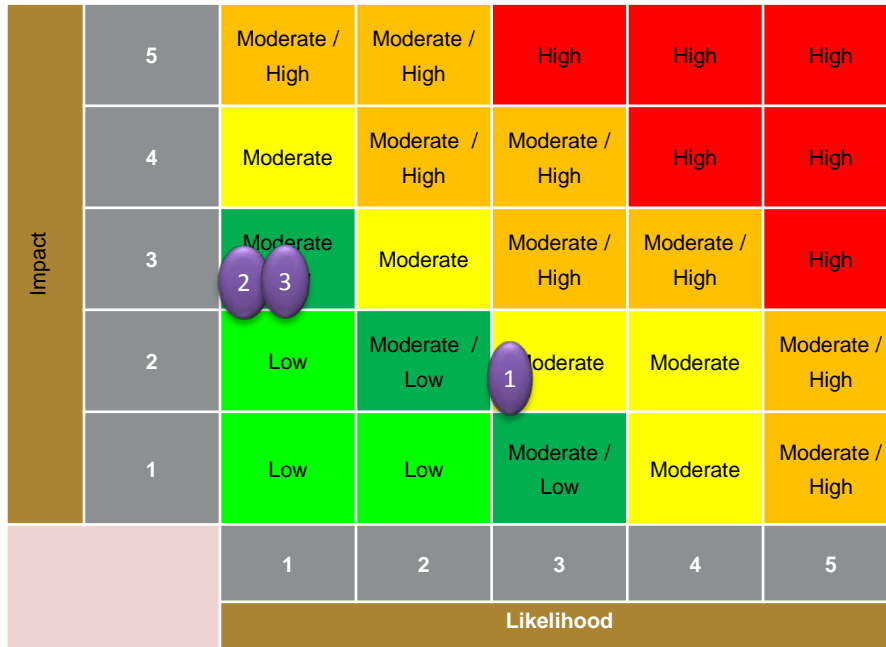
## Monitoring and reporting

- Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place.
- An effective monitoring process is essential for managing operational risk. It can assist in the early detection and correction
- Operational risk management reports must address both firm-wide and line of business results. These reports must summarize operational risk exposure, loss experience, relevant business environment and internal control assessments, and must be produced no less often than quarterly.
- Operational risk reports must also be provided periodically to senior management and the board of directors, summarizing relevant firm-wide operational risk information.
- Ongoing monitoring of operational risk exposures is a key aspect of an effective operational risk framework.
- To facilitate monitoring of operational risk, results from the measurement system should be summarized in reports that can be used by the firm-wide operational risk and line of business management functions to understand, manage, and control operational risk and losses.
- These reports should serve as a basis for assessing operational risk and related mitigation strategies and creating incentives to improve operational risk management throughout the institution.

## Risk Heat map

- A graphical representation of the risk profile of the business/location showing the top actual risks and emerging risk items
- The risks could be sourced from RCSA, KRI, Scenario Analysis, persistent Loss Events, New Business/Product Approval and management assessment
- Top risks will be rated on likelihood and impact
- Combination of the likelihood and impact will determine the categorization of the risk
- The number of boxes in different color should be determined in accordance to Risk Appetite
- For impact, we will take the higher of the risk rating of the four categories
- State the summary description of the risk and the mitigation action
- Statistics on the movement of the number of risk is included
- Monitor the position and changes of the risk (line on the sand)
- Risk Heat map can facilitate risk aggregation, comparison and monitoring
- Provide common platform for discussion and evaluation of risks
- Emerging risk items are those items which have not yet materialized but are put on the radar for business discussion and consideration

# Sample Risk Heatmap



#	Risks	Country	Likelihood	Impact	Residual Risk Rating	Action	Actions Owner	Due Date	Status

## Prominent and Emerging Risks Highlight

# Risk Assessment Criteria

## Impact Rating

		Financial	Non-financial		
Impact rating		Financial Loss Scale 1	Client Impact	Compliance Failure	Reputational Damage
5	High	>\$15MM	Major event likely to result in loss of a large number of clients or very significant clients	Serious systemic or material regulatory breach; regulatory fine and censure likely	Concerted, widespread or recurrent critical or hostile coverage in major / national media
4	Moderate / High	\$2MM - \$15MM	Severe event likely to result in loss of some clients or an important client(s)	Breach of multiple regulatory requirements which will require reporting to the regulator	Multiple instance of critical or hostile coverage in major / national media
3	Moderate	\$500k – \$2MM	Event likely to result in loss or damage to clients and complaints from some clients or significant client(s)	Material regulatory breach which will require reporting to the regulator	Single instance of unfavourable coverage in major / national media
2	Low / Moderate	\$250k - \$500k	Event likely to result in major inconvenience to a small number of clients or to a significant client(s)	Minor regulatory breach which will require to be reported to the regulator	Recurrent adverse coverage in minor / local media
1	Low	\$100k - \$250k	Event likely to result in minor inconvenience to a small number of clients or to a significant client(s)	Minor regulatory breach which may not require to be reported to the regulator	Single instance of adverse comment in minor / local media

## Likelihood Rating

Rating		Description
5	Frequent	Happening now or will occur at least monthly
4	Medium / High	May occur every 1 – 12 months
3	Medium	May occur every 1 – 3 years
2	Low / Medium	May occur every 3 – 10 years
1	Low	May occur every 10 or more years

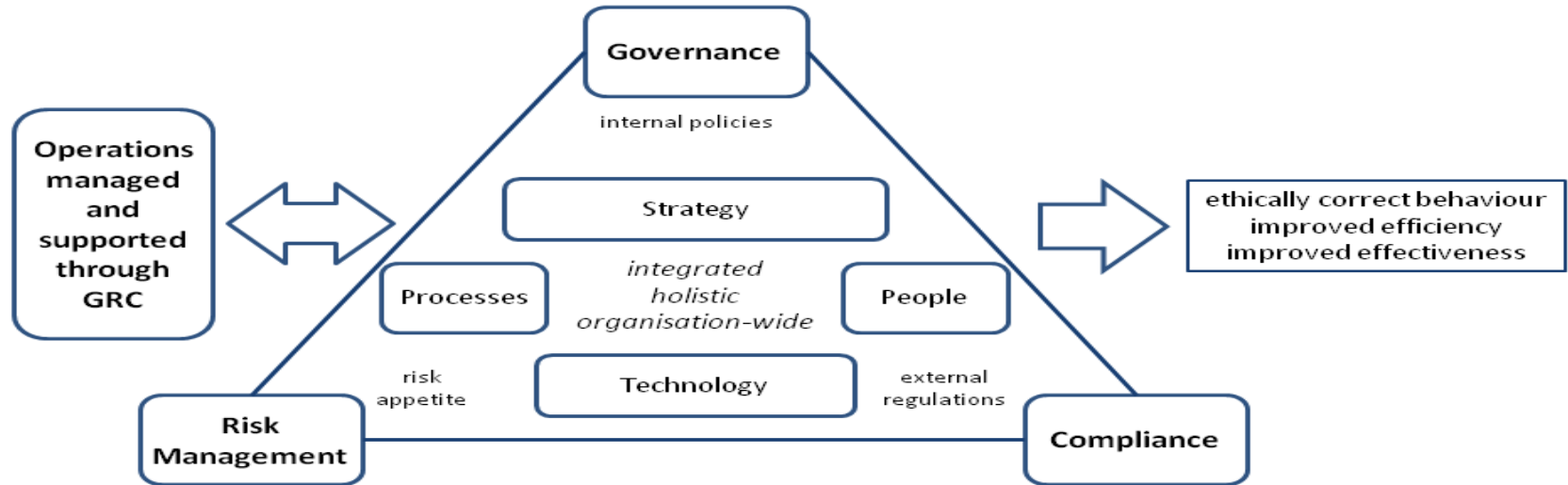
## HeatMap Matrix

		Likelihood				
		1	2	3	4	5
Impact	5	Moderate / High	Moderate / High	High	High	High
	4	Moderate	Moderate / High	Moderate / High	High	High
	3	Moderate / Low	Moderate	Moderate / High	Moderate / High	High
	2	Low	Moderate / Low	Moderate	Moderate	Moderate / High
	1	Low	Low	Moderate / Low	Moderate	Moderate / High
		1	2	3	4	5
		Likelihood				

Note: The overall impact rating is the higher of Financial and three categories of Non-Financial



## Governance, Risk and Compliance (GRC)



- Identify a methodology to link process and technology, effectively bridging together internal audit, risk management, information security, operations and compliance functions.
- Utilize GRC to effectively execute corporate strategy in tough economic times
- Grow GRC capabilities and transform a reactive and technologically focused approach, into a proactive and risk based approach

## Appendix 1

# Sample Indicators for Financial Institutions

### 8.2.1. Agency Services

Name	Nature	Description
Corporate Actions - Number of Corporate Action Mandates under Management	Leading, Current	The total number of approved corporate action mandates under management at the point of measurement.
Corporate Actions - Number of Voluntary Corporate Action Letters of Instruction or Direction not Executed	Leading, Current	The number of letters of instruction or direction received from non-discretionary voluntary mandate owners in response to our request for instruction regarding a set of corporate action events which are scheduled to occur within the foreseeable future, which currently have not yet been executed.
Custody - Frequency of Inventory Checks	Current	The average number of safe custody and safe deposit box inventory checks per month during the preceding 12 calendar months.
Custody - Number of Securities Received but not yet Registered in Customer's Name	Current	The number of non-bearer securities received into safe custody by the organisation on behalf of customers or clients during the preceding 14 business days and not yet registered in the customer's name as beneficial owner.
Custody and Actions - Ratio of Errors to Manual Transactions	Current, Lagging	The total number of errors detected during the preceding 3 calendar months, divided the number of manual custody and corporate action transactions processed.
Customer Mandates - Number of Breaches Not Disclosed to Customers within Threshold	Current, Lagging	The total number of detected breaches of customer mandates by the organisation, its employees, agents or representatives not yet disclosed to the relevant customer or client and beyond disclosure threshold.
Fee and Charge Reversals - Number	Current, Lagging	The total number of fee or charge reversals booked during the preceding 3 calendar months across all entities within the organisation.
Payment and Settlement Disputes - Number Open with Customers and Counterparties	All	The total number of open payment and settlement disputes with customers, clients and counterparties at the point of measurement.
Transaction Maintenance - Number of Maintenance Events Missed	All	The total number of transaction maintenance events during the preceding 6 calendar months that were not completed by the scheduled completion date.

### 8.2.2. Asset Management

Name	Nature	Description
Accredited Advisory Staff - Number with Out of Date Accreditation	All	The number of accredited advisors representing or acting on behalf of the organisation whose advisory license or accreditation is out of date at the point of measurement.
Best Execution - Number of Best Execution Exceptions	Leading	The number of transactions not executed at the best price or terms available, or not following best practices intended to ensure they are, which were identified during the preceding 3 calendar months.
Customer and Client Product Usage - Percentage of Product Suitability Approvals Outstanding	Leading, Current	The total number of currently outstanding customer and client product suitability approvals for products already offered to customers and clients, as a percentage of the total number of customer and client relationships.
Dealers, Traders and Investment Managers - Number of License Exceptions	Current	The number of transactions executed by approved dealers, traders and investment managers during the preceding 12 calendar months that did not comply with restrictions imposed by their trading licenses or where the individual lacked a current trading license.
Front-Running - Number of Instances Detected	Lagging	The total number of instances of front-running detected by the organisation during the preceding 3 calendar months.
Investment Guidelines - Number of Guideline Breaches Detected	Current, Lagging	The number of breaches of investment guidelines detected by the organisation during the preceding 12 calendar months.
Investment Guidelines - Number of Portfolios without Guidelines	Leading, Current	The number of investment portfolios currently under the management of the organisation for which no formal investment guidelines have been agreed with the customer.
Investment Management - Concentration Growth of Investments in New or High Risk Investments, Vehicles or Products	All	The growth by value in the composition of the value of a portfolio under management represented by investments, vehicles and products that are either new or deemed to be high risk, during the preceding calendar month.
Orders and Instructions - Number Executed without Required Authorisation	Current, Lagging	The total number of orders and instructions executed without the required authorisation during the preceding calendar month.
Transaction Volumes - Number of Disputed Transactions	Current, Lagging	The total number of open transactions currently disputed by the customer, client or counterparty.

Source: The Institute of Operational Risk

### 8.2.3. Commercial Banking

Name	Nature	Description
Branches, Disposal Points and Operations in High-Risk Countries - Number	All	The number of currently active branches, disposal points and operations located in countries deemed to be high-risk.
Collateral Agreements - Number Missing or Not Executed after Exemption Period	All	The number of collateral agreements currently missing or not executed and beyond the organisation's maximum exemption period.
Credit Facility Applications - Number Approved Based on Financial Reports Older than Threshold	Leading, Current	The number of credit facilities approved during the preceding 12 calendar months where at least one supporting financial report or document was older than a pre-defined threshold.
Credit Facility Reviews - Number not Performed within Policy Threshold	All	The total number of credit facilities that are currently beyond the pre-defined threshold for review and have not been reviewed.
Customer and Client Relationships - Number of Relationships not Reviewed within Threshold	All	The number of existing customer and client relationships that are beyond the pre-defined threshold for review and have not yet been reviewed.
Customers and Clients - Number of Financing Relationships based on Movable Underlying Assets	Current, Lagging	The total number of customer and client financing relationships where the underlying asset subject to the financing is mobile or readily transportable.
Mortgages, Commercial Property and Home Loans - Number of Interest Claims Settled	Lagging	The total number of interest claims raised against the organisation due to the late registration of a mortgage loan, delays in closure due to lost or misplaced title deeds or other processing delays, which were settled by the organisation during the preceding calendar month.
Payments - Number with Settlement Instructions Deviating from Standing Settlement Instructions	Current, Lagging	The total number of payments generated during the preceding calendar month with standing settlement instructions that were superseded by special instructions.
Payments - Ratio of Payments by Manual Payment Methods to Electronic Payment Methods	Current	The ratio of transactions settled using non-electronic payment methods to those using electronic payment methods during the preceding business day.
Workouts - Number of Credit Defaults Awaiting Workout	Current	The total number of credit defaults formally handed over for workout and recovery where workout has not yet commenced.

### 8.2.4. Corporate Finance

Name	Nature	Description
Accredited Advisory Staff - Number with Out of Date Accreditation	All	The number of accredited advisors representing or acting on behalf of the organisation whose advisory license or accreditation is out of date at the point of measurement.
Corporate Finance Deals - Number of Deals Executed without Timely Regulatory Filings	Lagging	The number of corporate finance transactions executed during the preceding 6 calendar months without timely regulatory filings before or during the execution process.
Corporate Finance Deals - Number of Post-Execution Reviews not Performed within Threshold	Current, Lagging	The number of post-execution reviews of corporate finance transactions not performed within threshold.
Custom or Structured Transactions - Number Modified or Terminated	All	The total number of custom or structured transactions executed by the organisation with its customers and clients that were modified or terminated during preceding 6 calendar months.
Insider Trading - Number of Instances Detected	Lagging	The total number of instances of insider trading detected by the organisation during the preceding 3 calendar months.
Limit Breaches - Number of Legal Lending Breaches	Lagging	The number of breaches of legal and regulatory lending limits during the preceding calendar month.
Special Purpose Vehicles - Number not Reviewed within Threshold Period	Current, Lagging	The total number of special purpose vehicles (SPV's) in use or under administration that are currently beyond the threshold for review and have not been reviewed.
Special Purpose Vehicles - Percentage Involvement per Vehicle	Current, Lagging	The current percentage of involvement for each special purpose vehicle in which the organisation has an interest.
Staff - Number of Staff with Inappropriate or Unnecessary Access to Proprietary Research	All	The number of staff who, during the preceding 12 calendar months, had unnecessary or inappropriate access to the organisation's proprietary research, regardless of whether that access resulted in any improper use.

Source: The Institute of Operational Risk

### 8.2.5. Payments and Settlements

Name	Nature	Description
Automated Clearing House Returns - Number	All	The number of files returned by all automated clearing facilities during the previous business day.
Cash Breaks - Number over Threshold	Current, Lagging	The total number of cash breaks on the organisation's clearing and/or Nostro accounts that are currently older than the organisation's predefined threshold.
External Payment System Outages - Number	All	The number of outages of external payment systems to which the organisation has interfaces and/or interdependencies, during the preceding 12 calendar months.
Legal Entity Payment Mismatches - Number	Lagging	The number of payment mismatches detected during the preceding calendar month across legal entities within the organisation.
Nostro Breaks - Number of Open Items	All	The total number of open Nostro breaks at the point of measurement.
Payment and Settlement Fails - Total Number of Fails	All	The total number of settlement fails during the preceding business day.
Payment and Settlement Fails - Total Value of Fails	All	The total gross value of settlement fails during the preceding business day.
Payment System Outages - Number	All	The number of outages of the organisation's payment systems during the preceding calendar month.
Payment Volumes - Percentage of Daily Settlement Volume Eligible for Netting	Lagging	The percentage of settlements during the preceding business day that were eligible for netting.
Payments - Number Generated without Standing Settlement Instructions	All	The total number of payments generated during the preceding calendar month that did not have applicable, predefined, standing settlement instructions.

### 8.2.6. Retail Banking

Name	Nature	Description
Branches and Disposal Points - Total Number of Robberies	Lagging	The total number of robberies by external parties across all the organisation's branches and disposal points during the previous calendar month.
Brokers, Agents and Intermediaries - Number of Introduced Customer Applications Rejected	All	The total number of new customer or client applications introduced to the organisation by brokers, agents and intermediaries during the preceding 12 calendar months that the organisation rejected.
Card Transactions Disputed - Number Open	Current, Lagging	The total number of card transactions disputed by customers and clients that currently remain open.
Cards - Number of Stolen Cards Reported	Current, Lagging	The total number of cards issued by the organisation to its customers and clients that have been reported stolen during the preceding 3 calendar months.
Customer and Client Accounts - Number of New Accounts Opened	Leading, Current	The number of new retail account relationships opened during the preceding month.
Customer and Client Relationships - Number of Instances of Returned Mail	Current, Lagging	The total number of customer or client relationships where mail has been returned by the postal services as undeliverable or refused during the preceding 3 calendar months.
E Crime - Number of E-Banking Accounts Compromised by Phishing or Trojans	Current, Lagging	The number of customer and client e-banking accounts which have been compromised specifically through phishing and/or trojans.
Forged Cheques/Checks and Drafts Presented - Number	Leading, Current	The number of instances of forged cheques/checks and drafts being presented to the organisation for payment that were detected during the preceding 3 calendar months. It includes both successful forgeries where value was extracted from the organisation and failed attempts.
Mortgages, Commercial Property and Home Loans - Percentage of Approved Loans not yet Taken Up	All	The percentage of approved loans granted or on which instructions are issued over the preceding calendar month which have not yet been taken up by the customer or which have been rejected by the customer.
Staff - Percentage of Staff not Completed Primary Fraud Detection Training	Current	The number of staff who have not yet completed all primary fraud-detection training required for their job function and grade, as a percentage of the total number of permanent employees.

Source: The Institute of Operational Risk

### 8.2.7. Retail Brokerage

Name	Nature	Description
Confirmations - Number of Unmatched Confirmations for Over-the-Counter Transactions with No Previous Cashflow	All	The total number of confirmations generated where no inbound confirmation has yet been received from the counterparty, the underlying transaction is an over-the-counter (OTC) one, and no cashflow has occurred.
Customer and Client Product Usage - Percentage of Product Suitability Approvals Outstanding	Leading, Current	The total number of currently outstanding customer and client product suitability approvals for products already offered to customers and clients, as a percentage of the total number of customer and client relationships.
Customer and Client Relationships - Number without Adequate Background and Reference Checks	All	The total number of current customers and clients that have not yet been through the organisation's background and reference checking procedure at the point of measurement.
Customer Mandates - Number of Breaches Detected	Current	The total number of breaches of customer mandates by the organisation, its employees, agents or representatives detected during the preceding calendar month.
Customers and Clients - Frequency of Changes to Standing Settlement Instructions	Current, Lagging	The average number of changes per month to a customer or client's standing settlement instructions, during the preceding 12 calendar months.
Customers and Clients - Number of Customer Money Segregation Breaches	Lagging	The number of breaches of customer and client money segregation policies and procedures arising from the processing of payments, during the preceding calendar month.
Dealers, Traders and Investment Managers - Number of License Exceptions	Current	The number of transactions executed by approved dealers, traders and investment managers during the preceding 12 calendar months that did not comply with restrictions imposed by their trading licenses or where the individual lacked a current trading license.
Dealers, Traders and Investment Managers - Percentage of Total without Dealing Mandates	All	The number of approved dealers, traders and investment managers who currently have no formal dealing mandate defining the limits on their delegated dealing, trading and/or investment authority, as a percentage of the total number of dealers, traders and investment managers.
Fee and Charge Reversals - Number	Current, Lagging	The total number of fee or charge reversals booked during the preceding 3 calendar months across all entities within the organisation.
Limit Breaches - Number of Dealing and Trading Limit Breaches	All	The total number of dealing and trading limit breaches detected during the preceding 6 calendar months.

### 8.2.8. Trading and Sales

Name	Nature	Description
Best Execution - Number of Best Execution Exceptions	Leading	The number of transactions not executed at the best price or terms available, or not following best practices intended to ensure they are, which were identified during the preceding 3 calendar months.
Confirmation Mismatches - Total Number	All	The total number of transactions within the matching process with mismatched transaction details or legal terms that currently remain unmatched.
Confirmation Mismatches - Total Value of Mismatched Transactions	Current, Lagging	The total value of transactions within the matching process with mismatched transaction details or legal terms that currently remain unmatched.
Dealers, Traders and Investment Managers - Percentage of Total without Dealing Mandates	All	The number of approved dealers, traders and investment managers who currently have no formal dealing mandate defining the limits on their delegated dealing, trading and/or investment authority, as a percentage of the total number of dealers, traders and investment managers.
Dealing and Trading Locations - Percentage of Transaction Volume using Non-Central Trading Platforms	All	The total volume of transactions executed using non-centralised dealing and trading platforms during the preceding 6 calendar months, as a percentage of the total number of transactions executed during the period.
Dealing Mandates - Number of Breaches Detected	Current	The total number of breaches of dealing mandates by the organisation or its dealers, traders and investment managers detected during the preceding calendar month.
Limit Breaches - Number of Dealing and Trading Limit Breaches	All	The total number of dealing and trading limit breaches detected during the preceding 6 calendar months.
Manual Deal Slips - Number Unaccounted For	All	The total number of manual deal slips issued for use during the preceding 12 calendar months that currently cannot be accounted for.
Models and Methodologies - Number Developed by End-users not Reviewed within Threshold	Current, Lagging	The total number of models and methodologies developed by end-users the organisation currently has available for use that have not yet been reviewed and are beyond threshold.
Pricing - Number of Transactions Identified Priced outside of Permitted Deviations	Leading, Current	The number of transactions executed at rates or prices outside the organisation's permitted deviation from market reference prices during the preceding 6 calendar months.

Source: The Institute of Operational Risk

### 8.2.9. Corporate Services

Name	Nature	Description
Access Rights to Applications by Staff - Frequency of Access Right Reviews	All	The average number of reviews per month of staff access rights to business applications during the preceding 12 calendar months.
Accounting - Number of Amendments to the Charts of Accounts	Leading, Current	The number of changes made to charts of accounts of the organisation during the preceding 12 calendar months.
Assets in Transit - Total Value	Current, Lagging	The total value of assets in transit at any point during the preceding business day.
Business Continuity Management (BCM and BCP) - Number of Plans not Authorised beyond Threshold	All	The number of Business Continuity Plans (BCP) which have been reviewed but which have not yet been re-authorised, and are beyond a pre-defined time limit for reauthorisation, as well as the number of Business Continuity Plans (BCP) which have been prepared for the first time, but which have not yet been authorised and are beyond the pre-defined time limit for authorisation.
Critical System Changes - Number of Emergency Software Changes	Current	The number of emergency software changes made to critical systems during the preceding 12 calendar months.
Critical System Outages - Average Duration	All	The average duration, expressed in minutes, of unscheduled critical system outages per month, during the preceding 12 calendar months.
Information Technology Support Requests - Number Outstanding beyond Threshold	Current	The number of information technology support requests currently outstanding and beyond threshold.
Litigation Cases - Number Closed	Current, Lagging	The total number of litigated customer and client compensation cases that were closed or withdrawn during the preceding 3 calendar months.
Offices and Operations - Number of Field Visits to Remote Locations	Leading, Current	The number of visits by senior management based in centralised locations to remote locations during the preceding 12 calendar months.
Physical Security - Number of Physical Security System Activations	Leading, Current	The number of instances during the preceding 12 calendar months that physical security systems and environmental problem detectors on the organisation's property and premises gave alarm for any reason.
Policy and Procedure Breaches - Number of Detected Instances of Inadequate Segregation of Duty	Current, Lagging	The number of segregation of duty policy breaches detected during the preceding 12 calendar months.
Project Management - Number of High-Risk Projects	All	The number of projects currently in progress which have been rated or are considered as being high-risk.
Property and Facilities - Number of Health and Safety Incidents Reported	Leading, Current	The number of incidents relating to health and safety at the organisation's properties and premises that were reported during the preceding 12 calendar months.
Regulatory Reports - Number of Errors	Current, Lagging	The total number of reports or statements provided to regulators in which errors were detected after the reports had been submitted, during the preceding 12 calendar months, across all jurisdictions and legal entities within the organisation.
Staff - Number of Staff with Non-Compliance of Holiday Regulations	Current, Lagging	The number of employees who currently are out of compliance with the organisation's vacation or holiday regulations and beyond threshold.

### 8.2.10. Insurance

Name	Nature	Description
Claims Assessor - Number of Assessor Appraisals not Completed Within Threshold	Lagging	The number of claims assessors who were given an appraisal within the given threshold, during the preceding 12 calendar months.
Complaints from Customers, Clients or Policy Holders - Number Received regarding Claims Assessors	All	The number of policy holder complaints with respect to the work of the claims assessors.
Insurance Claims - Average Number of Claims Per Client	Lagging	The total number of claims received over the preceding 12 calendar months divided by the total number of clients, representing the average number of claims per client.
Insurance Claims - Percentage of Claims Received Flagged as Suspicious	Current, Lagging	The percentage of all claims received during the preceding 12 calendar months which were flagged as suspicious.
Insurance Policies - Number of New Policies Issued with Unapproved Variances or Terms	All	The number of insurance policies issued during the preceding 12 calendar months which contained unapproved variances to standard procedures or terms and conditions which had not been specifically approved.
Insurance Proposals - Number of Non-Standard New Business Proposals Made	Lagging	The number of proposals for new insurance business made to clients during the preceding 12 months that related to non-standard cover or to custom or bespoke insurance policies.
Reinsurance Claims - Number Disputed	Current, Lagging	The total number of reinsurance claims made by the organisation in the preceding 12 calendar months that were disputed by the reinsurer.
Reinsurance Treaties - Number of Changes in Conditions that Cannot be Passed on to Policies	Leading, Current	The indicator captures the number of changes in reinsurance conditions during the past 12 calendar months that cannot be passed on to existing policies.
Reserves - Number of Errors in Calculating Claims Reserves	Leading, Current	The number of detected errors in the calculation of claims reserves.
Risk Assessor - Number of Assessors not Completed Primary Risk Assessment Training	Current	The number of risk assessors who have not yet completed all primary risk assessment training required for their job function and grade.

Source: The Institute of Operational Risk

# You can find me at :

## Dominic Wu

- Managing Director, Senior Risk Manager, Financial Markets and Treasury Services, Risk Management BNY Mellon  
Tel: 852.2840.9791  
Email: dominic.wu@bnymellon.com
- Chairman of Asia Chapter of the Institute of Operational Risk
- LinkedIn:  
[http://www.linkedin.com/profile/edit?id=26323027&trk=hb\\_t ab\\_pro\\_top](http://www.linkedin.com/profile/edit?id=26323027&trk=hb_t ab_pro_top)