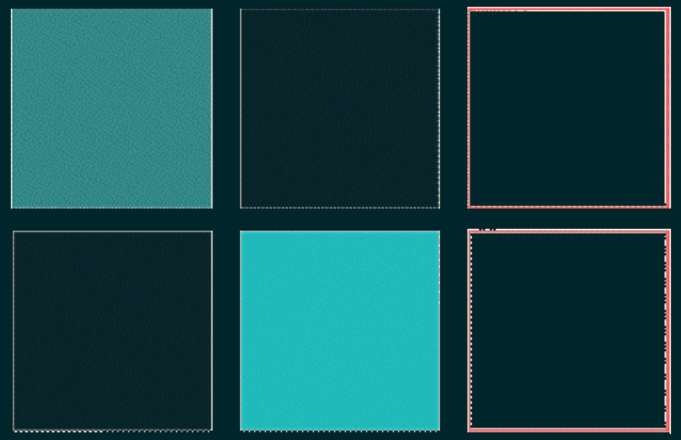
KMRC

ORM in Motion!

WEEK 2



03
CONTROL TAXONOMIES

OVERVIEW

What is a control taxonomy?

A Control Taxonomy provides a clear and organized framework for understanding, classifying, managing, and communicating internal controls. The taxonomy helps us to consistently categorize controls into specific groups, based on their nature, purpose, and area of application to make it easier for us to manage them.

Imagine you're putting together a puzzle...

- Each puzzle piece represents a unique control characteristic.
- When all the puzzle pieces are in one single pile, it is really difficult to find the piece we need and to see the big picture, in terms of how the pieces are supposed to fit together.
- When we sort the puzzle pieces into groups that make more sense – corners, edges, colours, and other common characteristics, it becomes easier to find what we need and to identify if any pieces are missing.

EXAMPLES

Control taxonomies

It is important to use a list of consistent definitions of key control characteristics to enable consistent understanding, classification, and assessment of internal controls.

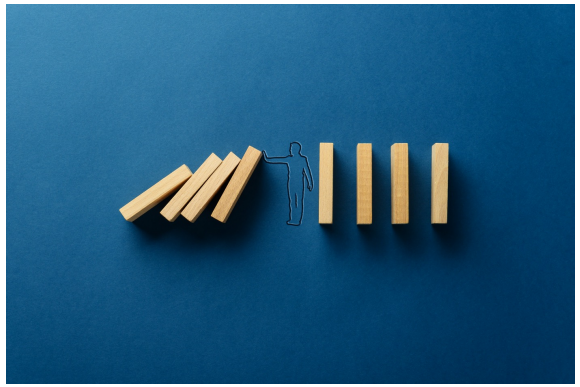
CONTROL CHARACTERISTICS					
CONTROL TYPE	**CONTROL METHOD**	**CONTROL COVERAGE**	**CONTROL FREQUENCY**	**CONTROL LAG TIME**	**CONTROL CERTAINTY**
Refers to whether the control is preventative, directive, detective, or corrective	Refers to whether the control is fully automated, partially automated, or fully manual. The higher the degree of automation, the higher the accuracy, consistency, and speed of the control.	Refers to the degree to which the control meets the control objective and address the underlying risks. 100% or less than 100%?	Refers to how often a control is performed over the defined period. Is it continuous, periodic (scheduled), or performed on an ad hoc basis?	Refers to the worst case scenario, in terms of how much opportunity there is for a risk to go undetected by the control. Preventative controls tend to have no time lag.	Refers to the degree of reliance that can be placed on the control. Is it definitive or does it require judgement?

Identify and define common control characteristics to enable consistent documentation and classification of internal controls in the control library and the risk assessments, monitoring, and testing activities.

ILLUSTRATIVE EXAMPLES

CONTROL TYPES

Let's explore the different **Control Types:**



PREVENTATIVE CONTROL

Preventative Controls are designed to stop risks from manifesting as breaches or events. These controls are designed to establish barriers that hinder the likelihood of undesirable outcomes.

DETECTIVE CONTROL

Detective Controls are designed to identify risks, issues, or incidents/events that have already occurred or are still occurring.

DIRECTIVE CONTROL

Directive Controls are designed to guide and direct the actions and behaviours of individuals to yield consistent outcomes.

CORRECTIVE CONTROL

Corrective Controls are designed to address and rectify issues, errors, or adverse events that have already occurred within an organization to mitigate the impacts of risk events.

ILLUSTRATIVE EXAMPLES

CONTROL METHODS

Let's imagine the **Control Objective** is to "prevent the grass from dying" or put another way, "to ensure optimal grass irrigation". Consider the pros and cons of each of the following potential control methods:

FULLY AUTOMATED SPRINKLER-SYSTEM

This sprinkler system is designed to:

- Ensure consistent and even coverage.
- Water at specific times when demand is lower
- Eliminate the need for human intervention, freeing up staff for other tasks
- Prevent over-watering
- Cover large areas efficiently
- Be remotely controlled, allowing adjustments to be made in real-time based on weather conditions and grass needs

MANUAL WATERING SYSTEM

This control involves staff manually:

- Conducting daily visual inspections to monitor grass health and moisture levels
- Performing soil probing to assess soil moisture depth and determine whether the grass is receiving adequate water
- Making adjustments to irrigation systems or moving hoses to provide additional water to drier areas or reduce water to areas with excess moisture

ILLUSTRATIVE EXAMPLES

CONTROL METHODS

Imagine the Control Objective is to "prevent us from getting wet when it rains". Control Coverage refers to the extent to which the control meets the control objective. Or, put another way, to what extent does the control cover the risk of getting wet when it rains?

WATER-PROOF SHELTER

This control is designed for 100% full coverage of the risk.

Going inside the water-proof shelter will keep you fully dry when it rains. That said, it may need to be combined with other controls to cover all circumstances.

UMBRELLA

While an umbrella can provide significant protection from rain, it may not keep you 100% dry under all circumstances.

An umbrella will shield you from rain falling directly from above, but rain can still reach you from the sides if the wind is blowing strongly or if the rain is coming at an angle.

RAINCOAT

While a good raincoat may provide more protection from rain than an umbrella, it may still not keep you 100% dry under all circumstances.

The raincoat will not protect your feet from getting wet and may let moisture in if exposed to prolonged periods of rain.

ILLUSTRATIVE EXAMPLES

CONTROL FREQUENCY

Control Frequency refers to how often a specific control activity is performed within a defined period. The **Control Objective** is to "prevent and detect burglary" so we have established the following 3 controls that have different control frequencies:

CONTINUOUS

This professional home security system provides 24/7 monitoring services. If an alarm is triggered, the monitoring center is alerted and will quickly contact you, emergency services, and/or dispatch security personnel if needed.

PERIODIC

This security patrol service provides regular and scheduled checks on the property to monitor its security and address potential risks.

AD HOC

You lock your doors every time you leave the house, which is not on a set schedule.

ILLUSTRATIVE EXAMPLES

CONTROL LAG TIME

Our **Control Objectives** are to 1) prevent heart disease, 2) detect heart disease early, and 3) receive timely medical care in the event of a heart attack, so we have established the following 3 controls that each have a different lag time:

1. NO LAG TIME

Healthy diet and exercise will help to prevent heart disease.

2. < 1 YEAR LAG TIME

Annual physicals increase the odds of detecting heart disease early by providing an opportunity for healthcare professionals to assess your overall health, identify risk factors, and catch early signs of heart-related issues.

3. <15 MINUTES LAG TIME

Wearing a medical alert bracelet that can be used to immediately alert 911 of your need of medical assistance will reduce lag time between when you have a heart attack and when you receive potentially life-saving medical intervention.

ILLUSTRATIVE EXAMPLES

CONTROL CERTAINTY

When determining Control Certainty, one should consider its reliability, consistency, and predictability. If the **Control Objective** is to "navigate mariners toward the nearest safe harbor or anchorage", then what would be the degree of Control Certainty for each of the following controls:

HIGH CERTAINTY - LIGHTHOUSE

- Resilient to adverse weather conditions.
- Provide highly consistent and predictable signals.
- Emit powerful light that can be visible over long distances
- Strong reference point for navigation in darkness and adverse weather conditions.

MODERATE CERTAINTY - BUOYS

- Susceptible to damage, corrosion, and wear
- Can be affected by changing water conditions, including waves and currents, which may impact their stability and visibility.

LOW CERTAINTY - TORCHES

- Dependent on battery life or fuel supply.
- Inconsistent in certain weather conditions.
- Dependent on the skill of the person handling them.

EXAMPLES

Control Hierarchies

The following is an illustrative example of a control hierarchy, which organizes controls based on their control objectives:

Control L1	Control L2	Control L3
Authorization & Segregation of Duties *People, systems, or processes serving as a gate between various parts of the firm's people, systems, or processes.*	Authorization Control Activities *Review and approval by authorized parties within the company of the authorization privileges granted across the enterprise.*	Authorizer and Stakeholder Check and Sign-off
		Employee Pre-Clearance
		Manager/Supervisor Approval
	Formal Approval of New Business Activities *A strict adherence to the review and analysis of all new processes, markets, countries, and services to be entered into by the company, by all impacted internal parties and external specialists.*	New Legal Entity Approval
		New Market/Country Approval
		New Product / Process Approval
		New Technology Approval
	Systems and Application Restrictions *Restrictions to prevent unauthorized access, modification, or unapproved use of systems and applications.*	Device Management
		Access Management
		Network Entitlements
		Systematic Blocks / Validation Edits
		Automated, Rule-Based Transaction Filtering

How are control taxonomies used in the ORMF?

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

#	ORMF element	How is taxonomy used/applied?	Benefits
1	**Internal Control Library**	• Taxonomies are used to capture mandatory metadata • Drop-down lists for users to select from when classifying and recording controls	• Consistent identification and documentation of controls • Avoid/reduce duplication of controls • Enables identification of gaps
2	**Risk mapping**	• Risks are mapped to key controls, identified using the control taxonomy (to define what is a key vs non key control)	• Enables firm to focus on what matters (i.e., key controls)
3	**Process mapping**	• Key controls are recorded in process maps, using the control library as the golden source of truth	• Enables controls to be defined in process maps at the appropriate and consistent level of granularity
4	**RCSA & NIRA**	• Taxonomy is embedded in control assessment methodology • Leveraged to identify relevant controls to address key risks	• Enables consistent assessment of control strength
5	**Testing**	• Embedded in the Test Universe and Test Plans • Used to define test scripts	• Avoid duplication of effort and gaps in coverage
6	**Scenario Analysis & Stress Testing**	• Used to identify relevant key controls to include in scenario • Used to document control gaps identified through scenario analysis, including updating control taxonomy to include controls to address future risks	• Supports clear and consistent understanding of control environment and landscape • Supports efficient build out of scenario
7	**Reporting**	• Embedded in thematic reporting on control environment • Categorization of issues and vulnerabilities being reported on	• Enables aggregation and disaggregation of control-related data (e.g., KCIs, issues, etc)

Key steps involved in establishing a Control Taxonomy

#	STEPS	DESCRIPTION
1	**Define Scope & Objectives**	• Define the objectives of the control taxonomy – how and where will it be used? • Define the scope of the control taxonomy – is it enterprise-wide, for a specific business unit or function, 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 control taxonomy, such as oversight functions, subject matter experts, internal audit, control owners, risk owners, etc
3	**Gather Relevant Information**	• Collect information about current state existing controls, which could include reviewing policies, procedures and other relevant documentation • Collect information about what controls are expected to be in place, which could include reviewing regulatory requirements, industry papers, benchmarking information, etc • Engage with subject matter experts (internally and externally) to gain insights into what controls should be in place to address the scope of the taxonomy
4	**Categorize Controls**	• Group controls into meaningful user-friendly universal categories, which could be based on control type, risk category, business process, control objective, or other relevant criteria. • Determine what logical and systematic structure will be applied to organize and group controls (e.g., hierarchical)
5	**Define Common Control Attributes**	• Define the common attributes that will be used to document each control within the taxonomy, including terms such as control owner, control objective, control characteristics, control performer, etc • Mandatory control attributes will enable generation of metadata that can be used to perform trend analysis
6	**Socialize Taxonomy & Refine**	• Share control 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 control taxonomy in the ORMF, including updating any relevant methodologies, templates, and enabling tools/systems

Let's Play...

KEY or NOT KEY CONTROL?

Let's play!

Scenario:

Rex and Ryan recently decided to undertake a large home renovation project. As part of this project, they would like to invest in buying the gourmet kitchen of their dreams. Before commencing on this project, they decide to perform a risk assessment to better understand the risks associated with their design decisions.

Ideally, they would like to have hardwood installed throughout the main floor, including in the kitchen but the risk assessment identified several risks that could damage the flooring in the kitchen, one of which is set out below:

Risk Statement

The risk of damage to the hardwood floors due to a refrigerator leak, caused by leaving the door open for too long.

Key or No Key Control?

Defining the Control Objective

Can you identify the strongest Control Objective to mitigate the identified key risk?

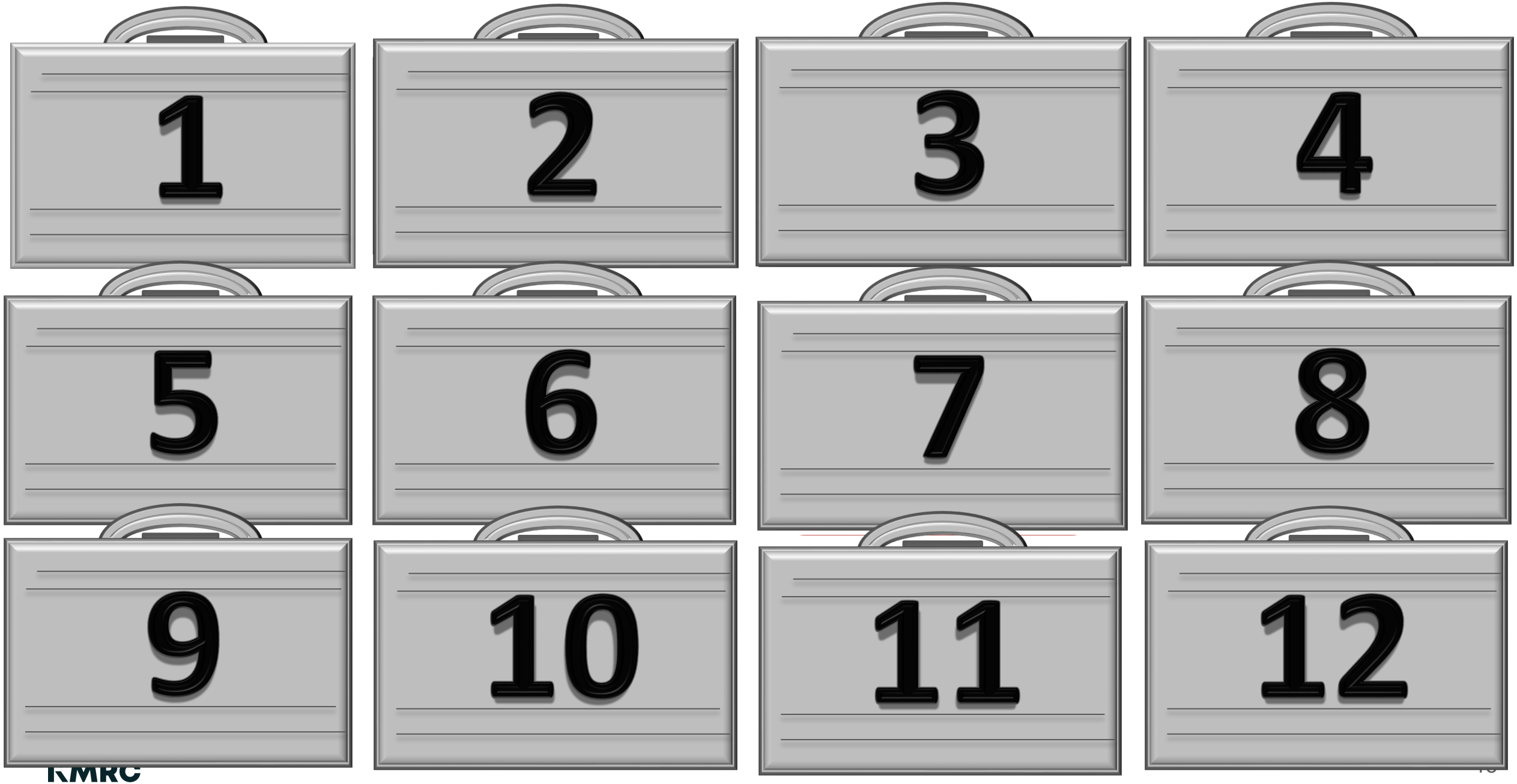
1. To prevent the refrigerator from leaking.
2. To prevent the refrigerator door from being left open.
3. To prevent the hardwood floor from being damaged.
4. To prevent the refrigerator door from being left open for more than 2 hours

How to play the game

Game Objective:
Theoretically, your goal is to select the case with the Key Control that satisfies the stated Control Objective (stated below) but the practical objective is to keep briefcases with higher control design effectiveness ratings in play long enough to get a good offer.

How to Play:

1. Start the game by selecting a case, which will be put aside for you.
2. Then choose one case at a time to be opened and eliminated.
3. After each case is open, the banker will make you an offer based on the probability that your first case contains the Key Control.
4. You will need to decide whether you will take the deal or say "NO DEAL".
5. You will continue to open one case at a time until you either accept a deal or all but two cases remain unopened (your original case and the remaining case in play).
6. When only two cases remain in play, you will have the option of swapping the cases.
7. Once you have made your decision of whether to swap your case with the remaining unopened case, the contents of each case will be revealed.


1
2
3
4
5
6
7
8
9
10
11
12

Control board

	Type	Method	Coverage	Frequency	Lag Time	Certainty	KEY?	Comments	Design Rating
Fridge door alarm	Preventative	Combination	100%	Continuous	n/a	High	YES	Will alert you if the door is left open but still requires human intervention to close the door	4
Training	Preventative	Manual	<100%	Periodic	n/a	Moderate	YES	Can raise awareness and promote routine to check and make sure the door is properly closed	3
Annual Maintenance & Repair	Corrective	Manual	<100%	Periodic	12 months	Low	NO	Can fix door seal but can't prevent the door from being left open	n/a
Reminder on the fridge door	Preventative	Manual	<100%	Continuous	n/a	Low	NO	Heavy reliance on human behaviour	n/a
Waterproof mat	Preventative	Manual	<100%	Continuous	n/a	Moderate	NO	Not relevant to the control objective.	n/a
Moisture detection flooring	Detective	Combination	100%	Continuous	5 minutes	High	NO	Not relevant to the control objective.	n/a
Keeping towels nearby	Corrective	Manual	<100%	Ad Hoc	<24 hours	Low	NO	Not relevant to the control objective.	n/a
Mop	Corrective	Manual	<100%	Ad Hoc	<24 hours	Low	NO	Not relevant to the control objective.	n/a
Freezer lock	Preventative	Manual	100%	Ad Hoc	n/a	Moderate	NO	The control would prevent us from meeting our business objective	n/a
Attestation	Not a control								
Operating Manual	Not a control								

KMRC