Canadian Institute of Actuaries
Institut canadien des actuaires

Practice Resource Document

Risk Appetite

Committee on Enterprise Risk Management

November 2021

Document 221124

Ce document est disponible en français

© 2021 Canadian Institute of Actuaries

The actuary should be familiar with relevant practice resource documents. They do not constitute standards of practice and are, therefore, not binding. They are, however, intended to assist members in considering whether they have addressed all relevant topics within a practice area. These may include skills and knowledge inventories (SKI), a compilation of other relevant material (internal or external to the CIA) related to the practice, as well as recognized best practices, where appropriate.

Canadian Institute of Actuaries / Institut canadien des actuaires

MEMORANDUM

To: Members in the enterprise risk management area

From: George Wang, Chair
Practice Development Council

Pierre Lepage, Chair
Committee on Enterprise Risk Management

Date: November 12, 2021

Subject: **Practice Resource Document: Risk Appetite**

The Committee on Enterprise Risk Management (ERMPC) has prepared this practice resource document to provide assistance to actuaries, risk practitioners, risk managers, executives, and board members who would like to gain a better understanding of risk appetite and incorporating a risk appetite framework into their enterprise risk management (ERM) program.

The document addresses key concepts, principles and objectives of an effective risk appetite framework. It provides assistance on how to translate these principles and objectives into meaningful risk appetite statements that can be easily understood across the organization, along with practical limits and on-going alignment processes to ensure its relevancy going forward.

An effective risk appetite framework can help organizations strike the right balance between uncontrolled risk taking and excessive caution, enhancing risk awareness and communication across an organization. Real life examples are included throughout this document.

This paper focuses on ERM from an actuarial perspective and is intended to assist practitioners in considering whether they have addressed all of the various potential topics of relevance.

In accordance with the Institute's *Policy on Due Process for the Approval of Practice Resource Documents*, this practice resource document has been prepared by the ERMPC and has received approval for distribution from the Practice Development Council on October 19, 2021.

Practice resource documents are intended to assist members in considering whether they have addressed all relevant topics within a practice area. These may include skills and knowledge inventories (SKI), a compilation of other relevant material (internal or external to the CIA) related to the practice, as well as recognized best practices, where appropriate. Such documents may be particularly helpful to members in small or in emerging areas.

The ERMPC would like to acknowledge the contribution of the working group that assisted in the development of this practice resource document: Karim Nanji (chair), Meagan Orr, Sarah Cheng, and Pierre Lepage.

1740-360 Albert, Ottawa, ON K1R 7X7 ☎ 613-236-8196 🖷 613-233-4552
head.office@cia-ica.ca / siege.social@cia-ica.ca **cia-ica.ca**

Questions or comments regarding this practice resource document may be directed to Karim Nanji at knanji@munichre.ca or Pierre Lepage at plepage@kpmg.ca.

GW, PL

Table of Contents

1. Introduction 5

2. Description of key concepts 5

3. Principles and objectives of an effective risk appetite framework 7

4. Risk appetite statement 8

4.1 Stakeholder considerations **8**

4.2 Risk type considerations **9**

4.3 Communication considerations **9**

4.4 Examples of risk appetite statements **10**

5. Risk capacity and risk tolerance 11

5.1 Risk capacity 11

5.2 Risk tolerances 12

5.3 Risk limits 13

5.4 Examples of risk limits 14

6. Risk measures and reporting 15

6.1 Risk measures 15

6.2 Risk aggregation and dependencies 16

6.3 Risk profile vs. risk limits 16

6.4 Risk limit dashboard 17

7. Risk governance 18

7.1 Roles and responsibilities 18

7.2 Role of the actuary 21

7.3 Ongoing alignment of risk appetite 21

8. Linking risk appetite to the business 22

8.1 Communicating risk appetite 22

8.2 Embedding risk appetite in business activities 22

8.3 Allowing for future business growth and change 23

8.4 Connecting risk appetite to risk culture 23

8.5 Examples of links to business 23

9. Bibliography 26

1. Introduction

Most organizations cannot operate successfully without taking risks. Taking risks leads to new opportunities, enhances innovation, and provides organizations with a competitive advantage.

An effective risk appetite framework helps organizations achieve their business objective(s), supports conscious risk-taking, and avoid unanticipated catastrophic losses. It is a key enabler for organizations to drive performance and empower risk-based decision making to the lowest appropriate level.

The purpose of this practice resource document is to provide assistance to actuaries, risk practitioners, risk managers, executives, and board members who would like to gain a better understanding of risk appetite and incorporating a risk appetite framework into their enterprise risk management (ERM) program. For further understanding of the various elements of ERM, actuaries and other practitioners can refer to the practice resource document, *Actuarial Aspects of Enterprise Risk Management*.

Risk appetite is a key component of an ERM program. It defines the aggregate level and types of risk that an organization is willing to accept in order to achieve its business objectives. As described in *Actuarial Aspects of Enterprise Risk Management*, there is often discussion regarding whether the organization's business strategy is derived from its risk appetite or whether the organization typically defines its business strategy first and then sets its risk appetite. In general, the two will typically be developed and evolve in tandem with the key point being that they remain internally consistent.

While the risk appetite framework is crucial to an organization's success, it can be difficult to connect an organization's risk appetite statement to its business strategies. This document helps address the main practical challenges an organization might face when designing and implementing a risk appetite framework with an emphasis on the benefits to the organization.

This document addresses key concepts, principles and objectives of an effective risk appetite framework. It provides assistance on how to translate these principles and objectives into meaningful risk appetite statements that can be easily understood across the organization, along with practical limits and on-going alignment processes to ensure its relevancy going forward. An effective risk appetite framework can help organizations strike the right balance between uncontrolled risk taking and excessive caution, enhancing risk awareness and communication across an organization. Real life examples are included throughout this document.

2. Description of key concepts

Risk appetite is the level and type of risk that an organization is willing to accept in order to achieve its objectives. It is expressed as a series of qualitative and quantitative risk appetite statements articulating risk appetite relative to earnings, capital, liquidity, and/or other measures as appropriate.

The **risk appetite framework** is an organization's overall approach to managing risk appetite. It includes policies, processes, controls, and systems through which risk appetite is established,

embedded, communicated, and monitored. It also outlines roles and responsibilities of those overseeing the implementation and monitoring of the risk appetite framework.

Risk capacity is the maximum level of risk an organization can accept before breaching risk constraints. These constraints are determined by regulatory capital and liquidity needs, the operational environment (e.g., technical infrastructure, risk management capabilities, expertise), and obligations to stakeholders (e.g., depositors, policy-holders, shareholders, fixed income investors, and regulators). Risk appetite is constrained by risk capacity.

Risk tolerance is the maximum level of risk that an organization is willing and able to accept. It is the practical application of risk appetite and operationalizes the risk appetite statements with qualitative and/or quantitative measures that can be monitored and reviewed.

Risk limits consist of qualitative and quantitative measures that allocate an organization's risk tolerance to business lines, subsidiaries, risk categories, concentrations, and other levels as appropriate. Risk limits translate risk tolerance into boundaries on risk monitoring measures. Some risk limits are hard limits; exceeding them represents an unacceptable level of risk and immediate corrective action is required. Some are soft limits that provide an early warning signal as risk profile approaches risk limits. Exceeding a soft limit prompts management to evaluate whether corrective action is necessary.

Risk profile is a point-in-time assessment of an organization's risk exposure, aggregated within and across each risk category, and measured against risk tolerance and risk limits.

Risk culture is the set of values and behaviours that shapes the thought processes and risk decisions of management and employees within an organization.

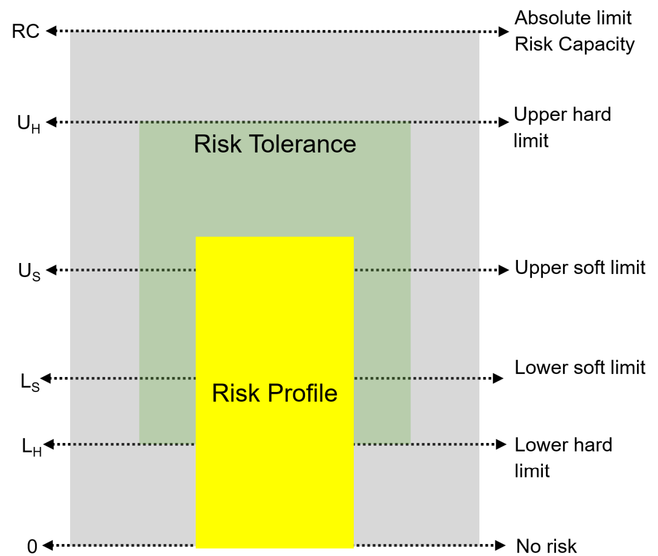
Risk measures are defined and documented metrics that quantify an organization's exposure to a specific risk. A given risk may be monitored using several different risk measures, each having a specific purpose.

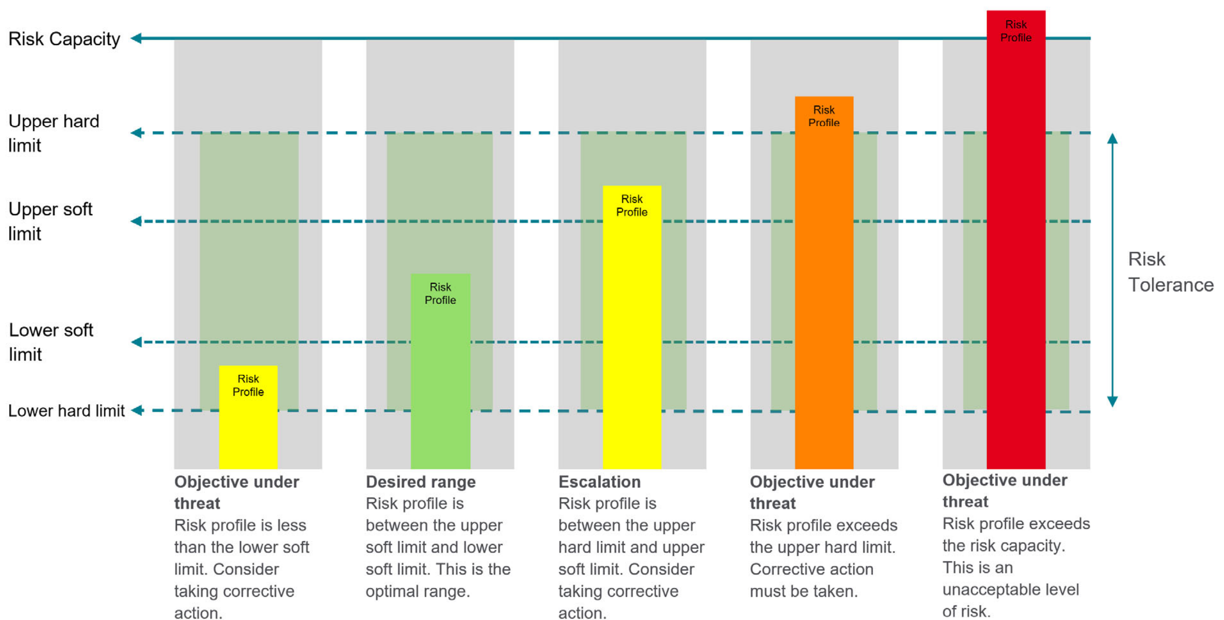
The following figure demonstrates the relationship between the above concepts.

Figure 1: Relationships between key risk concepts

This figure opposite, conceptually illustrates how risk capacity, risk appetite, hard and soft tolerance limits operate in practice. The example concerns a project timeline where there is an inbuilt project delay at level U_H.

In this example, the risk of project delay is setting between the upper soft limit (U_S) and upper hard limit (U_H). The risk therefore needs to be escalated as it exceeds the entity's desired range in between the upper soft limit and the lower soft limit.





3. Principles and objectives of an effective risk appetite framework

An organization's goals in establishing a risk appetite framework may include preserving capital adequacy, maintaining adequate liquidity, complying with regulatory requirements[1], and/or

[1] In Canada, the Office of the Superintendent of Financial Institutions (OSFI's) Corporate Governance Guideline requires federally regulated financial institutions to have a risk appetite framework.

improving risk awareness in business decisions, among others. The Financial Stability Board Consultative Paper, "*Principles for an Effective Risk Appetite Framework*" states that an effective risk appetite framework should:

- establish a process for communicating the risk appetite framework within the financial institution and to external stakeholders (as appropriate);
- have both top-down board leadership and bottom-up involvement of management. Risk appetite is embedded and understood throughout the organization;
- embed risk appetite into the organization's risk culture;
- evaluate opportunities for appropriate risk taking, and act as a defense against excessive risk taking;
- allow risk appetite statements to be used as a tool to promote discussion on risk. They are a basis upon which the board, ERM, and internal audit can debate and challenge management recommendations and decisions.
- be adaptable to changing business and market conditions so that opportunities requiring an increase to the risk limit of a business line or subsidiary can be met while remaining within enterprise-wide risk appetite; and
- cover activities, operations, and systems that fall within an organization's risk universe but that are outside of its direct control.

A risk appetite framework provides a common language and comparable measures to understand risks, and clearly defined boundaries to operate within in pursuit of business goals. It aids decision making, holds staff accountable, and supports the organization's risk culture.

An effective risk appetite framework is not solely focused on risk, but also on the achievement of organizational objectives. It is aligned with the organization's vision, business plan, strategy, capital planning, and compensation philosophy. It is forward-looking and proactive, identifying risk preferences for all material risks while considering the various interests and objectives of key stakeholders.

Establishing and maintaining a risk appetite framework is an iterative process requiring ongoing dialogue to achieve buy-in and fully embed risk culture within an organization.

4. Risk appetite statement

Risk appetite statements articulate and communicate the aggregate level and types of risk that a firm is willing to accept in order to achieve its business strategy. This section presents considerations and possible criteria to use in establishing a risk appetite statement.

4.1 Stakeholder considerations

The risk appetite statement is a concise statement that can be used by many stakeholders to relate business objectives and strategy to acceptable levels of risk. When drafting risk appetite statements, it is important to consider the audience and the risks most relevant to them. These stakeholders may include the following:

- ***Board of directors***: The board is ultimately responsible for approving the risk appetite framework. Risk appetite statements would be consistent with the framework within which the organization is allowed to operate in deploying its strategy.
- ***Management (including senior management):*** A well-defined risk appetite statement will serve as the basis for defining acceptable risks at a more granular level relevant to each part of an organization’s operations. It is also the basis for how the board will evaluate if management is operating within acceptable boundaries.
- ***Investors, regulators, and customers (e.g., depositors, policy-holders):*** The risk appetite statement can be an effective way of communicating to investors, regulators, and customers the most important risks of an organization as well as its risk tolerance at a high level.

4.2 Risk type considerations

Risk appetite statements are concise statements addressing the most important risks facing an organization. Risk appetite is about understanding how the following risks will impact an organization’s capitalization and solvency, variability of earnings, protection of franchise value and reputation:

- insurance risks
- market risks
- credit risks
- liquidity risks
- operational risks
- business and strategic risks
- regulatory and compliance risks

In general, risk appetite statements consider these risks (under both normal and stressed conditions), using a forward-looking view. The results of stress and scenario testing are examined to understand what type of events might cause the organization to exceed its risk appetite.

4.3 Communication considerations

Effective risk appetite statements are easy to communicate and easy for all stakeholders to understand. Organizations would consider the following factors in articulating a risk appetite statement:

- ***Links with the organization’s business strategy*:** Does it help define the boundaries of the business strategy? Can ongoing strategic decisions be made within the established risk-based context?
- ***Use of quantitative measures:*** Do the statements set clear limits that are measurable and that can be monitored?
- ***Use of qualitative measures:*** Many organizations consider qualitative statements as a complement to quantitative measures. Qualitative statements can set the tone for the

overall approach to risk taking within the organization and articulate the motivation for accepting or avoiding certain types of risks.

- ***Easily understandable:*** Is the risk appetite statement articulated in a way that is easy to understand and easy to monitor?

Other considerations

Some additional considerations for an effective risk appetite statement:

- Can the higher-level risk appetite statement be used to allocate risk to each business unit while maintaining an appropriate enterprise-wide view of aggregate risk assumed?
- Can quantitative measures be easily translated into risk limits?

4.4 Examples of risk appetite statements

In 2015, the CRO Forum conducted a survey of the goals that insurers use in their risk appetite statements.[2] The following seven goals are the most popular according to this survey (shown below in descending order):

1. preserve capital adequacy
2. maintain adequate liquidity
3. ensure customer protection
4. protect against earnings volatility
5. ensure alignment between risk and return
6. protect the organization's franchise value
7. achieve/maintain a specific debt rating

The following examples of risk appetite statements were provided by the CRO Forum[3]*:*

> XYZ Company's philosophy and approach to enterprise risk management strategy stems from our mission, corporate strategy and objectives, which are also aligned with the company's stakeholders (i.e., shareholders, policyholders, debtholders, regulators, rating agencies, etc.). Our mission is to [state mission]. Our corporate strategy is to focus on areas of expertise and deep experience, capitalizing on the company's competitive advantage. Corporate objectives are to achieve target performance and maximize shareholder value, preserve a level of solvency that will support XYZ Company in challenging environments, maintain adequate liquidity to satisfy obligations as they come due, and protect all aspects of the company's franchise value, including its brand and reputation.
>
> The company takes and manages risks to achieve our objectives, and the following risk appetite statement broadly describes the types and amounts of risk the company is willing to take in pursuit of these objectives.

---

[2] CRO Forum. Risk Appetite: Survey Results (March 2015)
[3] CRO Forum. Establishing and Embedding Risk Appetite: Practitioners' View (December 2013)

With regard to the types of risk we take in order to seek return, XYZ Company accepts and manages strategic, credit, and insurance risks in accordance with our corporate strategy, investment policy, and annual business plans. The company seeks to minimize potential exposure to market, capital & liquidity, and operational risks.[4]

5. Risk capacity and risk tolerance

5.1 Risk capacity

Risk capacity represents the maximum level of risk an organization is able to support before breaching constraints determined by factors such as regulatory capital, liquidity needs and obligations to customers, shareholders, and other stakeholders.

If we consider risk appetite as the organization's willingness to accept risk (in the context of achieving its business objectives), then risk capacity can be viewed as an absolute maximum ceiling on risk-taking imposed by forces outside the organization. Externally imposed constraints may include the following:

- ***Capital requirements***: Since capital represents the most readily accessible resource available to fund unexpected losses, risk-taking capacity is often closely associated with the amount of capital an organization already holds or can reasonably access. The level of required capital can be determined based on regulatory requirements, e.g., Minimum Capital Test (MCT) for general insurers and Life Insurance Capital Adequacy Test (LICAT) for life insurers, an economic view (i.e., based on the results of an economic capital model) or other stress testing exercises such as FCT, ORSA, or OSFI Guideline E-18 analysis.[5] Capital constraints on risk capacity may be determined using one or more of the following approaches:
    - A quantitative modelling approach determines capital needs via deterministic or stochastic modelling of the business, developing a minimum required economic capital position for the organization.
    - A ratings-based approach determines capital needs using a rating agency capital formula (or a multiple thereof), developing a minimum capital position required to maintain a desired rating.
    - A regulatory solvency approach sets the target operating capital level based on the regulatory minimum plus a margin.
- ***Liquidity requirements***: Risk capacity may be a function of not just the amount of capital available, but also the type of capital, how assets are generally invested and how readily they can be converted to cash to fund unexpected commitments.
- ***Earnings***: For many public companies, earnings volatility is a key determinant of risk capacity. Over the course of the economic cycle, various stakeholders will shift their focus between the income statement and balance sheet when assessing an

[4] CRO Forum. "Establishing and Embedding Risk Appetite: Practitioners' View" (December 2013)
[5] FCT = Financial Condition Testing; ORSA = Own Risk Solvency Assessment; E-18 = OSFI guideline on stress testing.

organization's current risk capacity and profile, making earnings an important structural complement to capital-based risk capacity metrics.

- ***Third-party credit and claims-paying ability ratings:*** The ability to refinance existing capital, access new capital, and the cost of funds associated with financing activities are key determinants of risk capacity impacted by third-party ratings. The deterioration of third-party ratings can also be a key strategic risk for many financial institutions, since existing or potential customers may qualify their prospective providers based on minimum acceptable third-party rating levels.
- ***Brand equity***: An organization's brand equity can also be a key consideration in determining its risk capacity, particularly when considering business issues or opportunities that may involve high levels of risk that could impact the organization's reputation.
- ***Operational capabilities:*** Management resources and capabilities are often the most important enablers or constraints shaping an organization's risk capacity. These include risk management expertise, business processes, operational and technology infrastructure, and governance and control frameworks used in the ongoing process of identifying, assessing, managing, monitoring, reporting, and communicating risk in the day-to-day pursuit of business goals.

5.2 Risk tolerances

Risk tolerances define the boundaries for the maximum amount of risk an organization is willing to accept.

A tolerance level sets out the overall quantitative and/or qualitative boundaries for a material category of risk. It is often expressed in the form of key metrics and targets, and is established after considering how much variability and risk-taking is acceptable to an organization in pursuing its business and strategic objectives. It is often described as "a line in the sand" beyond which an organization will not move without prior board approval.

The CRO Forum[6] describes risk tolerances as the quantitative measures and qualitative assertions for the maximum risk allowed by the risk appetite.

Quantitative measures for risk tolerance would include important elements of the risk appetite statement including capital adequacy, earnings, liquidity, and franchise value. Quantitative measures are useful for stress testing exercises. More refined measures for specific risks may be defined in terms of loss amounts, error rates, or other types of units. For example, establishing a tolerance of +/- 0.5 years of duration mismatch for interest rate risk.

In general, the following are desired criteria for risk tolerances:

1. Clear expectations for mitigating, accepting, or pursuing specific risk types.
2. Clear thresholds (boundaries) of acceptable risk taking and clear link with risk appetite statement.

[6] CRO Forum. "Establishing and Embedding Risk Appetite: Practitioners' View" (December 2013)

3. Clear consequences (or actions) for going beyond tolerance levels.
4. Forward-looking thresholds.
5. Management's ability to take action to move risk profile within thresholds.
6. Ability to apply consistently across business units to enable clear understanding of aggregate risk levels.

The following examples of risk tolerances underlying an organization's risk appetite were based on examples provided by the CRO Forum,[7] and adjusted where necessary to apply to Canadian organizations.

*1. **Achievement of target performance (earnings)**:* Our business should be monitored and managed so that we have 95% confidence that earnings will be no more than 50% lower than expected and 99% confidence that earnings will be no more than 75% lower than expected.

*2. **Preservation of capital***

> *a. **Regulatory capital**:* We seek to maintain a level of capital between 180% and 230% MCT. Our internal minimum level of capital is 180% MCT, which represents a 30%-point margin over the OSFI Supervisory Target of 150%. If the consolidated actual capital level falls below the internal minimum, then immediate remedial action plans will be implemented.
>
> *b. **Economic capital:*** We seek to maintain available capital in excess of 130% of economic capital. In addition, we also manage single risk exposures so that the value at risk (VaR) of each single exposure is less than $500m at a 99.5% confidence level.

*3. **Maintenance of liquidity:*** We seek to minimize exposure to liquidity risk, actively managing our liquidity position and collateral exposure to ensure we have ample resources to fund our obligations. At the organizational level, we maintain holding company cash and securities of two times (2X) annual fixed charges with half of the total holdings (1X) in pure cash equivalents or commercial paper.

*4. **Protection of franchise value:*** Operational risks that could lead to material reputational, legal, or regulatory problems should be minimized. We seek to maintain appropriate compliance with all applicable laws, have no tolerance for criminal or fraudulent activities, and maintain strict data security and privacy controls to protect customer information.

5.3 Risk limits

Risk limits are operational in nature and serve to translate risk tolerances into practical constraints on business activities. Operating within risk limits is a way to avoid exceeding the overall risk tolerance at the organization level. In a sense, limits can be viewed as being constraints on business inputs.

Risk limits are analogous to risk tolerances, but instead of a limit on organizational volatility, they are more granular limits established at the level of the organization that manages risk on a day-to-day basis. Risk limits are the "inner fence" added as extra protection within the "outer

[7] CRO Forum. "Establishing and Embedding Risk Appetite: Practitioners' View" (December 2013)

fence" of risk tolerances set in the risk appetite statement. They are the "no-go zone," in effect, how an organization can progress from "we don't want this to happen" (risk appetite) to "you can't do that."

Risk limits would be relatively easy to measure and monitor. They serve a dual purpose: to permit enough risk to be assumed while also limiting excessive risk taking. Some risk limits are "hard limits" for which action needs to be taken immediately to remediate a breach. Other risk limits are "soft limits" for which monitoring is intended to drive discussion, heighten awareness and influence decision-making – immediate remedial action may not be necessary. Some risks may have both hard and soft limits.

Effectively applied, risk limits become the tool with which management operationalizes the board's risk appetite, by curtailing activities that would contravene the overall risk appetite.

Effective risk limits:

- constrain risk taking within risk appetite by building a clear link to the risk tolerances and the risk appetite statement;
- are relevant to the business activities to which the limit is applied;
- are specific, testable, and reportable;
- are not overly complicated, ambiguous, or subjective;
- can make reference to market practices and benchmarks, but are not based strictly on peers and/or regulatory limits;
- may include material risk concentrations as appropriate;
- are monitored regularly (dashboards may be useful); and
- can be tested to ensure they are effective in controlling risk tolerances.

5.4 Examples of risk limits

Risk limits turn risk appetite statements into something that management can use on a daily basis.

Examples of **qualitative** limits:

- We will/will not write the following types of business, or assume risks from the following territories.
- No reinsurer to be below A- grade.

Examples of **quantitative** limits:

- Per life limit does not exceed the organization's life retention of $10M.
- We will maintain sufficient assets to cover payment obligations at the 99% confidence interval level over one year.
- Mismatching of foreign currency assets and liabilities is tolerated up to a limit of $10M by currency.
- Sub-investment grade assets are not to exceed 3% of the total portfolio.

- No more than 25% of our business is ceded to one counterparty.

6. Risk measures and reporting

6.1 Risk measures

Establishing a risk appetite statement involves specifying the metrics to be used for risk measures. Risks that are material to the organization are to be quantified as much as possible. The importance of each risk measure may vary depending on the stakeholder group, as the diverse interests of stakeholders will need to be considered.

Two common types of risk measures include: VaR and Conditional Tail Expectation (CTE), which is also referred to as Tail Value-At-Risk (TVaR). Both measure the risk associated over a specific time horizon for the loss distribution at a defined confidence level (or probability). VaR is defined as the maximum loss at a specified confidence level over a certain period of time. For example, if a financial institution's one-year 99% VaR is $50 million, there is only a 1% chance that losses will exceed $50 million in a one-year period. CTE or TVaR is the expected loss during a period of time, conditional on the loss exceeding a certain percentile. Continuing the example, the 99th percentile CTE (or TVaR) is the average loss over a one-year period, assuming that the loss is greater than $50 million.

The following table summarizes how risk measures can be used to articulate risk appetite relative to earnings, capital, and liquidity.

Risk appetite relative to:	**Risk measures (examples)**
Capital	Capitalization level depending on target solvency ratio and/or target rating (e.g., 150% of assets required to cover future obligations with 99.5% confidence level)
Earnings	Earnings-at-risk,[8] conditional tail expectation (e.g., the probability of a 10% loss in earnings in one year is less than 5%)
Liquidity	Liquidity-at-risk,[9] conditional tail expectation, leverage ratio, funding profile (e.g., sufficient liquid assets to cover obligations at a 99% confidence interval over a five-year period.)

The aggregate amount of risk an organization is willing to take (risk tolerance) needs to be allocated to specific risks using risk limits. The methods and/or models used in the context of risk limits vary in sophistication and complexity depending on factors such as the materiality of the risk and the risk type being modelled.

For certain types of risk, e.g., credit risk or catastrophic risk, mathematical models based on a "frequency and severity" approach are commonly used in the industry. The "frequency" component determines the probability of an event occurring in any given year, while the "severity" component determines the cost of the event if it occurs. Both the frequency component and the severity component may be calibrated based on historical record and/or expert judgment. VaR and CTE can be obtained using mathematical models. It is important for

[8] Earnings-at-risk is the loss of earnings at a specified confidence level.
[9] Liquidity-at-risk is the risk of unavailability of liquid funds at a specified confidence level.

the stakeholders of these risk measurements to understand the model risk inherent in these mathematical models.

For risks that are difficult to quantify, such as operational risk, qualitative assessments are often adopted, relying on the opinion of subject matter experts.

The following table summarizes the key considerations in constructing the measures by risk type. These examples are modified from the CRO Forum survey and are not an exhaustive list.

Risk type	**Key considerations**
Market risk	Funded yield vs. portfolio/plan yield, pricing interest margin, current and projected reserve margin, duration mismatch, sensitivity of MV surplus, and accounting to risk factors such as interest rates, foreign exchange, equity, and commodity indices
Credit risk	Counterparty rating, concentration, debt rating
Insurance risk	Underwriting, reserving, catastrophe, concentrations, trend, policy-holder behaviour
Operational risk	Risk control assessment outputs, operational loss events
Strategic risk	Earnings volatility, company share price volatility
Model risk	Root cause analysis of errors, back testing, model vetting processes, frequency of model validation
Emerging risks	Expert assessments of identified risk's impact

6.2 Risk aggregation and dependencies

Once individual risks have been measured, they are then aggregated based on the dependency structure by risk type in order for management to produce a view of the organization's overall risk profile. One common approach is to use correlation matrices, whereby the value of each risk is calculated in isolation and aggregated assuming a linear correlation. An alternative approach which could be adopted in a risk appetite framework is a copula approach, which determines joint distributions based on marginal distributions and a copula function. Expert judgment is most commonly used to identify drivers of dependencies between risk types.

6.3 Risk profile vs. risk limits

Risk profile is a point-in-time assessment of an organization's risk exposure, aggregated within and across each risk category, and measured against risk tolerance and risk limits. In monitoring and reporting an organization's risk profile against its risk tolerance as set forth in the risk appetite framework, management would ensure that the information is comprehensive, and that reports cover all risks at an appropriate level of detail. Management would also ensure risk reporting is accurate, auditable, and consistent with other management information circulated within the organization. It is important for risk reports to be forward-looking, rather than relying solely on current and past data. In providing information that is forward-looking, management would consider projections under both normal and stressed conditions and under the appropriate time horizon(s).

6.4 Risk limit dashboard

A more detailed quantitative assessment might take the form of a risk limit dashboard. Risk limits are developed for each major driver of risk, such as mortality, persistency, business mix, or property and casualty insurance risk. As shown in Figure 2, the use of colours and arrows serve as indicators for each stated risk limit (acceptable, monitoring, exceeding) and express trends (improving, unchanged, deteriorating) based on recent experience and expectations regarding the future.

Figure 2: Example of a risk limit dashboard

	Risk measures	Limit	Assessment	Outlook
Life insurance risk	Mortality A/E	No greater than 110%	99% (acceptable)	→ Unchanged
	Persistency A/E	No less than 90%	91% (monitoring)	↑ Improving
	Business mix (% males)	No greater than 60%	65% (exceeding)	↓ Deteriorating
Property & Casualty insurance risk	Underwriting (actual/technical premium)	No less than 90%	93% (acceptable)	→ Unchanged
	Catastrophe (market share in high-risk areas)	No greater than 10%	12% (exceeding)	↑ Improving
Market risk	Interest rate risk (dollar duration mismatch as % assets)	No greater than 10%	8% (acceptable)	↑ Improving
	Credit risk (non-investment grade bonds as % total)	No greater than 5%	3% (acceptable)	→ Unchanged
Operational risk	Voluntary staff turnover	No greater than 8%	8% (monitoring)	↓ Deteriorating
	Audit reports with issues needing significant improvement	No greater than 35%	15% (acceptable)	→ Unchanged

Management may define multiple limits with one serving as an early warning trigger (a.k.a. "soft" limits), which encourages dialogue on the course of action in anticipation of a "hard" limit breach. Such an assessment tool empowers ownership and accountability within an organization. When the risk limits (a.k.a. "hard" limits) are breached, management can choose to take immediate action to return within stated risk limits, or to allow the breach to exist for a certain period of time provided that a cure period is defined, during which the organization's risk exposure will return within stated risk limits.

Frequency of risk measurement and reporting will depend on the risk in question. Some risks may be appropriate to monitor monthly or quarterly, while others may require monitoring as close to real time as possible.

Management or the board may request a more qualitative risk profile assessment be conducted for a specific business line, which may consider risk exposures, management's concern level (high, medium, low) and recent movement (improved, minimal change, worsened).

7. Risk governance

An organization's risk governance is essential in clarifying lines of accountability and describing how staff are expected to adhere to the organization's risk appetite framework to ensure its success. Adopting an effective risk appetite framework requires the full buy-in of the board of directors and senior management. A strong governance structure makes risk considerations a key priority of the board and senior management. For companies operating in Canada as branches, this function of the board is performed by the Chief Agent and senior management.

Senior management refers to the core management team, excluding the board of directors. This normally includes the Chief Executive Officer, Chief Financial Officer, Chief Risk Officer, Chief Operating Officer, Chief Compliance Officer, and Corporate Secretary as well as other members.

The risk appetite framework supports risk governance by providing the board of directors and senior management with the information and tools necessary to understand and communicate the risks the organization is taking, risks that it should be taking, and risks which should be avoided, in line with the organization's risk appetite and business strategy.

7.1 Roles and responsibilities

Risk appetite would be applied consistently and continuously throughout all business units and involve key stakeholders from every level of the organization. It is critical that roles and responsibilities are established for monitoring adherence to the risk appetite framework.

Individuals within governance roles are expected to explicitly understand risk appetite when defining and pursuing objectives and developing and allocating resources. The board is expected to consider risk appetite when it approves budgets, strategic plans, new products, services, and markets.

The following sections outline key roles and functions as they pertain to the risk appetite framework. Note that functions outlined below may vary by organization and are not an exhaustive list. They are provided as examples. For ease of presentation, RAS refers to the risk appetite statement and RAF refers to the risk appetite framework.

The Board of Directors
▪ Is ultimately responsible for ensuring that an effective ERM program is in place, including a robust RAF. ▪ Approves the RAF which has been developed in collaboration with the CEO, CRO, and CFO and ensures that the RAF is consistent with the organization’s strategy, business and capital plans, risk capacity, and compensation schemes. ▪ Regularly reviews the actual risk profile against risk limits and holds the CEO and senior management team accountable for timely identification, management, and escalation of breaches of the RAF. The board also discusses and monitors action taken in response to breaches to risk limits. ▪ Obtains independent assessment of the design and effectiveness of the RAF. ▪ Ensures adequate resources are allocated to risk management and internal audit and that adequate support is available throughout the organization to enable identification, measurement, assessment, and reporting of risk in a timely manner. ▪ The board may also establish several sub committees, including: Risk Committee, Audit Committee, Management Resources and Compensation Committee, Corporate Governance Committee and others.
Executive Risk Committee
▪ Usually includes the CEO, CRO, CFO, other senior management and may include representatives from ERM or other departments. ▪ Discusses any material changes in risk appetite with regulators. ▪ Oversees the management of the organization’s risk policies and procedures, monitors key risks and material risk exposures and programs to manage and mitigate the risks. ▪ Sponsors strategic risk management priorities throughout the organization and reviews and assesses the impact of business strategies, opportunities, and initiatives on overall risk position.
Chief Executive Officer (CEO)
▪ Sets the “tone at the top” which influences the risk culture of the organization. The tone itself can be either positive (“do this”) or negative (“don’t do that”) in ensuring that risks are managed within acceptable limits. ▪ Along with the CRO and CFO, establishes the organization’s risk appetite and ensures it is consistent with the organization’s strategy, business and capital plans, risk capacity, and compensation schemes. The trio will also ensure that risk appetite is appropriately translated into risk limits for the lines of business. ▪ Ensures that the lines of business have the necessary processes in place to identify, monitor, measure, and report on risk and risk limits.

- Ensures that the organization’s RAS is implemented by senior management.
- Leads communication with internal and external stakeholders to embed appropriate risk taking into risk culture.
- Dedicates sufficient resources to ERM and internal audit (and information technology) to provide effective oversight.
- Ensures effective management and mitigation of material risk exposures in a timely manner.
- Establishes a policy to notify the board and regulator of serious breaches and unexpected material risk exposures.

Chief Financial Officer (CFO)

- Along with the CEO and CRO, develops the RAF, incorporates risk appetite into compensation and decision making processes, establishes, monitors, and reports on adherence to risk limits and acts in a timely manner to ensure effective management and mitigation of material exposures.
- Escalates any material breaches to the board and CEO.

Chief Risk Officer (CRO) and ERM

- Along with the CEO and CFO, develops appropriate RAS and risk limits for the lines of business.
- Obtains approval of risk appetite by the board of directors and regularly reports to the board on risk profile relative to risk appetite.
- Actively monitors the organization’s risk profile, risk appetite, strategy, business and capital plans, risk capacity, and compensation programs.
- Ensures the alignment of risk appetite with risk culture.
- Develops tools to measure and monitor aggregate risk exposures against risk tolerances.
- Monitors the organization's overall risk profile in relation to its risk appetite.
- Ensure effective management and mitigation of material exposures in a timely manner.
- Escalates material breaches to the board and CEO.

Lines of business leaders

- Manage risk within their business lines.
- Ensure alignment between risk appetite and planning, compensation, and decision-making processes.
- Embed risk appetite statements and risk limits into their business activities.
- Embed prudent risk taking into the organization’s risk culture and day to day. management of risk.
- Establish and monitor adherence to risk limits.
- Co-operate with CRO and ERM team.

▪ Implement controls and processes to identify, monitor, and report against risk limits. ▪ Act in a timely manner to ensure effective management and mitigation of material exposures. ▪ Escalate material breaches to the CRO and senior management.
Internal audit team
▪ Independently assesses the design and effectiveness of the RAF and its alignment with regulatory expectations and reports any material deficiencies to the board and senior management. ▪ Checks whether breaches are being identified, escalated, and reported on a timely basis. ▪ Assesses the effectiveness of RAF implementation, including the link to risk culture, strategic and business planning, compensation, and decision making. ▪ Assesses the design and effectiveness of risk measurement techniques.

7.2 Role of the actuary

Actuaries undergo extensive training and develop specialized experience in dealing with uncertainty and in making decisions involving risk and reward in many areas of their organizations. Therefore, actuaries are usually involved in developing and setting up risk appetite frameworks and risk appetite statements.

Actuaries are well positioned to fulfil any of the functions in the above table.

7.3 Ongoing alignment of risk appetite

As the organization's circumstances and opportunities change within the business environment (including changes in competition and regulation), the organization's board of directors and management would reassess its risk appetite and consider any necessary changes. A review of the organization's risk appetite would be performed at least once a year. This review can include proposed changes to the risk appetite statement, risk appetite framework and risk tolerance levels, alignment with business plans and risk policies, and management and board approvals. Organizations would ask themselves: Have there been any significant changes in the competitive, risk and economic landscape which may warrant a change in risk appetite and/or strategy?

Steps boards have taken to improve risk governance include:

1. revised committee charters to include risk-related concerns;
2. benchmarked their practices against peer companies;
3. obtained guidance from associations of directors and similar sources;
4. focused more attention on risk management and its value and shortcomings;
5. reviewed ethical guidelines and codes of conduct; and
6. solicited independent viewpoints. An independent review of an organization's risk governance program can highlight any gaps and prioritize areas for improvement.

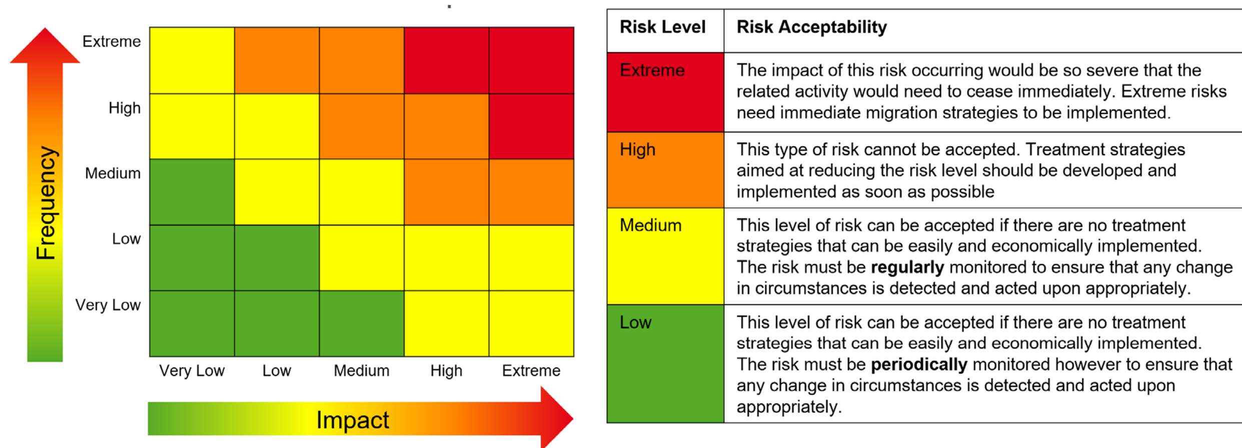
8. Linking risk appetite to the business

8.1 Communicating risk appetite

An effective top-down communication strategy and training on risk appetite is essential at all levels of an organization. Risk appetite would be communicated to all key stakeholders of an organization, including the board of directors, senior management, staff, policy-holders, regulators, and rating agencies. The diverse interests of parties relevant in achieving the organization's objectives would be considered. Breadth and depth of information will vary for internal vs. external reporting and for various stakeholders. For example, senior management may be interested in how the organization's risk exposure is likely to evolve given its business strategy, while staff may be more interested in granular risk limits governing their day-to-day activities.

An organization which communicates its risk appetite effectively is able to make decisions, set risk-based goals, and is more likely to achieve these goals. To ensure the risk appetite framework is consistently implemented across an organization, management needs to measure its current risk exposure against the stated risk appetite on a periodic basis. The analysis would be clearly and sufficiently reported to the organization's key stakeholders including senior management and the board. Some organizations may communicate risk appetite using tools such as risk heat maps with different colors representing various levels of risk appetite (see Figure 3).

Figure 3. Risk Heat Map



Risk Level	Risk Acceptability
Extreme	The impact of this risk occurring would be so severe that the related activity would need to cease immediately. Extreme risks need immediate migration strategies to be implemented.
High	This type of risk cannot be accepted. Treatment strategies aimed at reducing the risk level should be developed and implemented as soon as possible
Medium	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be **regularly** monitored to ensure that any change in circumstances is detected and acted upon appropriately.
Low	This level of risk can be accepted if there are no treatment strategies that can be easily and economically implemented. The risk must be **periodically** monitored however to ensure that any change in circumstances is detected and acted upon appropriately.

8.2 Embedding risk appetite in business activities

An organization's risk and other management committees are tasked with ensuring that risk appetite is cascaded to all levels of the organization and that appropriate monitoring is in place. In order to effectively embed risk appetite in the business, management would establish risk limits for each category of risk, operationalize risk appetite into day-to-day decision making and cascade it to lower levels within the organization. Key decision makers must know how much risk is acceptable as they consider ways to accomplish organizational objectives. An organization's risk committee and management committee need to ensure that business lines

have action plans in case any risk limits or risk tolerances are breached, and that decisions made are consistent with the organization’s risk appetite.

Each business unit is responsible for implementing risk limits and utilizing and refining existing policies, procedures, metrics, and monitoring practices. Making the link between existing practices and risk appetite encourages a culture that operates with a risk management mindset and empowers staff.

8.3 Allowing for future business growth and change

Many organizations are faced with taking on additional risk in order to remain competitive, increase innovation, adapt to changing circumstances and to grow their business. The challenge is to choose the right amount of risk to accept to sustain innovation and growth and develop the strategies necessary to pursue these objectives. Companies may be more willing to take on more risk during healthy economic times than during a recession. Changes in the competitive, risk, and economic landscape may require the organization to revisit its risk appetite statement, objectives, and overall strategy.

8.4 Connecting risk appetite to risk culture

Risk culture is the system of values and behaviours that shapes the risk decisions of management and employees within an organization. Risk appetite statements that are clearly defined and communicated throughout the company help organizations enhance their risk culture and manage their risks more effectively. It is impossible to have a strong risk culture without the requisite level of organization-wide understanding and consensus regarding the entity’s risk appetite. Risk appetite also provides shared context for facilitating the type of constructive challenge that is essential for building a strong risk culture, illustrating the interconnectivity that is inherent in critical risk culture shaping practices and conditions.

By reinforcing risk appetite, management creates a culture whose organizational goals are consistent with the board of directors. An effective risk culture starts with an appropriate “tone from the top” regarding acceptable levels of risk taking. Each member of the organization would have a clear understanding of this acceptable level of risk taking and their accountability in key risk-taking decisions. Employees would be incentivized to do the right thing, and incentive programs would be aligned to reward long-term prudent conduct that complies with the organization’s strategy and risk appetite. Such an environment will promote consistent goals, improve decision making and lead to greater overall benefits for the organization.

8.5 Examples of links to business

Pandemic and natural catastrophe risks	Organization provides coverage on products that are generally low frequency/high severity in nature. **Link to risk appetite:** Ensures that aggregate exposure does not breach a maximum limit. The organization can set appropriate budgets for these risks by looking at 1-in-200-year or 1-in-1000-year probable maximum loss (PML) scenarios and comparing against its current capital position. The organization sets tolerance thresholds, and if the exposure enters the “red zone”,

	the organization either ceases to write new business or considers reinsuring all or a portion of it.
New business pricing	Organization introduces a new preferred term product. Underlying assumptions include business mix (gender, age, preferred class, etc.). The risk is whether the real business mix turns out to be drastically different, which could result in a return on investment significantly lower than the target. **Link to risk appetite:** Product priced to achieve an internal rate of return (IRR) target of 12%. As business is written the business mix is compared to those used as assumptions in pricing, and appropriate changes are made to ensure that profitability stays on target. Changes can include premium adjustability (if applicable), modified commissions, or stopping sales of the product.
Investment guidelines/strategy	Organization develops an enterprise-wide investment guideline. **Link to risk appetite:** Establish controls that reflect the organization's risk appetite, for example: • Set limits on asset classes to ensure diversification and limit certain types of asset risk. • Individual asset name limits, taking into account bond and equity holdings, derivative counterparties, and reinsurance partners, to control credit risk. • Set duration mismatch limits to mitigate interest rate risk.
Variable annuities	Organization sells variable annuity products where earnings are based on a fixed percentage of the underlying assets and thus are exposed to market movements. **Link to risk appetite:** Low market risk for the organization. The organization will consider incorporating a portfolio hedge to offset losses from lower revenues in a declining equity market.
Pension funding risk appetite	An industry-wide multi-employer pension plan serves the retirement savings needs of a number of employers and employee groups working within that industry. The retirement savings vehicle is a defined benefit pension plan, one that is funded through a fixed contribution per hour worked. **Link to risk appetite:** The participating employers establish an objective of maintaining contribution rates within a band ranging from $4.00 to $5.00 per hour worked, with a specific maximum threshold of $6.00 not to be exceeded. The administrator then updates the funding and investment policy to align with those objectives.

Operational/cyber risk	Organization's data includes personal health information of its policy-holders. There is a data security risk that would result in financial loss and reputational damage in the event of a breach of data caused by a cyber-attack. **Link to risk appetite:** Organization has no tolerance for the loss of, or otherwise unauthorized disclosure of personal health information it collects from its policy-holders. The organization contracts a third party to perform a cyber risk assessment to ensure sufficient security safeguards are employed to prevent such a breach of data. The organization may also consider obtaining external cyber coverage.

In conclusion, an effective risk appetite framework provides a common language and comparable measures to understand risks, and clearly defined boundaries to operate within in pursuit of business goals. It aids decision making, holds staff accountable, and supports the organization's risk culture.

9. Bibliography

- CRO Forum. Risk Appetite: Survey Results (March 2015)
- Rebecca B. Scotchie and Christopher H. Murphy, Hungry for Risk? Practical applications of a risk appetite framework, *The Actuary Magazine*, July 2019.
- CRO Forum. Establishing and Embedding Risk Appetite: Practitioners' View (December 2013)
- Institute of Actuaries of Australia, DEVELOPING THE RISK APPETITE FRAMEWORK OF A LIFE INSURANCE BUSINESS, 2015
- Australian Government Department of Finance, Defining Risk Appetite and Tolerance, Comcover Information Sheet, Risk Management Policy, 2016.
- Canadian Institute of Actuaries, ERM Applications Committee, Enterprise Risk Management – How Do We Govern It? 2015.
- Bertrand K. Hassani. Risk Appetite in Practice: Vulgaris Mathematica, 2014
- Financial Stability Board, Principles for an Effective Risk Appetite Framework, 2013
- Risk Culture of Companies: Abstract of source article authored by ERM Initiative Faculty, April 15, 2009
- Canadian Institute of Actuaries, ERM publication: A New Wave of Risks: Building a Strong Risk Culture, Mike Stramaglia, 2019
- CAS/CIA/SOA, Joint Risk Management Section: Risk Appetite: Linkage with Strategic Planning, March 2012
- ERM PRACTICE NOTE © 2013 American Academy of Actuaries 6 www.actuary.org roles in all aspects of the ERM control cycle. Chief Risk Officers (CROs) may be credentialed actuaries.