

# THE ROLES OF RISK APPETITE AND TOLERANCE

Caroline McMichen, CCEP, CIA



[ 1 ]

1

## The Roles of Risk Appetite and Tolerance

In the session, we will discuss:

- what we mean by Risk Appetite and Tolerance
- how they are determined and how they inform Business Strategy and Objective-Setting
- how they can be applied to Compliance and Ethics Risks, Risk Management and Mitigation



[ 2 ]

2

## What do we mean by Risk Appetite and Tolerance?

- **Risk** – The possibility that events will occur and affect the achievement of strategy and business objectives\*
  - **Compliance Risks** are those *“relating to possible violations of applicable laws, regulations, contractual terms, standards, or internal policies where such violation could result in direct or indirect financial liability, civil or criminal penalties, regulatory sanctions, or other negative effects for the organization or its personnel.”\*\**
- **Risk Appetite** – The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value\*
- **Tolerance** – The boundaries of acceptable variation in performance related to achieving business objectives\*

\* Source: COSO Enterprise Risk Management

\*\* Source: Compliance Risk Management: Applying the COSO ERM Framework



3

3

## Polling Question

Has your organization established its risk appetite and tolerance levels as part of its overall Risk Management process?






- Yes
- No
- I don't know



4

4

# COSO ERM Principles

 Governance & Culture	 Strategy & Objective-Setting	 Performance	 Review & Revision	 Information, Communication, & Reporting
<ol style="list-style-type: none"><li>1. Exercises Board Risk Oversight</li><li>2. Establishes Operating Structures</li><li>3. Defines Desired Culture</li><li>4. Demonstrates Commitment to Core Values</li><li>5. Attracts, Develops, and Retains Capable Individuals</li></ol>	<ol style="list-style-type: none"><li>6. Analyzes Business Context</li><li>7. Defines Risk Appetite</li><li>8. Evaluates Alternative Strategies</li><li>9. Formulates Business Objectives</li></ol>	<ol style="list-style-type: none"><li>10. Identifies Risk</li><li>11. Assesses Severity of Risk</li><li>12. Prioritizes Risks</li><li>13. Implements Risk Responses</li><li>14. Develops Portfolio View</li></ol>	<ol style="list-style-type: none"><li>15. Assesses Substantial Change</li><li>16. Reviews Risk and Performance</li><li>17. Pursues improvement in Enterprise Risk Management</li></ol>	<ol style="list-style-type: none"><li>18. Leverages Information and Technology</li><li>19. Communicates Risk Information</li><li>20. Reports on Risk, Culture, and Performance</li></ol>

Source: COSO, *Enterprise Risk Management – Integrating with Strategy and Performance* (June 2017)



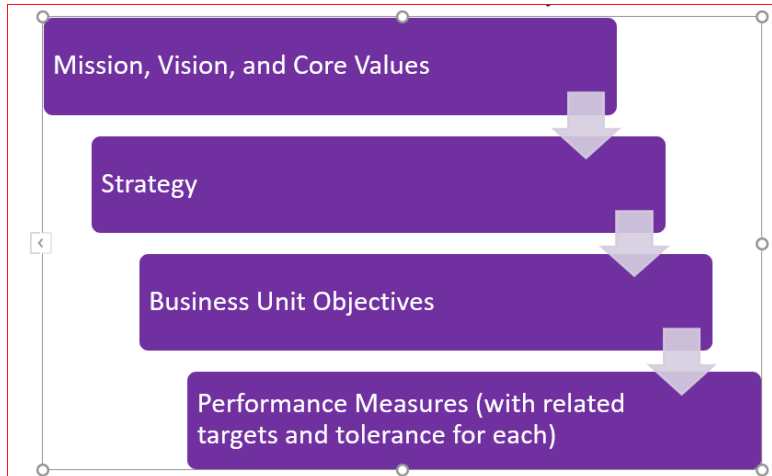
## COSO ERM Principle 7: Defines Risk Appetite

When determining Risk Appetite, leadership must consider:

- organization's vision, mission and strategy
- board and management perspectives on risk and risk appetite
- existing risk profile of the organization
- organizational culture
- shareholder interests



## COSO ERM Principle 7: Defines Risk Appetite



Adapted from *Risk Appetite – Critical to Success: Using Risk Appetite to Thrive in a Changing World*, COSO, May 2020



[ 7 ]

7

## COSO ERM Principle 7: Defines Risk Appetite

Once determined, Risk Appetite should be:

- communicated clearly
- applied to objective-setting and decision-making
- used to allocate resources
- used to develop tolerance measures for use in monitoring performance



[ 8 ]

8

## COSO ERM Principle 7: Defines Risk Appetite

Sample questions to facilitate questions on risk appetite:

- Do you believe management’s process for identifying, assessing and managing risk is effective?
- Is the organization’s strategy aligned with its risk appetite – or does there appear to be a conflict?
- Do compensation plans reflect existing risk appetite, or might they incent employees to take greater risk than acceptable?
- Are there areas in the organization where you feel the risk appetite is too high. Too low?



{ 9 }

9

## COSO ERM Principle 7: Defines Risk Appetite

A **risk appetite statement** “effectively sets the tone for risk management”. It “should be articulated and communicated so that personnel understand that they need to pursue objectives within acceptable limits.”

The statement:

- should be linked to operational, compliance, and reporting objectives
- will vary by organization
- must be clearly communicated and able to be implemented and monitored across the organization

Source: Adapted from COSO Enterprise Risk Management – Understanding and Communicating Risk Appetite by Dr. Larry Rittenberg and Frank Martens



{ 10 }

10

## COSO ERM Principle 7: Defines Risk Appetite

Example Risk Appetite Statement for a healthcare organization:

*“The Organization **operates within a low overall risk range**. The Organization’s **lowest risk appetite relates to safety and compliance objectives**, including employee health and safety, with **a marginally higher risk appetite towards its strategic, reporting, and operations objectives**. This means that reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment, and meeting our legal obligations will take priority over other business objectives.”*

Source: COSO Enterprise Risk Management – Understanding and Communicating Risk Appetite by Dr. Larry Rittenberg and Frank Martens



11

11

## COSO ERM Principle 7: Defines Risk Appetite

While risk appetite may be broadly defined, **risk tolerance** represents the application of risk appetite to specific objectives.

**Risk tolerance:**

- Represents the acceptable level of variation relative to achievement of a specific objective or performance measure
- is best measured in the same units as those used to measure the related objective
- considers the relative importance of the related objective and aligns with risk appetite

Source: Adapted from COSO Enterprise Risk Management – Understanding and Communicating Risk Appetite by Dr. Larry Rittenberg and Frank Martens



12

12

## COSO ERM Principle 7: Defines Risk Appetite

Example Risk Tolerance aligned with Risk Appetite for a healthcare organization:

Risk Appetite	Risk Tolerance
A health services organization places patient safety amongst its highest priorities. The organization also understands the need to balance the level of immediate response to all patient needs with the cost of providing such service. The organization has a <b>low risk appetite related to patient safety but a higher appetite related to response to all patient needs.</b>	We strive to treat all emergency room patients within two hours and critically ill patients within 15 minutes. However, management accepts that in rare situations (5% of the time) patients in need of non-life-threatening attention may not receive that attention for up to four hours.

Source: COSO Enterprise Risk Management – Understanding and Communicating Risk Appetite by Dr. Larry Rittenberg and Frank Martens



13

13

## Risk Appetite and Tolerance Approaches to Risk Mitigation

Management will determine the appropriate strategy for a particular risk after 1) analyzing the likelihood of occurrence and impact to the organization if it should occur, and 2) considering the organization's established risk appetite. These approaches are:

- Avoidance**
  - Discontinuing the activity that creates the risk.
- Reduction**
  - Taking action to reduce likelihood or impact related to the risk (e.g control activities, monitoring).
- Share or Insure**
  - Transferring/sharing a portion of the risk to reduce the impact.
- Accept**
  - No action is taken due to cost/benefit analysis or risk is determined to be at an acceptable level.



14

14

## Risk Appetite and Tolerance Applied to C&E Risks and Programs

In determining compliance risk appetite, consider:

- the organization's (Board and management) perspective on the level of acceptance of compliance risk in the pursuit of business objectives
- the current compliance risk profile of the organization
- the organization's culture
- shareholder interests



[ 15 ]

15

## Risk Appetite and Tolerance Applied to C&E Risks and Programs

Consider compliance risk by:

- type of risk,
- business unit or organizational function, and/or
- location or region.

*How might they differ?*

*What makes sense for your organization?*



[ 16 ]

16



## Risk Appetite and Tolerance Applied to C&E Risks and Programs

Determine and evaluate the relationships between compliance risks and the achievement of business objectives. Consider:

- how business objectives affect compliance risks.
- how responses to compliance risks may affect achievement of business objectives.
- how responses to other risks (e.g. strategic, financial, operational) may affect compliance risks.
- how responses to compliance risks may affect other risks.

*What role might risk appetite play?*

17



17

## Risk Appetite and Tolerance Applied to C&E Risks and Programs

Discuss risk appetite on a regular basis and update as necessary based on changes in compliance risk.

- As part of compliance risk assessment
- In business strategy and objective-setting meetings
- In regular discussions with senior leadership and the Board
- In reviewing results of monitoring or auditing activities

18



18

# Risk Appetite and Tolerance Applied to C&E Risks and Programs

Develop risk-centric appetite statements and tolerances associated with compliance risks. They can be:

- **Broad statement regarding regulatory compliance**  
Example: *“The Organization operates within a low overall risk range. The Organization’s lowest risk appetite relates to safety and compliance objectives, including employee health and safety, with a marginally higher risk appetite towards its strategic, reporting, and operations objectives. This means that reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment, and meeting our legal obligations will take priority over other business objectives.” – a Healthcare Company*
- **Specific to a particular risk area such as Corruption, Privacy, Competition etc.**  
Example: *“The Bank has no appetite for any dishonest or fraudulent behaviour and is committed to deterring and preventing such behaviour. It takes a very serious approach to cases, or suspected cases, of fraud or corruption perpetrated by its staff, and responds fully and fairly in accordance with provisions of the Code of Conduct.” – Reserve Bank of Australia*



# Risk Appetite and Tolerance Applied to C&E Risks and Programs

Examples Compliance Risk Appetite statements and related Risk Tolerance:

Risk Appetite	Risk Tolerance
<b><i>Company has a low risk appetite for compliance and ethics violations.</i></b>	All employees are required to complete Code of Conduct training upon hire and annually thereafter. Management accepts a 95% completion rate for the annual Code of Conduct training.
<b><i>Company has a very low risk appetite for corruption and bribery.</i></b>	Compliance due diligence is conducted prior to contracting with high risk third parties. Diligence may be reduced if third party passes initial screening and is considered low risk.



# Risk Appetite and Tolerance Applied to C&E Risks and Programs

## Use of Risk Appetite and Tolerance in Risk Remediation, Monitoring and Auditing

Consider Risk Appetite when:

- determining the best approach to risk mitigation
- designing control activities to mitigate compliance risk
- developing tolerance levels for possible control failure

Consider both Risk Appetite and Tolerances when:

- evaluating the effectiveness of internal control activities
- analyzing results of monitoring or auditing efforts and determining whether further remediation is needed



21

21

## Key Takeaways

- ✓ *Risk Appetite and Tolerance, though related, are different concepts*
- ✓ *Management must consider various perspectives when defining Risk Appetite*
- ✓ *Risk Appetite should inform strategy and objective setting in an organization*
- ✓ *Risk Appetite should be clearly communicated so that it can be applied to decision-making throughout the organization*
- ✓ *Tolerance should be applied to performance metrics at the objective level*
- ✓ *Risk Appetite and Tolerance should be re-evaluated regularly*



22

22