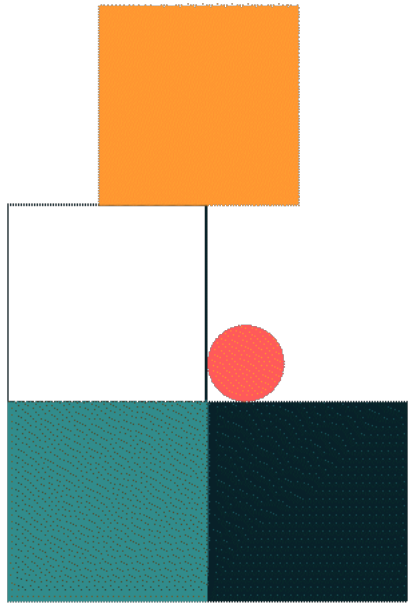

02

INHERENT RISK ASSESSMENT

INHERENT RISK ASSESSMENT

Illustrative example of a risk assessment formula

INHERENT RISK

WEIGHTING FACTORS

AU PROFILE

HIGH MODERATE LOW

+

INTERNAL & EXTERNAL RISK FACTORS

LIKELIHOOD

RARE UNLIKELY LIKELY CERTAIN

+

IMPACT

MINOR MATERIAL SIGNIFICANT CATASTROPHIC

LOW - MODERATE – HIGH – CRITICAL

CONTROL EFFECTIVENESS

KEY CONTROLS IDENTIFIED

DESIGN EFFECTIVENESS

To what extent is the control designed to prevent, detect, or respond to risk?

WEAK NEEDS IMPROVEMENT ADEQUATE STRONG

+

OPERATING EFFECTIVENESS

To what extent is the control actually preventing or mitigating risk?

WEAK NEEDS IMPROVEMENT ADEQUATE STRONG

WEAK – NEEDS IMPROVEMENT – ADEQUATE – STRONG

RESIDUAL RISK

Residual risks above stated risk tolerance must be actioned.

LOW – MODERATE – HIGH – CRITICAL

KMRC

It is important to make sure stakeholders understand the difference between *inherent* and *residual* risk before executing the RCSA

The nature and level of inherent risk (risk absent controls) must be well understood because if it's underestimated, we may not take the proper actions to reduce risk to within risk appetite and tolerance.

INHERENT RISK

- Think of a steep mountain road. The road itself is inherently risky, as its narrow and winding nature makes it more prone to accidents than say driving on a flat country road.
- The risk of going off the road is the same for everyone when we don't take into consideration who is driving or what type of vehicle they are driving, or how equipped they are to safely travel the narrow and windy roads.

RESIDUAL RISK

- The risk that we start off with still exists and is the same for everyone.
- But now we are actively reducing the likelihood and/or impact of an accident occurring by making sure our brakes work, putting on the snow tires, reducing our speed to 20km an hour, and putting emergency supplies in the trunk.

Understand the internal factors, unique to each AU, that can drive the likelihood and impact of operational risks

Factors unique to each AU that can affect the likelihood and/or impact of operational risks occurring include but are not limited to:

- Strategic importance of the AU
- Size of the unit (AUM, % revenue, % staff, etc)
- Degree of specialization and dependency on human expertise
- Transaction volumes
- Transaction sizes
- Customer type (e.g., retail, institutional, internal, etc)
- Product complexity
- Process complexity
- Extent of change within the unit

These factors (and others) should be well understood and considered when determining the likelihood and impact of key risks applicable to the AU.

Understand the external factors that can drive the likelihood and impact of operational risk occurrence

External factors that can affect the likelihood and/or impact of operational risks occurring include but are not limited to:

- Economic conditions
- Market dynamics and conditions
- Political stability
- Frequency of natural disasters
- Technological advancements
- Supply chain complexity and dependencies
- Pandemics and other health crises
- Market volatility
- Extent of cultural and social change
- Extent of regulatory change
- Customer behaviour and expectations
- Reliance on public infrastructure
- Labour market conditions
- Geopolitical events and tensions

These factors (and others) should be well understood and considered when determining the likelihood and impact of key risks applicable to the AU.

INHERENT RISK ASSESSMENT

Illustrative example of a Likelihood rating scale

RATING SCALE

LIKELIHOOD OF RISK OCCURRENCE RATING SCALE			
RARE (1)	**UNLIKELY (2)**	**LIKELY (3)**	**CERTAIN (4)**
Risk may occur once every 10 to 20 years but only if there is the right combination of several unlikely events.	Risk may occur once every 5 to 10 years but only if there is the right combination of a few unlikely circumstances	Risk may occur once every 2 to 5 years and in most business-as-usual circumstances	Risk event will occur routinely and under any circumstance

For each key risk identified, RCSA participants should consider the internal and external factors and determine which rating best applies to the risk, absent any consideration of internal controls.

Let's take the example of a ransomware attack within the Canadian Life Insurance segment. R

INHERENT RISK ASSESSMENT

ILLUSTRATIVE EXAMPLE OF AN IMPACT RATING SCALE

The following is an illustrative example of an operational risk impact assessment scale:

SCORE	DIRECT FINANCIAL	INDIRECT COSTS & EXPENSES	OPERATIONAL DISRUPTION	REGULATORY & LEGAL	REPUTATIONAL	COMMUNITY	EMPLOYEE	CUSTOMER
MINOR (1)	Non-material direct financial loss that is well within risk appetite.	Minimal opportunity costs/foregone revenue or other costs associated with event response, recovery, and/or remediation that are well within risk appetite.	Little to no impact on operations.	Little to no change in regulatory scrutiny, frequency of contact, and/or requests for operational or governance changes	Little to no national coverage, limited and controlled local adverse media attention toour brand, name, or industry status	No adverse impact(s) on the environment or community stakeholders. R	Event impacts <10% of employees R	Event impacts <10% of customers
MATERIAL (2)	Material direct financial loss that could put pressure on risk appetite.	Some opportunity costs/foregone revenue or other costs associated with event response, recovery, and/or remediation that could put pressure on risk appetite.	Some disruption to non-critical operations or disruption to critical operations that is well within risk appetite and impact tolerances.	Limited and specific increase in regulatory scrutiny, frequency of contact, and/or requests for information, operational or governance changes. Non-material impact to our ability to conduct business and achieve objectives. R	Limited/controlled national and/or substantial local adverse media attention to our brand, name, or industry status	Minimal and isolated adverse impact(s) on the environment or community.	Event impacts 10 to <40% of employees	Event impacts 10-<40% customers
SIGNIFICANT (3)	Significant direct financial loss that could breach risk appetite. R	Significant opportunity costs/foregone revenue or other costs associated with event response, recovery, and/or remediation that could breach risk appetite. R	Significant disruption to one or more critical operation that could breach risk appetite and put pressure on impact tolerances.	Material and broadening increase in regulatory scrutiny, frequency of contact, and/or requests for information, operational or governance changes. Ability to conduct business and achieve strategic business objectives is materially affected.	Substantial national adverse media attention with short-to-medium term damage to our brand, name, or industry status R	Significant adverse impact(s) on the environment or wide-spread harm to the community.	Event impacts 40% to <60% of employees	R Event impacts 40% to <60% of customers
CATASTOPHIC (4)	Catastrophic direct financial loss that could threaten or breach risk capacity.	Catastrophic costs associated with event response, recovery, and/or remediation that could breach risk capacity.	R Prolonged and significant disruption impacting critical operations that could breach impact tolerances.	Substantial and pervasive increase in regulatory scrutiny, frequency of escalations and contact, and requests for information, operational and governance changes. Ability to conduct business and achieve objectives is significantly compromised due to lack of regulatory confidence.	Sustained adverse global media attention with medium-to-long term damage to our brand, name, or industry status. Ability to conduct business and achieve strategic objectives is affected by lack of public confidence.	Catastrophic and irrevocable harm to the environment and community.	Event impacts ≧60% of employees	Event impacts ≧ 60% of customers

Where more than one impact may occur (which is the norm), the worst-case impact determines the overall impact rating. Let's take the example of a ransomware attack affecting the Canadian Life Insurance segment.

R **POTENTIAL IMPACT RATING = CATASTROPIC**

INHERENT RISK ASSESSMENT

Can you identify the 9 financial impacts?

Financial impact refers to the direct financial loss and indirect costs and expenses associated with an operational risk event.

KMRC

INHERENT RISK ASSESSMENT

Can you identify the 5 regulatory impacts?

Regulatory Impact refers to the impact of an operational risk event on the relationship between the firm and its Regulators.

KMRC

INHERENT RISK ASSESSMENT

Can you identify the 7 operational impacts?

Operational impact refers to the impacts of an operational risk event on day-to-day operations.

INHERENT RISK ASSESSMENT

Can you identify the 7 reputational impacts?

Reputational impact refers to the harm that can result from an operational risk event on a firm's reputation.

KMRC

INHERENT RISK ASSESSMENT

Can you identify the 6 customer impacts?

Customer impact refers to the harm and effects that an operational risk event can have on a firm's customers or account holders.

KMRC

INHERENT RISK ASSESSMENT

Can you identify the 3 employee impacts?

Employee Impact refers to the harm and effects of an operational risk event on the firm's employees.

KMRC

INHERENT RISK ASSESSMENT

Can you identify the 6 community impacts?

Community impact refers to the harm and effects an operational risk event can have on the firm's relationship with or on the well-being of the broader community, in which it operates.

INHERENT RISK ASSESSMENT

Can you identify the 7 strategic impacts?

Strategic impact refers to the harm and effects that an operational risk event can have on a firm's strategy itself and/or ability to achieve its strategic objectives.

KMRC

COMBINE THE LIKELIHOOD RATING WITH THE POTENTIAL IMPACT RATING TO DETERMINE OVERALL INHERENT RISK RATING

OVERALL INHERENT RISK RATING SCALE

LIKELIHOOD OF RISK EVENT					
	CERTAIN	MODERATE	HIGH	CRITICAL	CRITICAL
	LIKELY	MODERATE	HIGH	HIGH	CRITICAL
	UNLIKELY	LOW	MODERATE	HIGH	HIGH
	RARE	LOW	LOW	MODERATE	MODERATE
		MINOR	MATERIAL	SIGNIFICANT	CATASTROPHIC
		POTENTIAL IMPACT OF EVENT			

1. RISK OF RANSOMWARE ATTACK
2. RISK OF AN INCORRECT FUND TRANSFER
3. RISK OF UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION