Carmichael.

20 April 2022

**Risk Management
Wicklow PPN
Marian Barnard
The Carmichael Centre**

About Carmichael

- Carmichael is a leading specialist training and support body for non-profits in Ireland

- We facilitate about 50-55 scheduled workshops every year – currently mostly online

- We also provided customised training and consultancy, working with non-profits across 26 counties – 274 such events in 2021.

Guiding nonprofits

About Carmichael

Carmichael is also an accommodation provider with over 40 non-profits co-locating in a shared space, pooling resources and tapping into peer support and services, enabling them to save time, reduce cost, upskill and thereby, focus more on delivering quality services to their beneficiaries.

Guiding nonprofits

Agenda

- What is Risk?
- Examples of risk
- Approaches to risk management, internal controls
- The benefits of risk management
- Questions
- Risk Processes and Calculations
- The Risk Register
- Break Questions and discussion
- Risk Proceses (continued)
- Conclusion

Risk

What is Risk?

Risk is the uncertainty of an event occurring that could have an impact (positive or negative) on you, your organisation and it's stakeholders.

There is always uncertainty in our lives and we are faced with risk every day whether it be in our home, in work or elsewhere.

Why take on Risk?

Why take on Risk?

For reward

For every risk we take there is a much greater chance of being rewarded. Sometimes the more risk we take, the greater the reward and the sense of achievement we feel.

Risk Vs Reward

SHOULD I APPLY FOR THAT JOB?

SHOULD I INVEST IN A PENSION?

SHOULD WE BUY A BIGGER HOUSE?

Risk in Business

We usually think of things like fire, flooding or having an accident.

In business, risk is not an event... risk is the uncertainty as to whether that event will occur or not.

So when we say measuring risk, we mean measuring the **uncertainty** around a significant event e.g. whether a fire of flood will occur and the impact it will have.

The Difference between Risk and No Risk

Situation 1

If a house is situated in the middle of a desert with no rivers or rain, you would say there is no chance of it being flooded or there is "no risk" of it being flooded.

Situation 2

Conversely, if the house was built directly beside a riverbank and the river bursts it banks every year without fail, the house is guaranteed to be damaged by flooding. We also say here that there is "no Risk" because the flood and ultimately the damage is a certainty.

Risk Vs No Risk

It is only when an event is a certainty to either occur or not occur that we can say no risk exists.

For all other situations there is always uncertainty and therefore there is always risk.

These are the situations that require risk management.

Risk and Not-for-Profits

The trust of it's stakeholders is crucial to the survival of a not-for-profit. Stakeholders must believe the organisation is stable.

If that trust is broken it could cause stakeholders to withdraw their support and cause reputational damage. This could cause the organisation to close. Therefore we must give no reason to doubt the stability of the organisation.

Always think of the **impact** that risk events would or could have on your organisation.
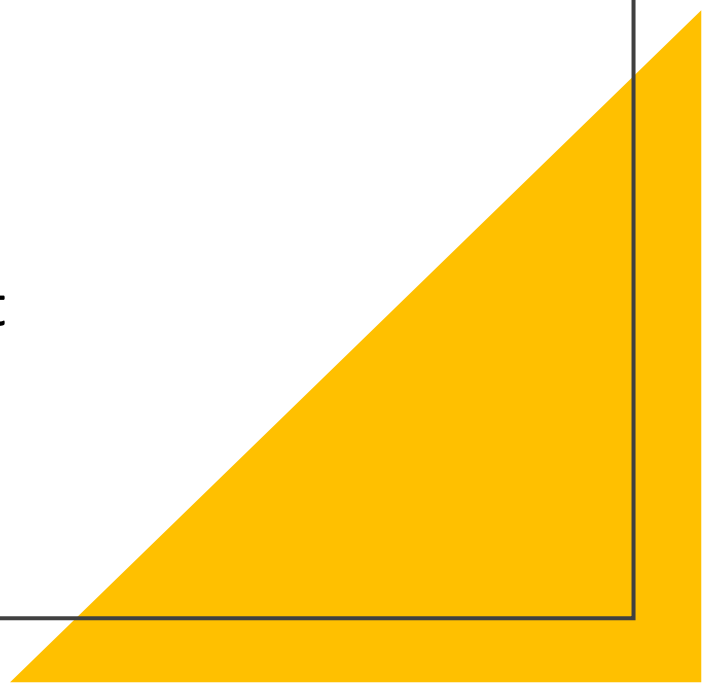
Risk Categories Not-for-Profits

Governance Risk

Strategic Risk

Compliance Risk (legal or regulatory)

Operational Risk

Financial Risk

Environmental Risk

Reputational Risk
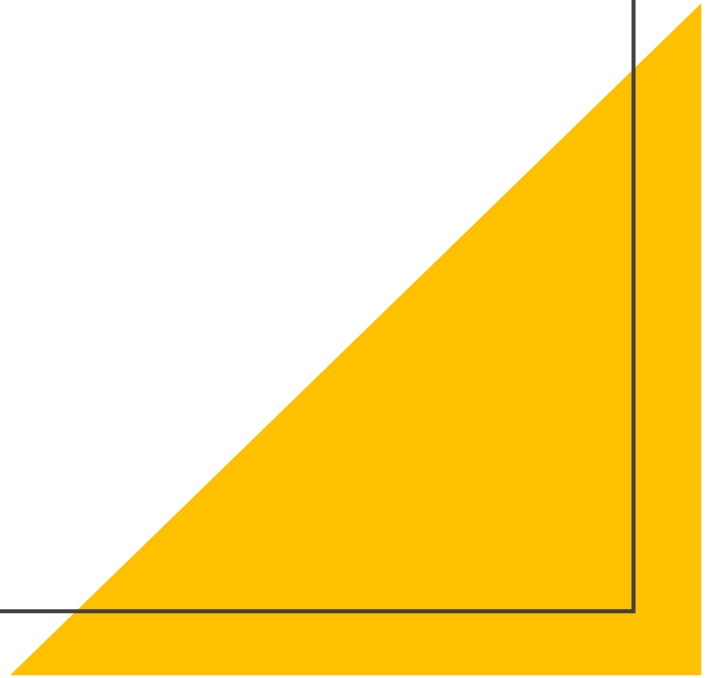
Governance Risks

- Governing body not knowing or living up to their responsibilities
- High board turnover
- Conflict on the governing body
- The risk that conflicts of interest are not manages
- Absence/non compliance with PPPGs
- The risk that there is not effective oversight of the organisations functions through lack of required skills/knowledge/engagement
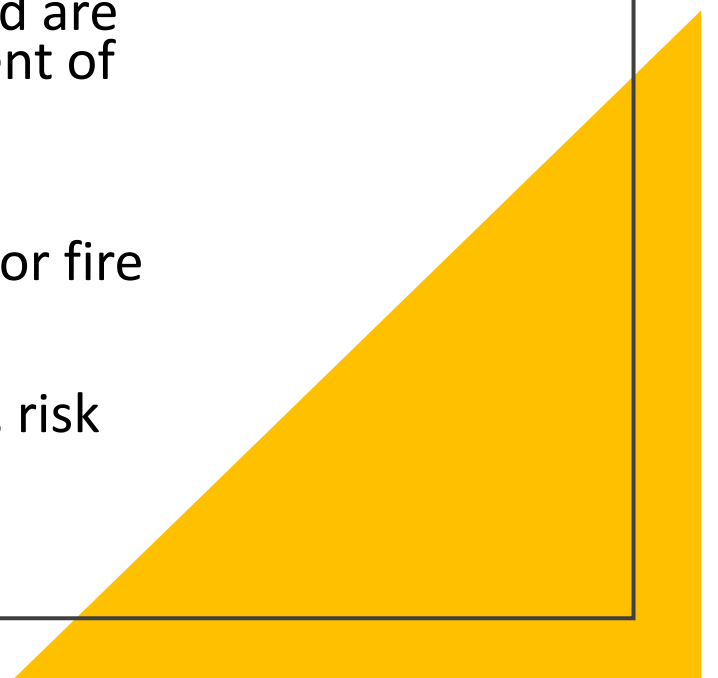- The risk that unethical behaviour is allowed to fester

Strategic Risks

- The risk of inadequate planning and implementation by the governing body
- The risk of inadequate resourcing to deal with business demands
- The risk of introducing new products or services without adequate planning/testing/resourcing

Compliance Risk

- The Risk of non-compliance with applicable legislation e.g. Data Protection, Charities Act, Companies Act etc..

- Failure to have an appropriate level of insurance in place for the organisation.

- The risk of non-compliance with the organisation's own policies and procedures

Operational Risks

- The risk of volunteers or employees being unavailable for duty, or volunteers or employees that are only trained for one role and are unable to cover for another volunteer or employee in the event of an absence

- The risk that the organisations premises is damaged by flood or fire

- The risk of IT systems being inadequate, risk of a data breach, risk of permanently loosing data

Financial Risk

- Failure to meet financial management and reporting requirements
- Failure to maintain prudent financial reserves
- Failure to plan to meet future needs
- Failure to properly assess and understand the financial viability of the organisation
- Misunderstanding funder priorities, poorly articulated funding applications or missed deadlines for funding applications
- The risk of internal fraud

Environmental Risk

- These are external risks to the business
- They are often out of your control but identifying them will enable the organisation to plan for the possibility of it happening

Reputational Risk

- Not for profits in general rely heavily on their reputation
- The organisation should consider the actual and perceived impact of the decisions it takes, ensuring that all decisions are taken in line with the best interests and purpose of the organisation.
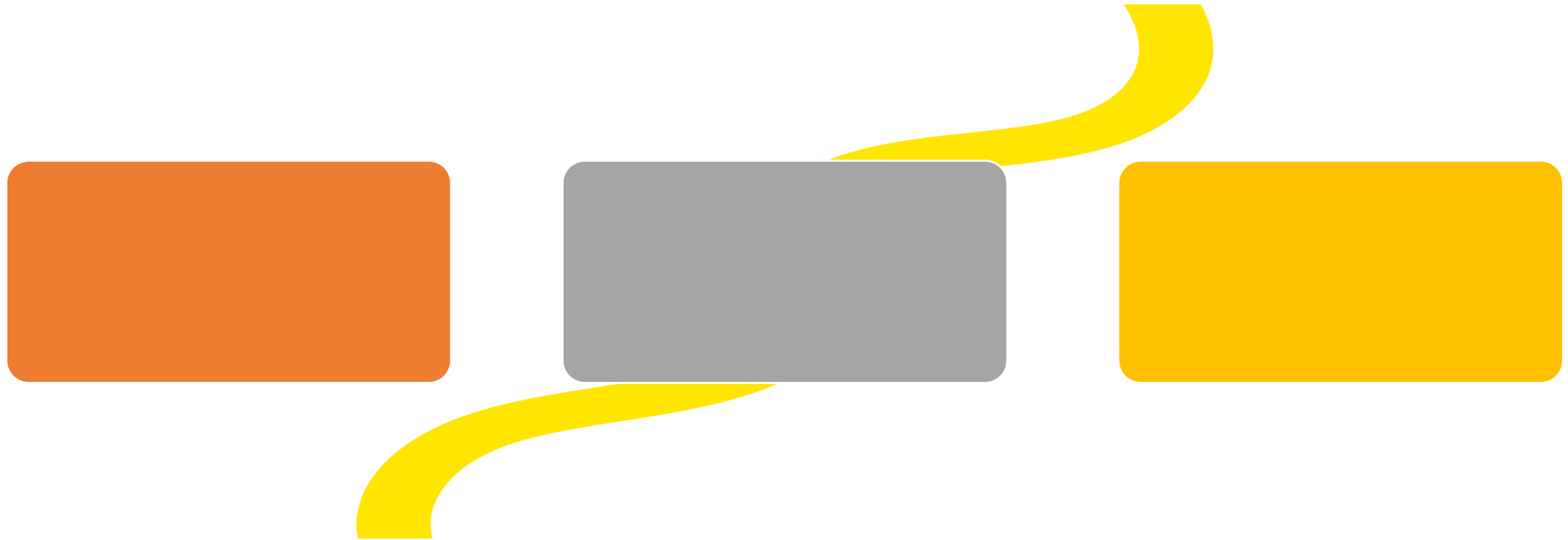
What can we do about Risk?

What can we do about Risk?

Accept

What can we do about Risk?
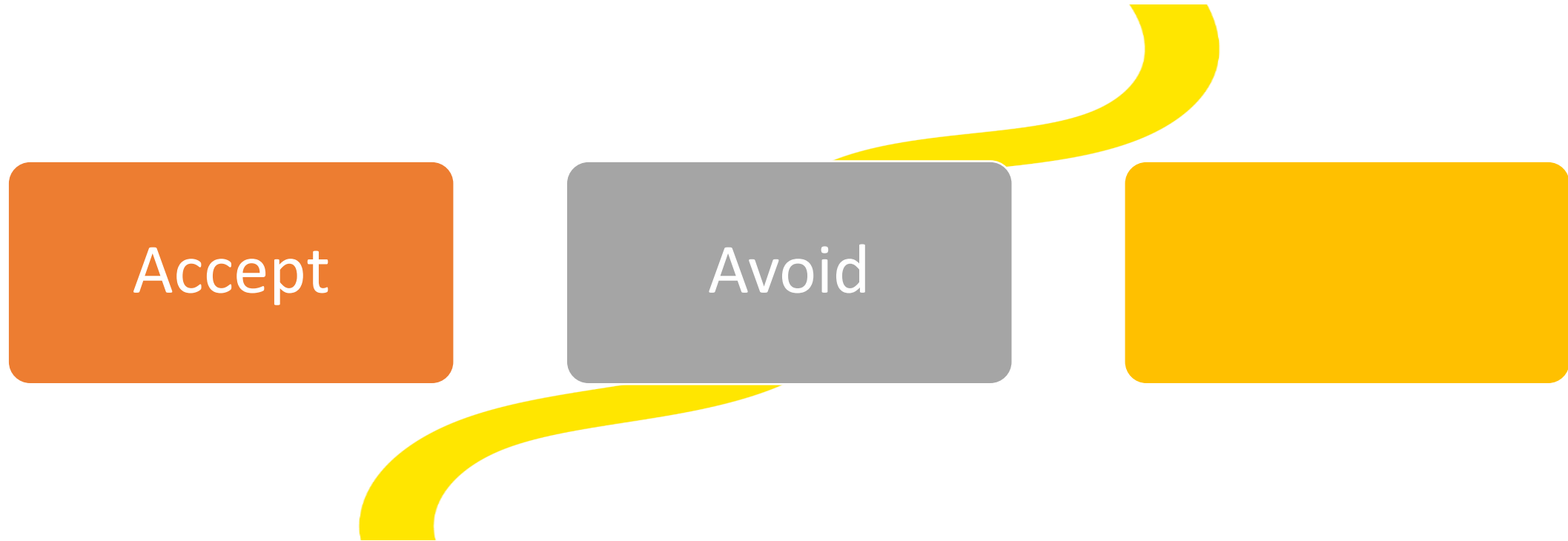
Accept

Avoid

What can we do about Risk?

Accept

Avoid

Mitigate
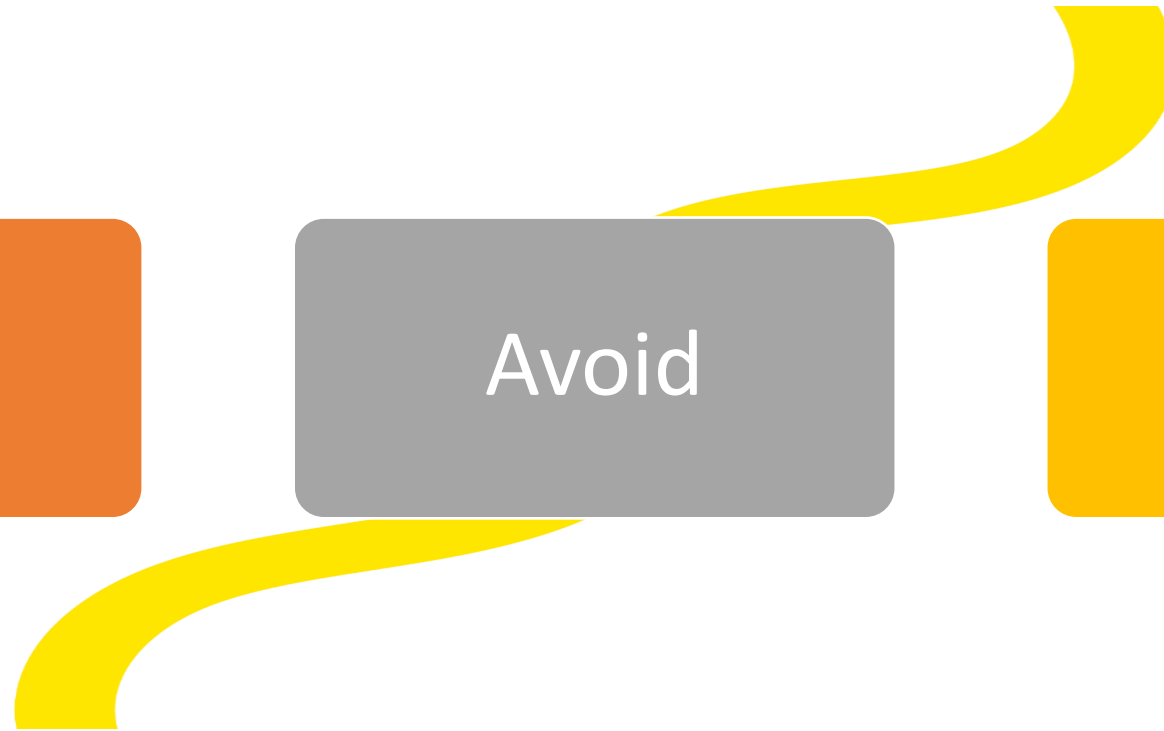
Internal Controls

The purpose of an internal control is to:

- Minimise the impact of the risk

- Minimise the likelihood of the risk occurring

- Or a combination of both

Types of Internal Control

Directive – minimise the likelihood of the risk occurring e.g. a policy or procedure

Corrective – these controls kick in when the event has occurred and are designed to minimise impact

Detective – aims to detect a risk at it's earliest opportunity an example would be checks carried out by an auditor.

Preventative – the most effective as they restrict an action or event from occurring which may pose a risk to the organisation. An example would be an IT system which blocks certain users from accessing certain areas of the system.

Approaches to risk management

Informal Approach

- No assigned officer
- Focus on perceived threats
- Reactive management of risks – no forward planning
- No risk reporting
- Seen as a one off exercise
- Ad hoc controls

Systematic Approach

- Asign a risk management Officer
- Objective analysis of risks
- Proactive management of risks
- Establish lines of reporting
- Risk culture set from the top
- Ongoing and evolving
- System of internal controls

Benefits of Risk Management

- More informed decision making – board and management

- Enhancements to processes and services – greater analysis will highlight areas for improvements

- Transparency and accountability – personnel become more accountable for their decisions

- Better prepared to respond to future risk events – "no surprises"

- Efficient allocation of resources – sufficient resources can be appointed to areas that pose the greatest threat

- Improved stakeholder confidence and trust

- Reputation – improves overall

Questions

Risk, Internal Controls

Definitions

Impact – The damage or effect a risk event would have should it occur

Likelihood – The likelihood of a particular risk event occurring

Internal Controls – measures put in place to reduce or limit the threat posed by the risk

Risk mitigation – the actions taken to enhance internal controls in order to reduce the threat posed by the risks
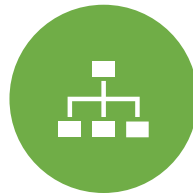
Risk Management Framework – The overall structure and approach within which you organize risk. Includes processes, policies, roles and responsibilities, controls and systems through which risk is managed.

- Risk Register – A documented list of the analysed risks to which your org is exposed.

- Risk Management Officer – The person appointed to maintain the risk framework.

- Risk Management Culture – Collective system of values and attitudes towards risk and risk management that shapes decisions.

- Risk Capacity – The amount of loss the org is able to absorb before it destabilises. Risk capacity will influence risk appetite.

- Risk Appetite – The amount of risk the org is willing to accept in pursuit of it's goals (low, medium, high). It should not exceed risk capacity.

- Risk Tolerance – Determines the level of risk tolerated before it initiates risk mitigation.

Definitions (continued)

Gross Risk Vs Net Risk

Gross Risk is the level of risk posed **before** systems and control measures that relate to the risk are put in place.

Net Risk is the level of risk posed **after** the consideration of the systems and control measures put in place to manage or mitigate the risk.

Four Step Approach to Risk Management

Step 1
Risk Strategy

A risk Appetite Statement

A Risk Management Policy

Risk Tolerances

Role Descriptions

Reporting Structures

Step 2 - Risk Assessment

1 Identify the risks

2 Analyse the risks

3. Evaluate the risks

Identify Risks

Brainstorm (all risks)

Minor to major risks

Include key individuals

Audit outputs

Complaints

Compliance Reports

Risk Events

Reference Strategic Plan

Analyse

- Analyse risk by risk
- Analyse risks without controls in place
- Assess likelihood of occurrence without controls
- Consider the impact if risk occurred

Measuring Impact

What is the Impact
           Score

- There is negligible or no impact
           1

- There is minor impact
           2

- There is significant impact
           3

- There is very serious impact which would undermine the stability of the org
           4

- There is a disastrous impact on the org which could result in termination of business
           5

Measuring Likelihood

What is the Likelihood   **Score**

- The risk is very unlikely to occur   1

- There is some possibility that the risk will occur   2

- It is likely that this risk will occur   3

- It is very likely that this risk will occur   4

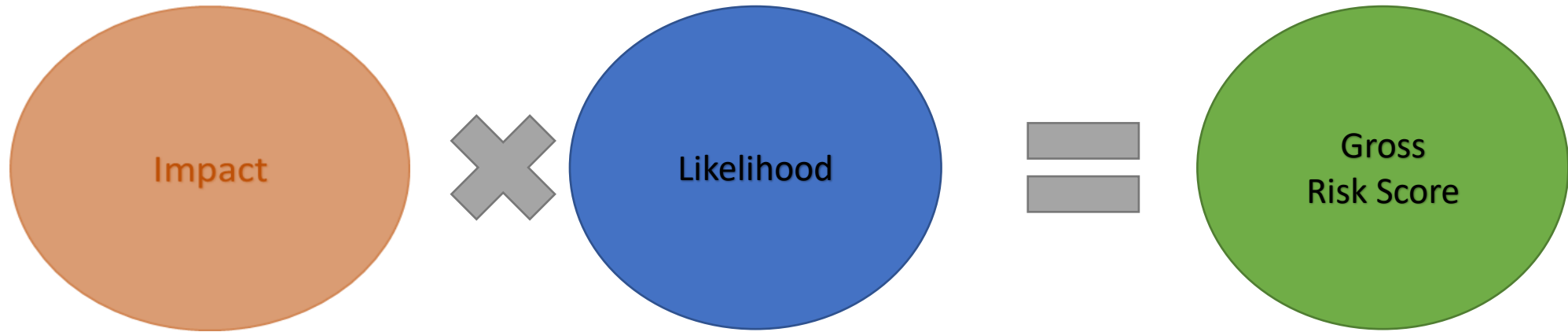- It is almost certain that this risk will occur   5
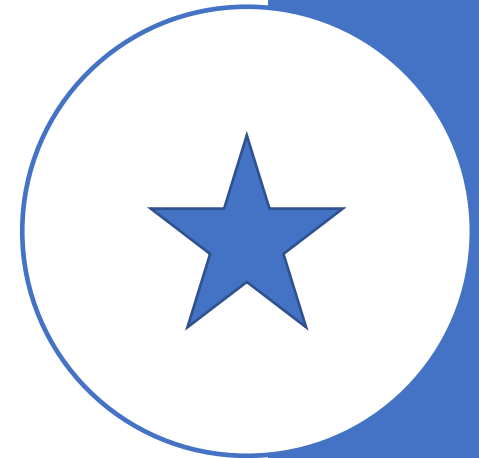
Calculating a Gross Risk Score – where controls don't exist

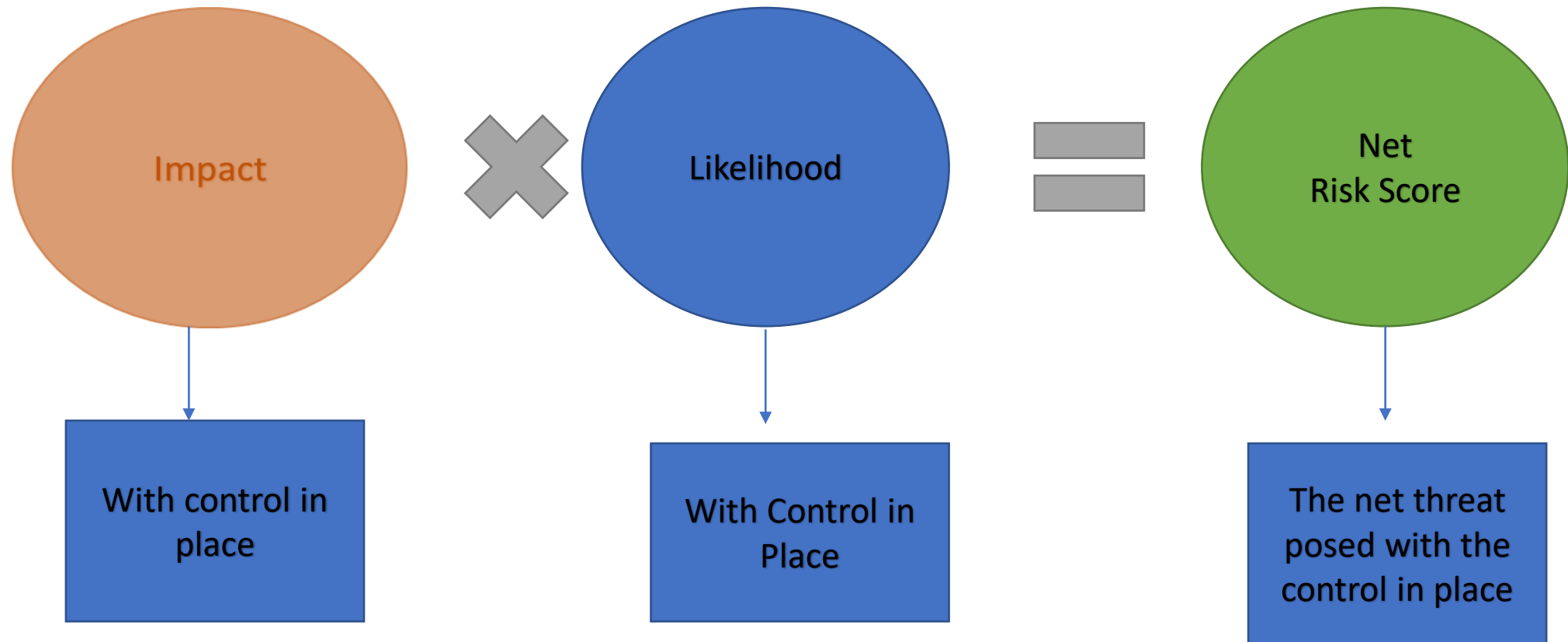Impact **×** Likelihood **=** Gross Risk Score

Evaluate

- With reference to the risk appetite and risk tolerance
- Assess risk with controls in place

Calculating a Net Risk Score – where controls do exist

Impact

Likelihood

Net Risk Score

With control in place

With Control in Place

The net threat posed with the control in place

Consequences		Likelihood				
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
5 Catastrophic		5 Moderate	10 High	15 Extreme	20 Extreme	25 Extreme
4 Major		4 Moderate	8 High	12 High	16 Extreme	20 Extreme
3 Moderate		3 Low	6 Moderate	9 High	12 High	15 Extreme
2 Minor		2 Low	2 Moderate	6 Moderate	8 High	10 High
1 Negligible		1 Low	2 Low	3 Low	4 Moderate	5 Moderate

Risk Matrix

Risk Register

- These analysed risks are recorded in the **risk register**
- Assigning a score to each risk allows the org to rank all their risks
- Those posing the least threat are lower on the register
- Those posing the greatest threat are highest on the register

Risk Action Plan and Communication

The risk register includes a plan of action for any areas where there are gaps in the control measures. These plans will be prioritised and regularly communicated to the appropriate personnel and to the governing body.

Outcome of Assessment

Risk Register

Step 3 – Risk Mitigation

- Risk Mitigation Plan
- Enhance controls
- Testing of controls

Step 4 – Risk Monitoring

Key Indicators

Risk Events

Trigger Events

On-going testing

Why Measure Risk?

Informed decision making: the more you know about a risk, the better you can compare it against the possible rewards. This will lead to a more informed decision.

Responsibilities

- The governing body

- The Risk Management Officer

- Auditors

- Regulators

- Other Stakeholders

- Everybody is responsible for risk management in an organisation – should not take excessive risks

- Risk culture
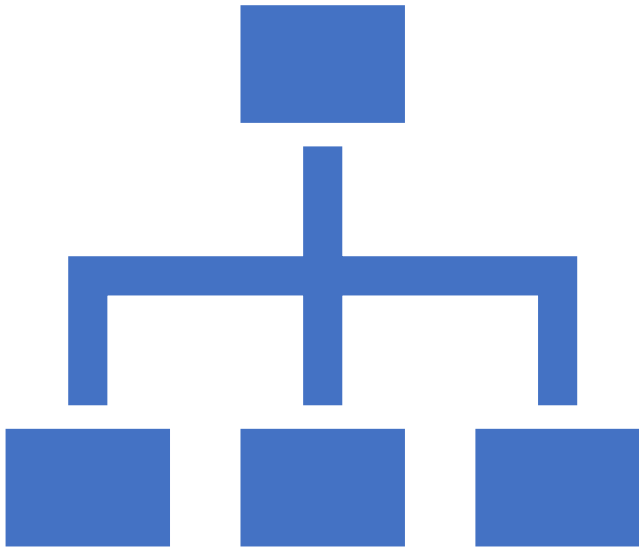
Overseeing the Risk Management Systems

- Training for all personnel

- Reporting - Board Minutes

- Risk Committee
  Review policy regularly

- Risk register maintained and up to date and reflect a range of views

- Internal Controls continually improved

Conclusion

Risk Management creates the environment for effective decision making. This environment is created via a framework of risk identification, analysis and evaluation, and controls, plans, assessments, mitigation, improvements and audits.

It packages the information and allows for the necessary oversight and effective decision making we need to sustain funding, safeguard our beneficiaries and keep the trust and confidence of our stakeholders

Final Questions and Discussions

Carmichael.

https://www.carmichaelireland.ie/courses/

Guiding nonprofits
carmichaelireland.ie