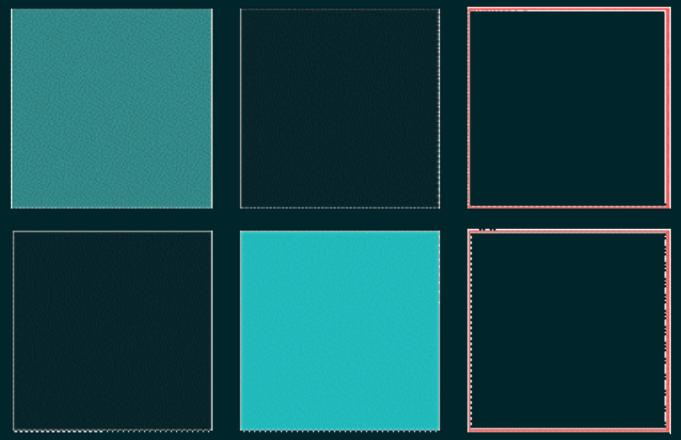
KMRC

ORM in Motion!

WEEK 2



02

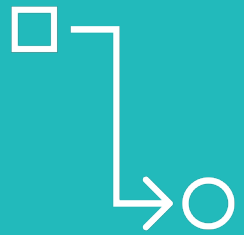
RISK TAXONOMIES

WEEK 2

What is a Risk Taxonomy?

A Risk Taxonomy is a system used to consistently organize and classify sets of risks. There are many types of risk taxonomy used in the ORMF, including but not limited to:

Reporting Taxonomy



Causal Taxonomy

Event Taxonomy

Impact Taxonomy

Op Risk Themes

Key Terminology*

ILLUSTRATIVE EXAMPLES

Operational risk reporting taxonomy

L1	Definition
Business disruption	*The risk of disruption or compromise to the performance of critical operations*
Cyber risk	*The risk of unauthorized access, modifications, or malicious use of information technology assets*
Damage to physical assets	*The risk of damage to the firm's physical assets*
Fraud	*The risk of intentional deception or misrepresentation for purposes of personal gain.*
Health and safety risk	*The risk of harm to individuals' physical, emotional, or mental wellbeing while performing business activities on or off firm premises*
Financial reporting risk	*The risk of inaccurate or failed financial reporting*
Information risk	*The risk of data integrity, availability, or confidentiality being compromised*
Information technology risk	*The risk of system errors, malfunctions, or unavailability*
Legal risk	*The risk of violating laws or being involved in a legal dispute brought forward by another party*
Model risk	*The risk of inadequate or failed design, development, implementation or use of internal models.*
Processing risk	*The risk of inadequate or failed processing of a transaction*
Third party risk	*The risk of relying on or engaging with third-parties*

ILLUSTRATIVE EXAMPLES

Operational risk themes

Individual risk categories can be grouped into higher level "themes" for reporting purposes. For example:

- Legal risks
- Regulatory compliance risks
- Readiness for regulatory change

- Third-party risk
- Business disruption risk
- IT and cyber risk
- Data risk
- Climate change
- Processing risk
- Model risk
- Project risk
- People risk

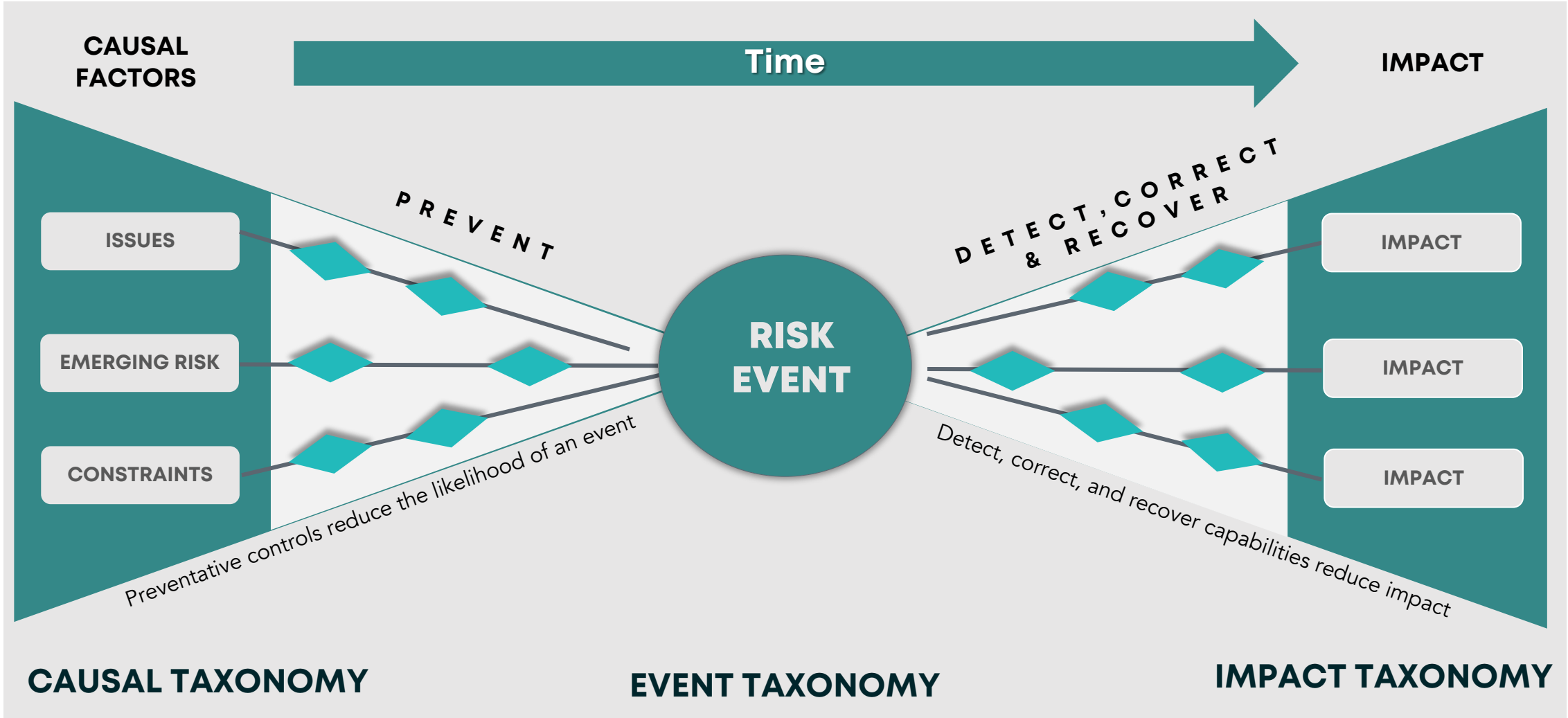
- Fraud
- Money laundering
- Bribery and corruption
- Cyber risk
- Unauthorized trading

- Health and safety risk
- Theft and damage to non-digital assets
- Theft, and damage to digital assets
- Information security risk

- Culture risks
- Social risks

ILLUSTRATIVE EXAMPLES

A “bow-tie” taxonomy enables more precise classification of risks



ILLUSTRATIVE EXAMPLES

Operational risk causal taxonomy

L1	L2 (not exhaustive)	L3 (not exhaustive)
People causes	Misaligned incentives and culture	Inappropriate incentive and compensation
	Detrimental human behaviour	Human error
	Inadequate talent management	Inadequate availability or allocation of people
Strategy and process causes	Inadequate design	Inadequate process design
	Flawed execution	Model error
	Inadequate controls	Inadequate records management
System and infrastructure causes	Inadequate technical design	Poor system design
	Unavailable or inadequate non-IT infrastructure	Unavailable non-IT infrastructure (e.g., building)
	Inadequate security	Inadequate physical security
External causes	Third party failure	Third party failure
	Criminal activities	Criminal activities
	Geopolitical events	Geopolitical events

ILLUSTRATIVE EXAMPLES

Operational risk events taxonomy

L1 (not exhaustive)	L2 (not exhaustive)	DEFINITIONS
Digital asset	Data integrity compromise	*The risk of data being deleted, corrupted, or altered by an internal party, external party, or process*
	Data availability compromise	*The risk of data being made unavailable, missing, or incomplete by an internal party, external party, or process*
	Data confidentiality compromise	*The risk of data being disclosed or stolen without authorization, by an internal party, external party, or process*
Non-digital asset	Theft of assets	*The risk of a physical asset (incl. physical assets containing data, such as papers) being stolen by an internal or external party*
	Damage to physical assets	*This risk of a physical asset being damaged by an internal party, external party, or process*
	Workplace disruption	*The risk of employees not being able to access or work out of the office*
People	Harm to individuals	*The risk of physical or mental harm to individuals or theft of personal property on premises*
	Breach of employment relations	*The risk of non-compliance with labour and human rights laws*
	Scandal	*The risk of the firm, an employee, or group of employees being involved in an action, event, or situation regarded as morally questionable or wrong by the public*
Financial crime	Fraud	*The risk of intentional deception or misrepresentation for purposes of unfair advantage or financial gain*
	Rogue trading	*The risk of an employee or group of employees engaging in speculative or high-risk unauthorized trading activities*
	Bribery and corruption	*The risk of giving, offering, or agreeing to provide benefits to others to improperly influence an outcome or to obtain or retain an advantage or economic gain*

ILLUSTRATIVE EXAMPLES

Operational risk impact taxonomy

L1	L2 (not exhaustive)	Definitions
Financial	Regulatory fines and monetary penalties	Direct monetary fine or penalty levied by a Regulator, resulting from a risk event
	Legal costs	Costs associated with legal process (e.g. attorney fees, settlement costs, litigation losses), resulting from a risk event
	Missed financial gain	Financial gain is not able to be realized (e.g. unable to trade)
Non-financial	Regulatory scrutiny	Regulatory letters, warnings, increased frequency of exams, etc
	Reputational damage	Degradation brand and competitive standing due to loss of stakeholder respect or trust
	Diversion of resources	Unplanned diversion of resources (e.g. management attention)
	Employee detriment/culture	Detriment to employees (e.g. lowered morale, physical injury, loss of information
	Relationship damage	Damage to relationships with strategic Business Partners or other external stakeholders (e.g., Plan sponsors)

How are risk taxonomies used in the ORMF?

There are many ways in which the risk taxonomies are used in the ORMF:

#	ORMF element	How is taxonomy used/applied?	Benefits
1	**Risk Register**	• Taxonomies are used to capture mandatory metadata • Drop-down lists for users to select from when classifying and recording identified risks	• Consistent identification and documentation of risks • Avoid/reduce duplication of risks in register
2	**Risk mapping**	• Mapping risks at consistent levels of granularity	• Enables upstream and downstream visibility into risks
3	**OREs, Incidents, Issues**	• Classification of risk event/incident/issue by event category • Classification of root cause by causal category(ies) • Classification of impact(s) by impact category	• Enables consistent analysis and aggregation of data • Identification of patterns and systemic problems
4	**Risk Assessments**	• Taxonomy is embedded in risk assessment methodology • Leveraged to identify key and emerging risks	• Enables consistent assessment of inherent and residual risks
5	**Monitoring**	• Used to consistently identify and define KRIs (i.e., causal taxonomy for leading, events taxonomy for lagging)	• Enables consistent monitoring across enterprise • Avoid duplication of effort and gaps in coverage
6	**Scenario Analysis & Stress Testing**	• Causal and event taxonomies used to identify relevant key risks and inform scenario narrative • Impact taxonomy used to inform scenario narrative and impacts	• Supports clear and consistent understanding of control environment and landscape • Supports efficient build out of scenario
7	**Reporting**	• Used to analyse and categorize risks • Used to aggregate and report on risks, trends, and themes	• Enables aggregation of risk data • Enables accurate and consistent understanding of risk profile

Key steps involved in establishing a Risk Taxonomy

#	STEPS	DESCRIPTION
1	**Define Scope & Objectives**	• Define the objectives of the risk taxonomy – how and where will it be used? • Define the scope of the risk taxonomy – is it enterprise-wide, for a specific risk program, is it to address a specific risk type?
2	**Identify Key Stakeholders**	• Identify key stakeholders that should be involved in or that will be affected by the risk taxonomy, such as oversight functions, subject matter experts, internal audit, control owners, risk owners, etc
3	**Gather Relevant Information**	• Collect information about risk landscape • Collect information about what risks your peers and regulators are focused on • Engage with subject matter experts (internally and externally) to gain insights into key and emerging risks and risk trends
4	**Categorize Risks**	• Group risks into meaningful user-friendly universal categories • Determine what logical and systematic structure will be applied to organize and group the risks (e.g., hierarchical, relational, etc)
5	**Define Common Risk Attributes**	• Define the common attributes that will be used to document each risk within the taxonomy • Mandatory risk attributes will enable generation of metadata that can be used to perform trend analysis
6	**Socialize Taxonomy & Refine**	• Share risk taxonomy with key stakeholders and obtain feedback on the structure, categories, and attributes • Refine the taxonomy based on feedback and finalize
7	**Integrate within ORMF**	• Embed the risk taxonomy in the ORMF, including updating any relevant methodologies, templates, and enabling tools/systems