RiskSpotlight

Operational Risk Appetite Statement Example

Introduction

Many financial services organizations are currently in the process of defining or revising their operational risk appetite framework. A key part of the framework is defining the risk appetite statement. Such statements are the main channel through which an organization can effectively communicate and instill risk management into their decision making process. Developed and utilized effectively they can support the business as a whole to make risk based decisions at all levels.

Challenges

- The risk appetite statement typically covers confidential information about the organization and hence it is unlikely that any organization will publicly make its risk appetite statement available.
- Most organizations do not have prior experience of formally defining and documenting their operational risk appetite. Due to this a high level of uncertainty currently exists on what should be included in the risk appetite statement.
- The above two factors combined together has created a gap within the operational risk community on what are the best practices related to content covered within a risk appetite statement.

Solution

To address the above challenges, the RiskSpotlight team has performed in-depth research on risk appetite focusing on the operational risk element. The research has covered diverse sources such as The Financial Stability Board, ISO 31000, COSO ERM & The Institute of Risk Management.

Based on the best practices identified from the researched sources, we have created an operational risk appetite statement for a fictitious organization – RWS Bank. This statement contains all the key topics a financial services organization should consider covering within its own operational risk appetite statement. Our intention by sharing this with the operational risk community is to give a starting point for the operational risk practitioners to have a structured discussion on this topic. While practitioners may be reluctant to share their own company specific content on the internal appetite statement, we expect that they would be more willing to provide their inputs on an appetite statement for a fictitious bank.

RiskSpotlight will publish this document on all the key risk management LinkedIn groups so practitioners can provide their feedback and inputs to further enrich this document. Based on the inputs received, we will periodically release new versions of this document, so it can become a standard template for the operational risk community to use for defining and benchmarking their own internal operational risk appetite statements.

The team at RiskSpotlight have expertise and experience in developing the frameworks, content and providing training on all the key elements that go into creating an effective Risk Appetite framework. We can offer training, content and consultancy in support of all of these areas and are going to be offering an online training course focused on Risk Appetite for Operational Risk.

Visit www.riskspotlight.com for additional content, training and consulting related to operational risk management.

RWS Bank

Banking on Innovation

Background to Operational Risk at RWS Bank

Purpose: - This section provides high-level information related to the operational risk framework utilized at RWS Bank, where such information is pertinent to the operational risk appetite statement that follows.

About RWS Bank

RWS Bank is a medium-sized retail bank based in the east coast of US. It provides the following products and services: -

- Consumer Banking
- Residential Mortgage
- Commercial and Business Lending

It currently serves one million retail consumers and 25,000 commercial organizations across 5 states. It serves the customers from its 200 branches and through its online channel.

Here are some financial statistics for the most recent year: -

Financial Item	Figures
Net Interest Income	$681 Million
Noninterest Income	$290 Million
Assets	$27 Billion
Loans	$18 Billion
Deposits	$19 Billion

Operational Risk at RWS Bank

RWS has adopted the following definition of operational risk: -

Potential events (including sets of circumstances),

- which may result in positive and/or negative impacts **and**
- where such impacts may influence one or more operational objectives of the bank **and**
- where there is a level of uncertainty about one or more of the above aspects

The above definition is based on the definition of risk covered within ISO 31000, which is the international standard for risk management.

The bank recognizes that operational risks: -

- Are inherent within its current business operations **OR**
- May emerge from new business decisions impacting the business operations **OR**
- May emerge from changes within the internal or external context of the bank

Unlike other banks, RWS does not perceive operational risks to be just potential events with negative impacts. RWS's business strategy is based on adopting and implementing innovative ideas and technologies within its products, services, customer interactions and business processes. The bank recognizes that to implement an innovation-driven business strategy, it will not only need to mitigate certain operational risks but also increase its exposure to certain operational risks. So unlike other banks, which adopt a completely defensive strategy for operational risk management, RWS has adopted a combination of defensive and offensive strategies for operational risk management.

RWS operational risks are categorized across the following categories: -

- Business Process Execution Failures
- Damage to Tangible and Intangible Assets
- Employment Practices and Workplace Safety
- External Theft & Fraud
- Improper Business Practices
- Internal Theft & Fraud
- Regulatory & Compliance
- Technology Failures & Damages
- Vendor Failures & Damages

The Group OpRisk Department has defined a library of 125 operational risks based on the library provided by RiskSpotlight (www.riskspotlight.com) across the above categories. These have been utilized as a starting point for risk registers for every business unit, who can add risks specific to their business context.

For each operational risk, the following data items are captured to fully understand the risk during risk identification and risk assessment: -

- Internal and/or External Causes that may increase or decrease the likelihood of the risk. For each cause, a source from where the cause could emerge is also captured
- One or more positive impacts that may result from the risk
- One or more negative impacts that may result from the risk
- One or more operational objectives that may be influenced by the above impacts

Risk Assessment Criteria

This section briefly covers the key aspects of Risk Assessment Criteria, which are relevant within the risk appetite context. The complete documentation on Risk Assessment Criteria is not covered here.

The bank has aligned the risk assessment criteria to the guidance provided within ISO 31000, which is a widely adopted international standard on risk management.

For each operational risk, one or more impacts are identified. In the example below, Risk 101 has two impacts. Both impacts are negative impacts and this is represented with the red background color.

In the example below, Risk 102 has three impacts. Impacts 111 and 112 are negative impacts. Impact 113 is a positive impact and this is represented with the green background color.

For each impact, an assessment of Likelihood & Impact is performed.

For negative impacts, the matrix below is used to derive the “Impact Level” for each impact.

Impact	Very High	Low	Medium	High	Very High	Very High
	High	Low	Medium	High	Very High	Very High
	Medium	Low	Low	Medium	High	High
	Low	Very Low	Low	Low	Medium	Medium
	Very Low	Very Low	Very Low	Low	Low	Low
		<=10%	11% to 25%	25% to 50%	50% to 90%	>=91
		Very Low	Low	Medium	High	Very High
		Likelihood				

For positive impacts, the matrix below is used to derive the “Impact Level” for each impact.

Impact	Very High	Low	Medium	High	Very High	Very High
	High	Low	Medium	High	Very High	Very High
	Medium	Low	Low	Medium	High	High
	Low	Very Low	Low	Low	Medium	Medium
	Very Low	Very Low	Very Low	Low	Low	Low
		<=10%	11% to 25%	25% to 50%	50% to 90%	>=91
		Very Low	Low	Medium	High	Very High
		Likelihood				

The example below highlights the concepts discussed above for 2 risks.

Risk 101		Likelihood	Impact	Impact Level
	Impact 101	Very Low	Medium	Low
	Impact 102	Medium	Low	Low

Risk 102		Likelihood	Impact	Impact Level
	Impact 111	Low	Very High	Medium
	Impact 112	High	High	Very High
	Impact 113	Low	Very High	Medium

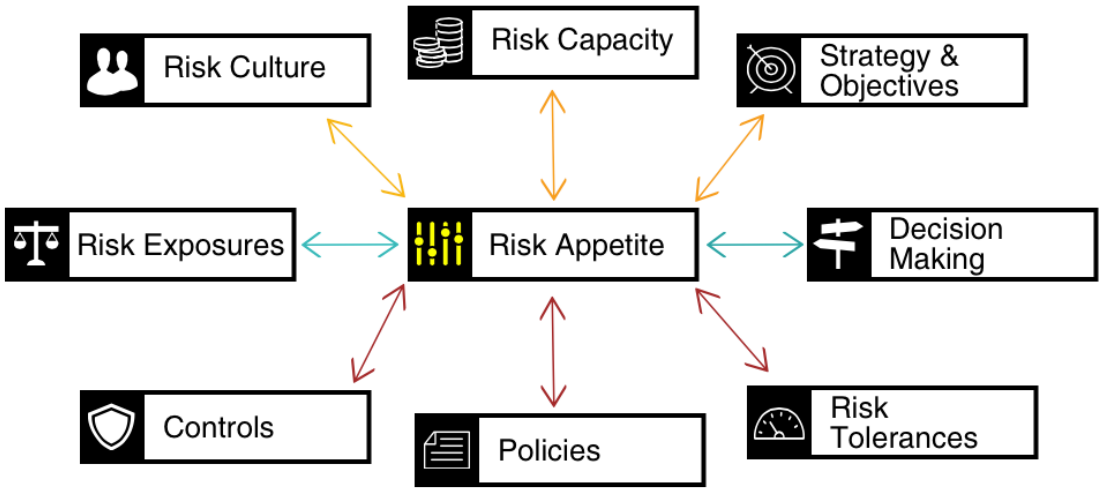
Based on pre-defined aggregation criteria, the assessment of individual impacts is aggregated at the risk level. The negative impacts are aggregated as threats posed by the risk and the positive impacts are aggregated as opportunities presented by the risk.

The example below highlights aggregation for two risks.

	Threats			Opportunities			
	Overall Likelihood	Overall Impact Level	Overall Threat Level	Overall Likelihood	Overall Impact Level	Overall Opportunity Level	Overall Threat or Opportunity
Risk 101	Medium	Medium	Medium	N.A.	N.A.	N.A.	Threat
Risk 102	High	Very High	Very High	Low	Very High	Medium	Threat

Risk Appetite – Related Concepts

The diagram below highlights the various concepts that RWS Bank has considered when defining their risk appetite.



Driving Concepts

The three most important concepts which influence risk appetite framework include: -

- Risk Culture
- Risk Capacity
- Strategy & Objectives

Application Concepts

The two key areas where risk appetite is applied include: -

- Evaluating Risk Exposures
- Decision Making

Implementation Concepts

The three most common methods for implementing risk appetite include: -

- Controls
- Policies
- Risk Tolerances

Operational Risk Appetite Statement for RWS Bank

Version: 1.0

Published Date: 27th August 2015

Information Classification: Confidential

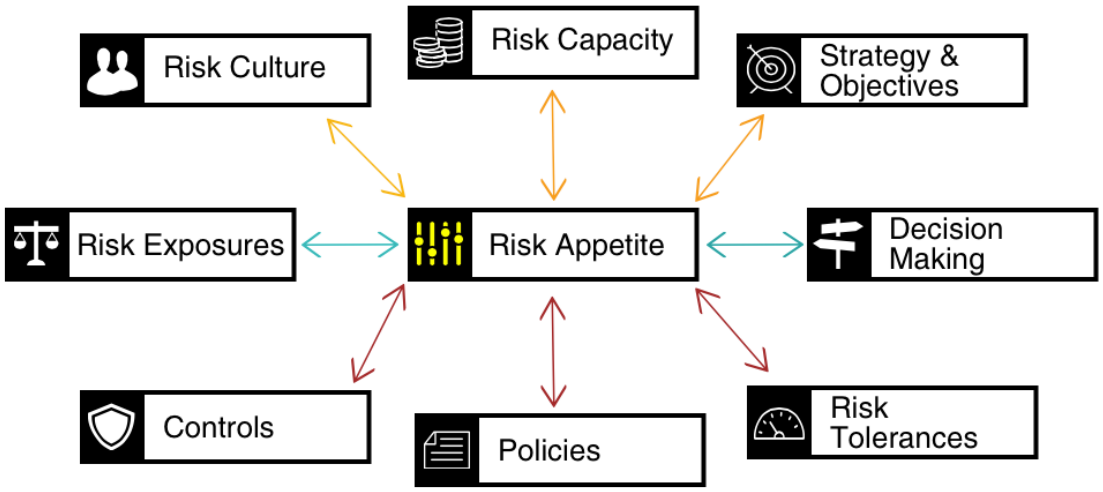
Table of Contents

Introduction

The purpose of this document is to define and communicate key operational risk appetite related concepts and criteria, as covered within the operational risk appetite framework of the bank. The content of this document should provide clear guidance to the reader on which operational risk exposures are acceptable and unacceptable to the bank. Such clarity can facilitate risk-informed decision making across the bank on operational risk related topics.

This document has been reviewed and approved by the Board of the bank.

The diagram below highlights the various concepts that have been considered when defining the risk appetite of the bank: -



Purpose of the Operational Risk Appetite Statement

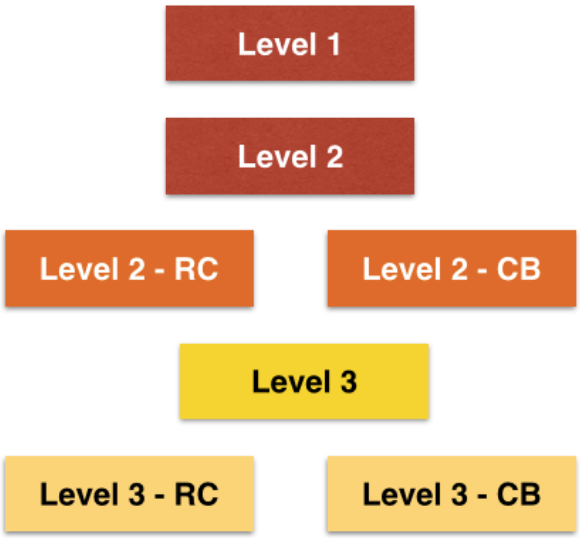
The bank has identified that the risk appetite statement should be a valuable reference in the following scenarios: -

- When an individual or groups are making a significant business decision related to the business operations of the bank. Examples of such decisions may include outsourcing significant processes or IT systems, introducing new technology within products & expanding into new geographic locations. In such scenarios, the statement should provide clear guidance on the bank's approach towards which operational risks are acceptable and unacceptable.

- When an individual or groups are performing risk assessments and they need to identify whether the risk exposures are aligned with the bank's approach towards acceptable and unacceptable operational risks.
- When a new board member or senior executive joins the bank and needs to understand the bank's approach towards which operational risks are acceptable and which are unacceptable.
- When an external stakeholder (e.g. regulator) wants to review the bank's approach towards which operational risks are acceptable and those that are unacceptable.

Risk Criteria

The guidance on acceptable and unacceptable operational risks is defined in the form of risk criteria, which are covered within this document. The risk criteria have been categorized into multiple levels, which are highlighted below.

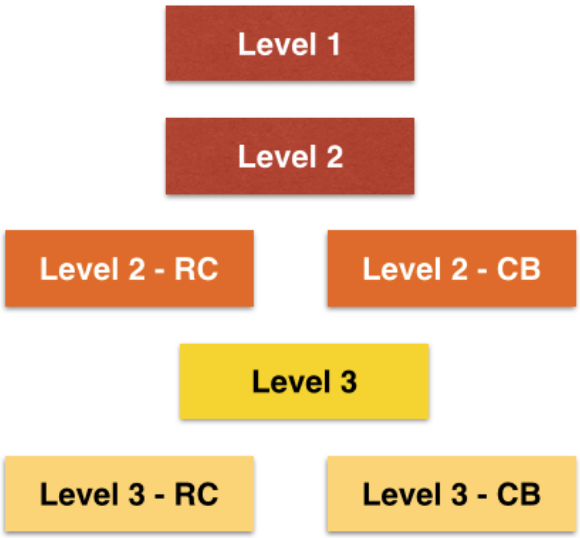


Level 1 provides guidance on operational risks that are unacceptable under all circumstances. Other levels provide guidance on operational risks that are avoidable under all circumstances but the bank may have to accept a higher level of exposure due to one or more of the following reasons: -

- Choice to benefit from potential opportunities associated with the risks
- Resource Constraints
- The benefits of risk treatments (e.g. controls) do not justify the level of investments required to implement the risk treatments.

Risk Criteria Levels

The diagram below highlights the different levels used for categorizing the set of criteria, defined as part of guidance on risk appetite for operational risks. The levels defined below are used to structure the “Risk Appetite Breach Report”, which is the main communication method used for communicating risk appetite breach related information.



The following table covers the details of the various criteria that are applied to identify if exposure of a risk is in breach of bank’s risk appetite. Any risk that meets the criteria defined below should be covered within the “Risk Appetite Breach Report”.

Level 1

In this level, the bank includes the following types of risks: -

- Risks which are unacceptable under any circumstances and the Overall Threat Likelihood of risk is not “Very Low”

The bank will not accept risks under any circumstances that fall under the below defined criteria: -

- Where the risk involves intentionally breaching one or more laws or regulations. Examples include: -
  - Intentionally mis-selling products/services to clients
  - Intentionally selling products/services to clients who are covered by national or international embargoes and sanctions
  - Intentionally providing incorrect information to regulators or law enforcement agencies

- Where the risk involves potential exposure to significant physical injury or loss of life for employees. Examples include: -
  - Harassment of employees by their managers or colleagues
  - Discrimination of employees by their managers or colleagues
  - Exposing employees to faulty machines or equipment
  - Exposing employees to machines or equipment, where this may result in detrimental known impact on health of the employee

- Where the risk involves potential exposure to significant physical injury or loss of life for external stakeholders such as customers and suppliers. Only the risks owned by the bank should be considered. Examples include: -
  - Harassment of external stakeholders by staff or executives
  - Exposing external stakeholders to faulty machines or equipment
  - Exposing stakeholders to machines or equipment, where this may result in an known detrimental impact on health of the stakeholders

- Where the risk may breach the firm's zero tolerance for the following types of fraud and corruption: -
  - Accepting or offering bribes by any employee
  - Embezzlement or misuse of assets for personal gains by employees in Grade A, B, C and D (these grades cover middle management and senior executives, including board members)
  - Financial statement fraud by employees in Grade A, B, C, D (these grades cover middle management and senior executives, including board members)

Level 2

In this level, the bank includes the following types of risks: -

- Risks which are avoidable under all circumstances and
  - the Overall Threat Likelihood of risk is “High” or above and
  - the bank has resources to prevent the risk and
  - the benefits of risk treatment (e.g. controls) justifies the level of investments required to implement the risk treatments

Risks meeting the following criteria should be considered under this level: -

Customers

- Where the risk may result in customers being unable to access or operate their accounts held with the bank.
- Where the risk may result in the bank unintentionally providing incorrect information to customers regarding their accounts, funds or products.
- Where the risk may result in incorrect charges or transactions added to the customer accounts.
- Where the risk may result in unintentional damage (including theft) to customer funds and/or assets.
- Where the risk may result in an increase in the level of yearly customer churn beyond 12%
- Where the risk may result in decrease in the level of new customer acquisition below 5%

Information & IT Systems

- Where the risk may result in the bank unintentionally sharing information (e.g. about customers, employees, suppliers) with inappropriate individuals, business units or external organizations.
- Where the risk may result in disruption to key non-customer related IT Systems (e.g. Corporate Balanced Scorecard, Payroll Processing etc.)

Laws, Regulations & Obligations

- Where the risk may result in the bank unintentionally breaching one or more laws or regulations.
- Where the risk may result in the bank unintentionally breaching its contractual obligations to third parties.

Theft & Fraud

- Where the risk may result in theft or fraud committed by employees in Grade E and below.
- Where the risk may result in theft or fraud committed by external parties.

Employee

- Where the risk may result in an increase in the level of staff turnover beyond 20%

Financial

- Where the total potential negative financial consequences of a risk is more than 20% of the total budget of the business unit where the risk is owned.

Level 2 – RC (Resource Constraints)

In this level, the bank includes the following types of risks: -

- Risks which are avoidable under all circumstances and
  - the Overall Threat Likelihood of risk is “High” or above and
  - the bank does not have adequate levels of resources to prevent the risk

Risks within the criteria defined for Level 2 should also be considered for this level.

By defining this level, the bank recognizes that it may not be able to mitigate all high exposure risks due to lack of adequate resources. However, by informing the board and senior executives about such risks, the bank can make an informed decision to retain high levels of exposure for such risks.

Level 2 – CB (Cost-Benefit)

In this level, the bank includes the following types of risks: -

- Risks which are avoidable under all circumstances and
  - the Overall Threat Likelihood of risk is “High” or above and
  - the benefits of risk treatment (e.g. controls) does not justify the level of investments required to implement the risk treatments

Risks within the criteria defined for Level 2 should also be considered for this level.

By defining this level, the bank recognizes that it may not be able to mitigate all high exposure risks when the benefits of risk treatment does not justify the level of investments required to implement the risk treatments. However, by informing the board and senior executives about such risks, the bank can make an informed decision to retain high levels of exposure for such risks.

Level 3

In this level, the bank includes the following types of risks: -

- Risks which are avoidable under all circumstances and
  - the Overall Threat Likelihood of risk is below “High” and
  - the Overall Threat Level is above the Target Threat Level defined for the risk and
  - the bank has resources to prevent the risk and
  - the benefits of risk treatment (e.g. controls) justifies the level of investments required to implement the risk treatments

Bank’s operational risk framework requires risk owners to define a Target Threat Level for each risk owned by them.

By defining this level, the bank wants to escalate any low or medium exposure risks that are beyond their pre-defined Target Threat Level.

Risks within the criteria defined for Level 2 should also be considered for this level.

Level 3 – RC (Resource Constraints)

In this level, the bank includes the following types of risks: -

- Risks which are avoidable under all circumstances and
  - the Overall Threat Likelihood of risk is below “High” and
  - the Overall Threat Level is above the Target Threat Level defined for the risk and
  - the bank does not have adequate levels of resources to prevent the risk

By defining this level, the bank wants to escalate any low or medium exposure risks, which are beyond their pre-defined Target Threat Level and recognize that it is unable to further mitigate such risks due to lack of adequate resources. However, by informing the board and senior executives about such risks, the bank can make an informed decision to retain current levels of exposure for such risks.

Risks within the criteria defined for Level 2 should also be considered for this level.

Level 3 – CB (Cost-Benefit)

In this level, the bank includes the following types of risks: -

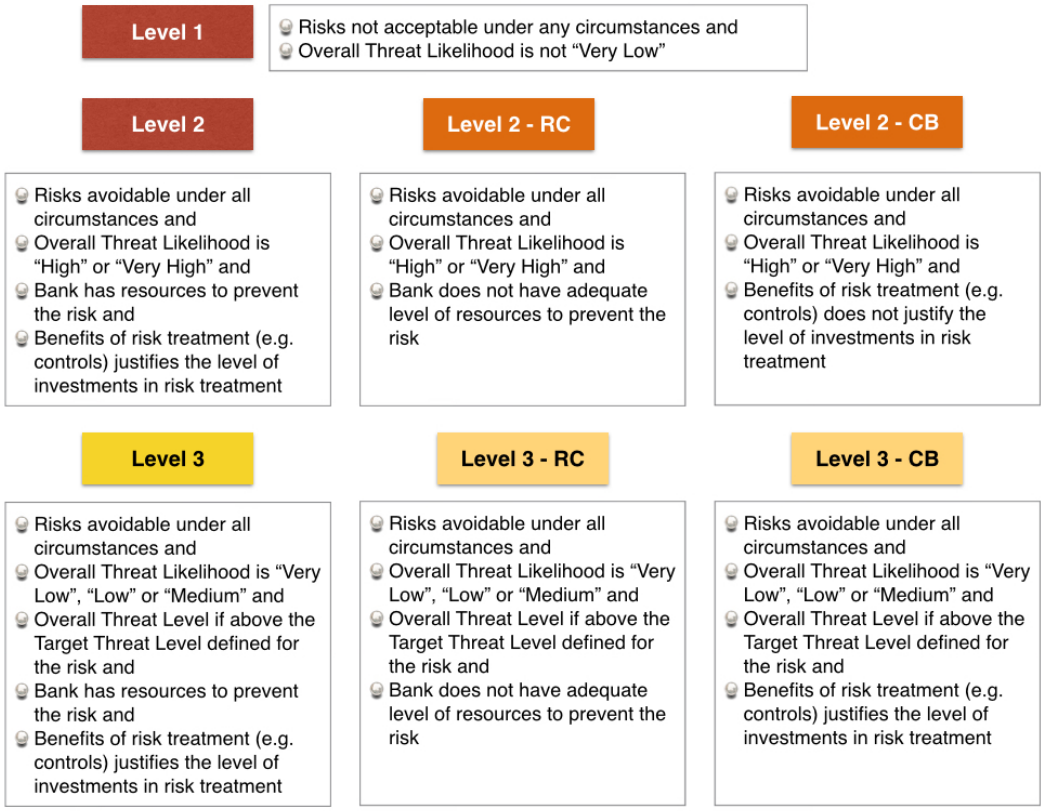
- Risks which are avoidable under all circumstances and
  - the Overall Threat Likelihood of risk is below “High” and
  - the Overall Threat Level is above the Target Threat Level defined for the risk and
  - the benefits of risk treatment (e.g. controls) does not justify the level of investments required to implement the risk treatments

By defining this level, the bank wants to escalate any low or medium exposure risks, which are beyond their pre-defined Target Threat Level and recognize that it is unable to further mitigate such risks because the benefits of risk treatments does not justify the level of investments required to implement the risk treatments. However, by informing the board and senior executives about such risks, the bank can make an informed decision as whether to retain current level of exposure for such risks.

Risks within the criteria defined for Level 2 should also be considered for this level.

Summary of Levels & Related Criteria

The table below highlights all the risk appetite levels and their related criteria.



Loss Thresholds

The bank has also defined the loss event thresholds below for the current financial year. This is the maximum amount of loss the bank will tolerate.

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

The following information should be included in the Risk Appetite Breach Report: -

- **Potential Breach of Loss Thresholds**: - This section should contain list of all risk categories, where the actual year to date loss is above 60% & less than 100% of the above thresholds. Details of any significant losses for each category included in the report should also be provided.
- **Actual Breach of Loss Thresholds**: - This section should contain list of all risk categories, where the actual year to date loss is 100% or more of the above thresholds. Details of any significant losses for each category included in the report should also be provided.

In addition to information mentioned above, risks meeting the following loss event criteria should also be included in the Risk Appetite Breach Report: -

- **Potential Breach Based on Previous Year**: - This section should contain list of all risks, where the actual year to date loss is above 60% & less than 100% of the total loss amount for the same risk in the last financial year. Only risks with actual year to date loss amount of more than $250,000 should be included in the report.
- **Actual Breach Based on Previous Year**: - This section should contain list of all risks, where the actual year to date loss is 100% or more of the total loss amount for the same risk in the last financial year. Only risks with actual year to date loss amount of more than $250,000 should be included in the report.

Risk Appetite Breach Report

The Risk Appetite Breach Report is the main channel used for escalating risks to the board, risk committee, audit committee and senior executives.

The report is created quarterly by the Group OpRisk Reporting team and made available via the Risk Dashboard.

Two versions of the report are created: -

1. **Group Level***: This report contains risks covered under the following levels defined earlier in this document: -
   - Level 1
   - Level 2
   - Level 2 – RC
   - Level 2 – CB

   Additionally, information highlighted in the Loss Threshold section should also be included in this report.

   This report is presented to the following stakeholders: -
   - Risk Committee
   - Audit Committee
   - Board Members
   - Executive Committee (consisting of CEO, CRO, COO, CFO etc.)
   - Group OpRisk Committee

**Note the risks related to Level 3 are not included in this report to facilitate above stakeholders to focus on the most important risks for the bank at the group level.*

2. **Business Unit Level**: This report is created for each business unit to facilitate escalation of risks at the business unit level. This report contains risks covered under all levels defined earlier in this document.

   Additionally, information highlighted in the Loss Threshold section should also be included in this report.

   This report is presented to the following stakeholders: -
   - CRO
   - Group OpRisk Committee
   - Head of Business Unit
   - OpRisk Manager responsible for the Business Unit
   - Business Unit Level Risk Committee, if present

Including Business Context Information

To ensure that the decision makers get a holistic view of each risk included within the Risk Appetite Breach Report, the risk owners should also include any business context information related to the risk within the report. Business context can cover the types of information outlined below: -

- List the key strategic and/or operational objectives which may be influenced by the risk
- Explanation of threats and opportunities associated with the risk
- Explanation of resource constraints which may be preventing risk owner from implementing risk treatments
- Explanation of cost-benefit analysis done on benefits from additional risk treatment and the level of investment required in such treatment
- Explanation of recent loss events associated with the risk
- Explanation of any open issues associated with the risk and related remediation actions
- Explanation of any key risk indicators associated with the risk and their recent performance
- Explanation of any external information associated with the risk. This may include loss events at other banks, warning by regulators, emerging trends/patterns etc.

Evaluating Threats and Opportunities

The current level of threat related measures are mainly used to include a risk within the Risk Appetite Breach Report. However, in certain cases the decision makers would also need to consider any opportunities corresponding to the threat related measures included in the report. Any decision related to implementation of further risk treatment for risks included in the report should be based on a balanced view of the level of threat and any corresponding opportunities. This will enable the decision makers to take a holistic view and balance the various strategic and operational objectives that may be influenced by the risk.

Example 1 – Increase in credit card fraud

The credit card team continuously introduces new technological features within credit card products. Such innovative measures are needed to maintain a competitive advantage against our key competitors. Such innovative measures have also resulted in increase in the value of the bank's brand over the last five years, especially within the customers aged between 18 and 30, which constitutes 80% of our current customer base.

However, due to the high level of uncertainty associated with new technological features, the credit card team typically expects an increase in the level of credit card fraud exposure during the first 6 months of introducing such features. Appropriate levels of risk treatments are implemented during the 6 months to closely monitor any actual increase in fraud and maintain these within pre-defined target levels.

In such cases, the credit card fraud related risks might be included within Level 2 or Level 3 sections of the report. However, the decision makers will need to weigh the threat level against the opportunities associated with such risk in the form of maintaining a competitive advantage, maintaining the brand value and level of satisfaction within customers.

Implementing Risk Appetite through Risk Tolerances

The risk appetite levels and their associated criteria should be implemented in the form of risk tolerances. This is implemented through the definition of upper and lower thresholds on key business objectives.

Example: -

Business Objective	Maintain annual customer churn under 9%
Lower Threshold	7%
Upper Threshold	12%

Any business decision taken within the bank that may impact a given business objective should consider the defined thresholds. All business decisions should aim to maintain the performance within the defined thresholds. If a business decision needs to be taken which may breach the defined threshold, then the OpRisk Manager responsible for the business unit (where the decision needs to be taken) should approve such business decisions.

Implementing Risk Appetite through Policies

The risk appetite levels and their associated criteria should also be implemented through new policies or clauses within existing policies, where appropriate.

Example: -

- The criteria defined in Level 1 around safety of employees and external stakeholders should be implemented through clauses within the Health & Safety Policy
- The criteria defined in Level 1 around zero tolerance for bribery should be implemented through clauses within the Anti-Bribery Policy
- The criteria defined in Level 2 around unintentionally sharing customer information should be implemented through clauses within the Information Security Policy

Implementing Risk Appetite through Controls

The risk appetite levels and their associated criteria should also be implemented through implementation of controls, where appropriate.

Example: -

- The criteria defined in Level 1 around safety of employees and external stakeholders should be implemented through controls such as Fire Safety training, Performing health and safety due diligence when buying new equipment etc.
- The criteria defined in Level 1 around zero tolerance for bribery should be implemented through controls such as yearly anti-bribery training, performing corruption related due diligence before starting conducting business with any external organization etc.
- The criteria defined in Level 2 around unintentionally sharing customer information should be implemented through controls such as classification of information based on level of confidentiality, approval process before authorizing an individual access to IT systems with sensitive information etc.

Aligning Risk Appetite with Risk Capacity

The bank has a finite amount of risk capacity, which is defined as “The maximum level of resources the bank can invest or expose in managing its risks without requiring a significant change to its business strategy”. The risk capacity of the bank consists of the following: -

- Budget or provision allocated for expected operational risk losses (e.g. credit card fraud, legal fees)
- Capital allocated for operational risks across the various business units
- Reserves which can be accessed for unexpected operational risk losses

The risk capacity of the bank will continue to evolve with its business strategy and hence it is important that it is aligned with the various criteria associated with the risk appetite levels.

Customize Risk Appetite Statement for Business Units

This risk appetite statement has been defined to be applicable for the group level of the bank and hence any context specific to business units has not been included. It is expected that individual business units will utilize this document as a basis for creating a risk appetite statement document for risk owners and other stakeholders within their business unit. Such customized statements should include context information specific for the business unit, so its content can be relevant for the consumers of the statement within the business unit.

Such customization should retain the criteria defined within Level 1 of this document. New criteria can be added but existing criteria cannot be modified or removed. Business units can make any changes to criteria defined in all other levels.

The Group Risk Appetite Framework Team should approve any business unit specific version of risk appetite statements.

If a business unit does not define a customized version of the risk appetite statement, then this document will be applicable for all risk appetite related activities (e.g. reporting) of such business units.

Monitoring Risk Appetite

In addition to the Risk Appetite Breach Report, risk owners should also define one or more indicators for their risks to monitor potential or actual breach of any criteria defined earlier in this document. Continuous monitoring risks using such indicators can provide risk owners with information on a timely basis. Without such information, risk owners may only find out about potential breaches during the quarterly assessments and this may sometimes restrict the amount of time available to risk owners for making decisions related to potential breach of risk appetite.

Examples of such monitoring indicators may include: -

- Number of whistleblowing issues reported in last one week
- Number of new issues created for a risk in last one week
- Number of new loss events reported for a risk in last one month
- Number of exceptions raised in last one month for specific policies such as Anti-Bribery Policy, Information Security Policy etc.
- Number of audit findings raised for a risk in last one month

Risk Appetite & Risk Culture

The bank defines risk culture as “Set of shared beliefs and values regarding management of risks”. The bank recognizes that risk culture is a very important factor driving the risk appetite. However, the bank also pro-actively intends to use the risk appetite to influence the risk culture, so the risk culture can facilitate the bank to achieve its business objectives.

Review of Risk Appetite Statements

The Group and Business Unit Risk Appetite Statements should be reviewed annually as part of the overall OpRisk Framework & Process Review process. The Group OpRisk Committee should approve any changes to the statements.

End of the Risk Appetite Statement for RWS Bank

Authors

Manoj Kulwal
Manoj is currently the Co-Founder & Chief Risk Officer at RiskSpotlight. He is responsible for management of strategic, operational & compliance risks related to the RiskSpotlight business. He has developed an ERM framework for RiskSpotlight, based on best practices within external frameworks such as ISO 31000, COSO ERM & OCEG's GRC Capability Model.

He also leads the content development initiatives at RiskSpotlight. He is also involved with strategic consulting & training engagements. He has 18 years of industry experience and holds an Executive MBA from Cass Business School, UK.

He hosts & publishes RiskStudio, which is a bi-monthly podcast on risk management topics.

He is member of the UK committee, which is currently providing recommendations to ISO on the ongoing revision of the ISO 31000 standard. He is also part of the Chartis Advisory Board where he provides guidance on risk management related topics.

Simon Wilkins
Simon is the Co-Founder & CEO at RiskSpotlight. He leads the consulting, business development, commercial & partnership related initiatives at RiskSpotlight. He has over 22 years of experience within the financial services industry as a Management Consultant. He has focused on operational risk over the last 10 years leading major change programmes related to Basel and Solvency II at global financial services organizations.

In addition to his responsibilities at RiskSpotlight, he is also CEO of SolvRisk and a regular contributor to financial services publications on regulatory change.

More Guidance on Operational Risk Appetite

RiskSpotlight can provide additional guidance on Operational Risk Appetite through: -

Training

RiskSpotlight periodically organizes online training course titled “Practical Approaches For Implementing An Operational Risk Appetite Framework”. This is a three-hour interactive online course conducted by Manoj Kulwal. As this is an online course, you can attend the course from anywhere in the world just with a computer and internet connection.

RiskSpotlight can also customize the above course based on your operational risk framework and deliver it onsite for your operational risk management stakeholders.

Visit www.riskspotlight.com/training to find out more about the risk appetite related and other risk management courses.

Consulting

You can also get access to additional guidance on operational risk appetite through RiskSpotlight’s consultancy services. Our consultancy services are focused on delivering concrete benefits to our clients. We can provide following types of consulting services on this topic: -

- Share external guidance and best practices on operational risk appetite
- Collaborating with your operational team to develop a new operational risk appetite framework for your organization
- Evaluating your current operational risk appetite framework and providing advise on the strengths and gaps within the framework

Visit www.riskspotlight.com/consulting to find out more about our risk appetite related and other consulting services.

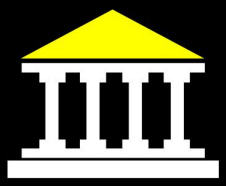
RiskSpotlight

RiskSpotlight focuses on providing specialized content, consulting and training services related to risk management. Following are some of the main offerings from RiskSpotlight (click on the each offering to visit the website for more details).

RiskSpotlight Portal

- ✓ A web-based subscription service providing access to news articles, organised by 125 operational risks for financial services firms.
- ✓ Articles are updated on daily basis, so you can get access to the most recent news articles for any of the 125 operational risks.
- ✓ Access to such news articles can be valuable input for risk assessments, scenario development and external monitoring of risks.

See more details...



Operational Risk Library

- ✓ Fully populated library of 125 operational risks for financial services firms.
- ✓ For each risk, the following content is provided:
  - Causes
  - Controls
  - Key Risk Indicators
  - Early Signs of Risk
  - Financial Impacts
  - Reputational Impacts
  - Business Impacts
- ✓ The library can be used to fast-track development of your internal library of risks, controls or key risk indicators.

See more details...

Conduct Risk Library

- ✓ Fully populated library of 44 key conduct risks for financial services firms.
- ✓ For each risk, the following content is provided:
  - Causes
  - Controls
  - Key Risk Indicators
  - Early Signs of Risk
  - Financial Impacts
  - Reputational Impacts
  - Business Impacts
- ✓ The library can be used to fast-track development of your internal library of risks, controls or key risk indicators.

See more details...

Visit www.riskspotlight.com for details of additional offerings and risk management resources.