Approaches to detect when a business unit is approaching close to breaching its pre-defined operational risk appetite

An organisation may have several business units and the activities of each unit may be unique e.g. a bank may have a retail banking and commercial banking business units. Each business unit will be exposed to a set of risks that may influence its ability to achieve its objectives. It may also be exposed to some risks that may also influence the ability of other business units or the overall organisation to achieve their objectives.

The type and level of risk exposures for a business unit may continuously change due to various factors such as decisions undertaken, organizational factors, changes in the external environment and crisis/incidents. The senior executives responsible for the business unit's performance need to continuously review whether the risk exposures are within the pre-defined risk appetite. Other stakeholders such as operational risk group, internal auditors, risk committees and board members would also be typically interested in periodic assurance on the alignment of risk exposures of various business units with their pre-defined risk appetite.

What approaches do you use in your organisation to detect whether a business unit is close to breaching its operational risk appetite or when this has already been breached?

Here are some common approaches from my experience to get this discussion started.

Approach 1 – Risk Appetite criteria on specific risk categories or risks

Let's understand this approach with an example.

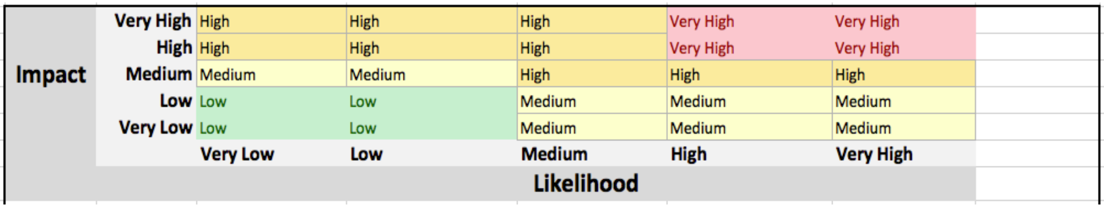
Example: -
Within its operational risk appetite statement, RWS Bank (fictitious bank) has defined risk appetite criteria as below: -

- "Any risks related to intentional or accidental misuse of customer data is unacceptable".

The bank has a risk category titled "Data Protection" and has following risks mapped to it within its Retail Banking business unit: -

- R1: Intentional misuse of customer data by sales and marketing function
- R2: Intentional misuse of customer data by outsourcing vendors
- R3: Intentional misuse of customer data by re-sellers

For simplicity, assume following assessment scales are used for performing risk assessments: -



Impact						
	Very High	High	High	High	Very High	Very High
	High	High	High	High	Very High	Very High
	Medium	Medium	Medium	High	High	High
	Low	Low	Low	Medium	Medium	Medium
	Very Low	Low	Low	Medium	Medium	Medium
		Very Low	Low	Medium	High	Very High
				Likelihood		

The table below highlights the translation of risk appetite criteria into risk assessment measures: -

Risk Appetite Criteria	Risk Appetite Criteria Translated as Risk Assessment Measures
Any risks related to intentional or accidental misuse of customer data is unacceptable	The Likelihood level above Very Low or Impact level above Very Low is unacceptable for any risks related to intentional or accidental misuse of customer data.

Following are the risk assessment outcomes in Q1-2016: -

Risk	Likelihood	Impact	Level of Risk
R1: Intentional misuse of customer data by sales and marketing function	Very Low	Very Low	Low
R2: Intentional misuse of customer data by outsourcing vendors	Very Low	Very Low	Low
R3: Intentional misuse of customer data by re-sellers	Very Low	Very Low	Low

Based on the above risk assessment outcomes, the Retail Bank business unit is within its pre-defined risk appetite.

Following are the risk assessment outcomes in Q2-2016: -

Risk	Likelihood	Impact	Level of Risk
R1: Intentional misuse of customer data by sales and marketing function	Medium	Medium	High
R2: Intentional misuse of customer data by outsourcing vendors	Very Low	Very Low	Low
R3: Intentional misuse of customer data by re-sellers	Very Low	Very Low	Low

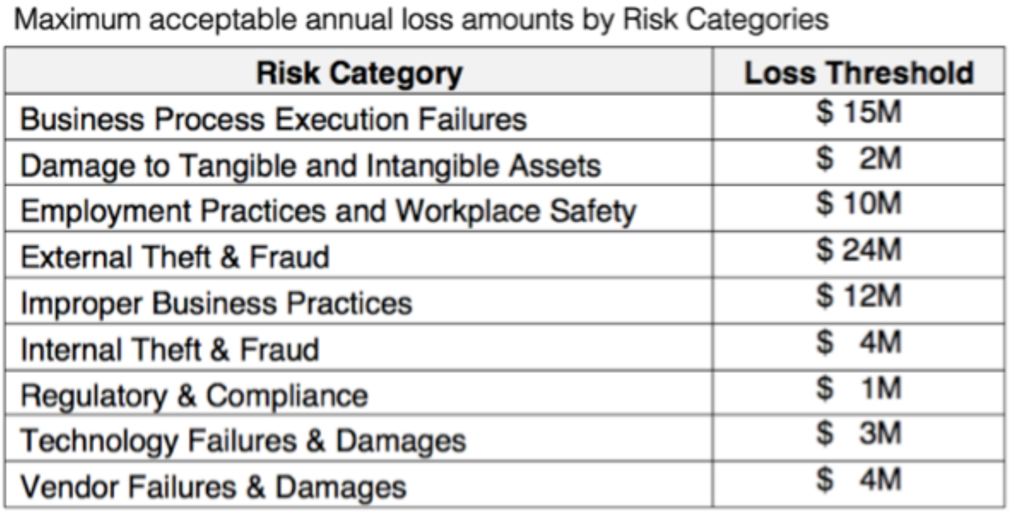
Based on the above risk assessment outcomes, the Retail Bank business unit has breached its pre-defined risk appetite.

In addition to risk assessments, following types of information may also indicate potential breach of risk appetite: -

- A high priority issue is raised by internal audit team regarding controls related to “R1: Intentional misuse of customer data by sales and marketing function” risk. If this issue is not addressed within 2 months, they assess the Impact of the risk will become “High”.
- A near miss event related to “R1: Intentional misuse of customer data by sales and marketing function” risk. Upon investigation of this event, it was discovered that one key control associated with this risk failed.
- A KRI associated with “R1: Intentional misuse of customer data by sales and marketing function” has turned from green to amber.

Approach 2 – Maximum Acceptable Loss Amounts

In this approach, organisation defines maximum acceptable of loss amounts for specific risk categories or risks over a period (e.g. year). Example of this is highlighted below for the Retail Bank business unit of fictitious RWS Bank: -



Maximum acceptable annual loss amounts by Risk Categories

Risk Category	Loss Threshold
Business Process Execution Failures	$ 15M
Damage to Tangible and Intangible Assets	$ 2M
Employment Practices and Workplace Safety	$ 10M
External Theft & Fraud	$ 24M
Improper Business Practices	$ 12M
Internal Theft & Fraud	$ 4M
Regulatory & Compliance	$ 1M
Technology Failures & Damages	$ 3M
Vendor Failures & Damages	$ 4M

Assume that the financial year period for above threshold is from 1Jan to 31Dec. To determine potential breach of appetite, the bank has defined following two thresholds for escalation as part of risk appetite breach reporting: -

- If the actual loss amount YTD for all risks within a risk category reaches above 70% and is below 90% of the annual loss threshold.
- If the actual loss amount YTD for all risks within a risk category reaches above 90% and is below 100% of the annual loss threshold.

So if on 15Jun2015, a loss event occurs which increases the total amount of losses YTD for risks within “Employment Practices and Workplace Safety” category from $6.5m to $7.2m, then the risk category should be escalated as part of any potential risk appetite breach reporting as it is breached one of the above loss thresholds.

Approach 3 – Monitor Performance Indicators

In this approach, one or more performance indicators are identified as signal of potential breach of risk appetite. Let’s look at an example: -

Indicator: - Rate of new customer acquisition

For the retail bank business unit of RWS Bank, typical new acquisition rate is 5% every month. The current processes and IT systems are designed based on this assumption. So if the new acquisition rate unexpectedly increases beyond 5%, it may be considered as signal of excessive risk taking and hence potential breach of appetite. So following thresholds can be defined for escalation as part of risk appetite breach reporting.

Green	New customer acquisition rate of 5% or below.
Amber	New customer acquisition rate of 6% to 10% for 3 consecutive months.
Red	New customer acquisition rate of 6% or more for 6 consecutive months.

Through such escalation, timely review of the impact of unexpected increase in new customer acquisition over potential risk exposures can be performed to determine whether the business unit may potentially breach its risk appetite in the near future.

Additional examples of such indicators may include: -

- Unexpected changes in revenue levels
- Unexpected changes in revenue sources
- Unexpected changes in number of customers
- Unexpected changes in level of customer churn
- Unexpected changes in number of customer complaints
- Unexpected changes in number of products
- Unexpected changes in number of vendors
- Unexpected changes in unplanned costs
- Unexpected changes in number of employees
- Unexpected changes in level of staff turnover
- Unexpected changes to level of staff turnover within leadership or senior executive roles
- Unexpected changes in level of ratio between permanent and temporary employees

Approach 4 – Monitor Risk Indicators

In this approach, one or more performance measures are identified as signal of potential breach of risk appetite. Let’s look at an example: -

Indicator: - Percentage of preventative controls which are assessed as “Not Effective”

Preventative controls are the most important type of controls for operational risks, as they prevent incidents/loss events from occurring. So these controls should be monitored closely as weaknesses within preventative controls may signal deterioration within the control environment. So following thresholds can be defined for escalation as part of risk appetite breach reporting.

Green	100% of preventative controls are effective.
Amber	5% to 10% of preventative controls are not effective.
Red	More than 10% of preventative controls are not effective.

Through such escalation, timely review of the impact of changes in the effectiveness of the control environment over potential risk exposures can be performed to determine whether the business unit may potentially breach its risk appetite in the near future.

Additional examples of such indicators may include: -

- Unexpected changes in number of high priority issues
- Unexpected changes in number of high priority audit findings
- Unexpected changes in number loss events
- Unexpected changes in the average loss amount
- Unexpected changes in the total loss amount
- Unexpected changes to number of risk indicators with current level of Amber
- Unexpected changes to number of risk indicators with current level of Red
- Unexpected changes to the number of risks where the level of risk has deteriorated between last 2 risk assessments
- Unexpected changes to the number of controls where the level of control effectiveness has deteriorated between last 2 control assessments
- Unexpected changes in level of whistleblowing events
- Unexpected changes in number of risks within the risk profile of the business unit