# Further exploration and reflection on governance: A focus on the role of risk management in good governance.

A presentation for Boards & Executive Management Teams in the governance, operation and oversight of designated centres.

Ciara McShane – Interim Deputy Chief Inspector
Conor Brady – Regional Manager
Tanya Brady – Regional Manager

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

# Welcome & Introduction

Ciara McShane
Interim Deputy Chief Inspector

- Purpose
- Intended Outcomes
- Q&A

**Ciara McShane**
**Interim Deputy Chief Inspector – Disability**

Ciara McShane is an experienced regulator, with over 23 years experience working in a variety of key roles in the field of health and social care and regulation. Ciara has worked in leadership roles across areas including adult and children social care services, services for physical and neurological disabilities, and as a Senior Consultant within the sphere of education, health and social care. Ciara has over 11 years experience working in regulation, having worked a number of roles in the regulation of disability services. Ciara holds qualifications in Applied Social Care, Psychology, Health and Safety and most recently completed a post graduate qualification in Governance through the Institute of Public Administration.

**Conor Brady**
**Regional Manager– Disability**

Conor Brady is a very experienced regulator with over 24 years expertise in the health and social service domain. Conor has worked in areas including Disability Services, Children's Early Intervention Services, Juvenile Justice/Probation Services, Child Protection & Welfare Services and Third Level Education. Conor possesses professional qualifications in Training and Education, Disability Studies, Health and Social Studies & Social Care, Sociology & Social Work, Governance & Risk Management and is currently studying at the Harvard - Kennedy School of Leadership & Management. Conor has a keen interest in Corporate Governance, Leadership & Applied Risk Management.

**Tanya Brady**
**Regional Manager– Disability**

Tanya Brady has over 34 years of experience in a variety of roles within health and social care settings. Tanya has worked in acute healthcare, community care, specialist clinical and disability settings in addition to third level education. Tanya has multiple qualifications and is driven to support the education of others through her roles as lecturer, external examiner and student placement facilitator for a number of third level institutions. Tanya as the health and social care professional representative contributed to the development of *'A National model of care for Paediatric Healthcare Services in Ireland'.* Tanya is a non-executive member of boards of management and has a unique understanding of corporate governance, corporate responsibility, leadership and management of risk.

# Provider Seminar
## March 2024- Reflection

Ciara McShane
Interim Deputy Chief Inspector

# Provider Seminar March 2024- Summary

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

- A collaborative working group was established to plan and implement the programme for the seminar

- Took a joint approach – voice of participating stakeholders

- Working group for the seminar consisted of representatives from:

    - The Disability Federation of Ireland
    - The National Federation of Voluntary Service Providers
    - The National Disability Services Association
    - The Health Service Executive
    - The Chief Inspector of Social Services Directorate within HIQA.

- The event explored the importance and value of the relationship between the board of directors and executive management team of provider organisations.

# Provider Seminar March 2024- Summary

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

- The importance of good relationships between the board and the executive
- Governance reviews

Roles and responsibilities – clarity and execution

Leadership

Strategy planning and implementation

Performance monitoring and reporting ( KPIs )

Capacity and capability of governance and leadership team and individuals

Compliance with legal, regulatory and governance obligations

Risk management system

Performance accountability arrangements

Internal controls systems

Board and sub-board structure / committee / working group effectiveness

Values and their visibility

Financial governance, management controls and reporting

Audit and assurance arrangements

# Recap-
# Good Governance

Ciara McShane
Interim Deputy Chief Inspector

# Corporate Governance- What is it?

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

It is the system by which organisations direct and control their functions and relate to stakeholders, in other words,

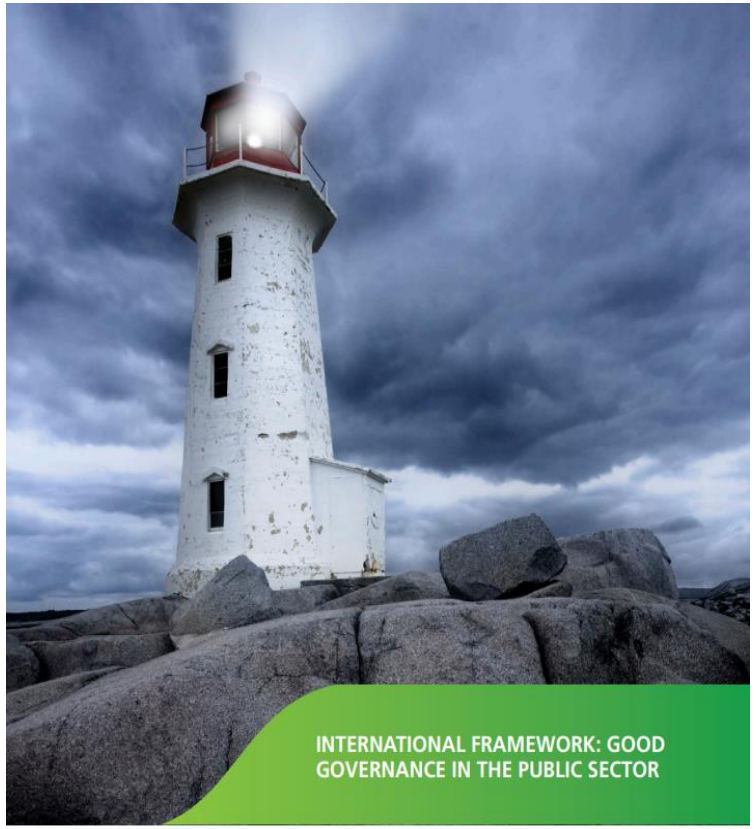
***the way in which organisations manage their business, determine strategy and objectives and go about achieving those objectives***

# Principles for Good Governance in the Public Sector

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

- Governance comprises the arrangements put in place to ensure that the intended outcomes for stakeholders are defined and achieved.

- The fundamental function of good governance in the public sector is to ensure that entities achieve their intended outcomes while acting in the public interest at all times.




IFAC International Federation of Accountants®

CIPFA The Chartered Institute of Public Finance & Accountancy

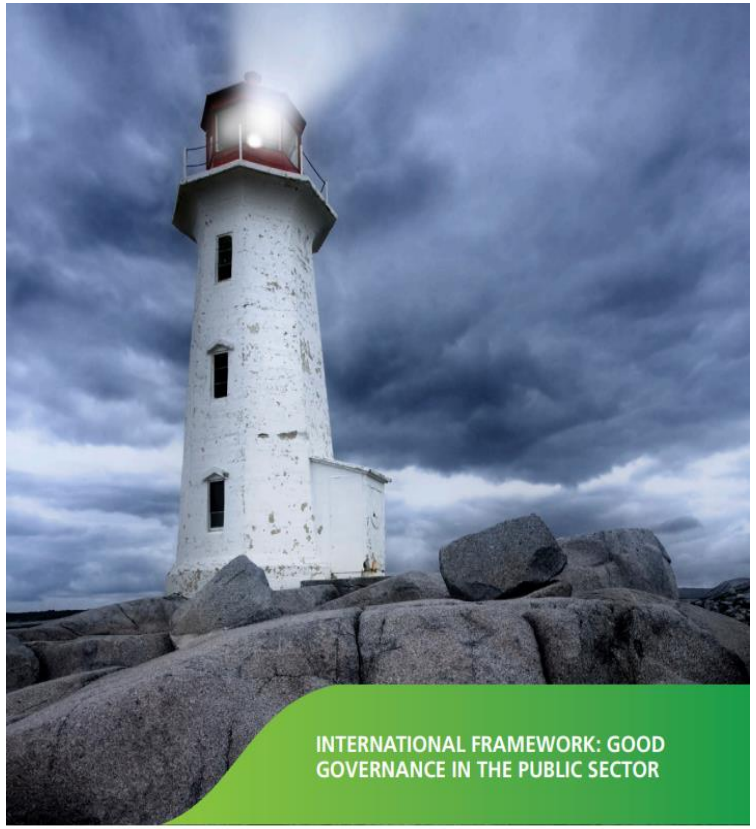
# Principles for Good Governance in the Public Sector continued

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

Acting in the public interest requires:

1. Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law.

2. Ensuring openness and comprehensive stakeholder engagement.




IFAC International Federation of Accountants®

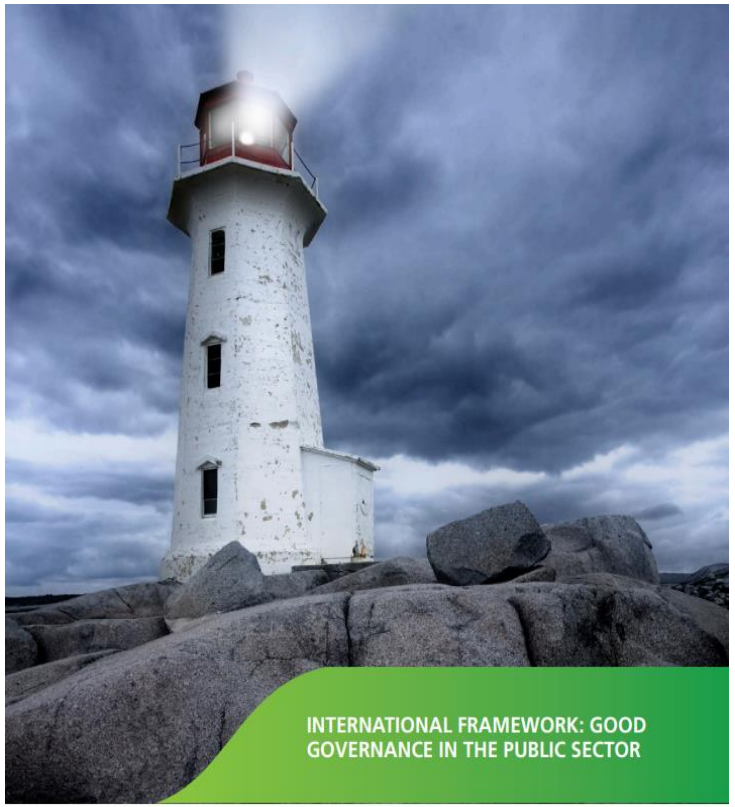
CIPFA The Chartered Institute of Public Finance & Accountancy

# Principles for Good Governance in the Public Sector continued

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

It also requires for arrangements be in place for:

3. Defining outcomes in terms of sustainable economic, social, and environmental benefits.
4. Determining the interventions necessary to optimize the achievement of the intended outcomes.
5. Developing the entity's capacity, including the capability of its leadership and the individuals within it.
6. Managing risks and performance through robust internal control and strong public financial management.
7. Implementing good practices in transparency, reporting, and audit, to deliver effective accountability




IFAC International Federation of Accountants®

CIPFA The Chartered Institute of Public Finance & Accountancy

# Why does Corporate Governance Succeed or Fail?

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

Bob Tricker, a renowned expert in Governance, observed:

*"Corporate Governance is more about human behaviour than about structures and strictures, rules and regulations. Corporate governance and effective risk management involves the use of power.*

*It is a political process."*

*(Tricker, 2020)*

# Focus on Risk

Conor Brady
Regional Manager

Tanya Brady
Regional Manager

# A Focus on Risk…

A key challenge for a Board/Governance structure is to balance strategic risk with acceptable reward

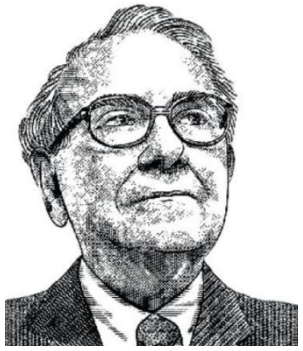
The risk appetite of the organisation is the level of risk the Board/Governance structure is willing to accept to achieve it's objectives

Awareness that risk is the effect of uncertainty on objectives and that the effects can be both positive and negative

- Predominant focus is on threats, vulnerabilities or exposures
- Balanced with a need to welcome and accept opportunities

"Risk comes from not knowing what you're doing."

– Warren Buffett



# Risk Management Concepts & Ideology


A large mass of cross sectoral Risk Management Theory & Concepts available. Much of this is transferable – Health, Aviation, Financial, Health & Safety, Regulatory, etc.

**Risk Management**

First step – Understanding Risk

Next Step -

**Developing a Culture of Risk Awareness at ALL levels in the organization…..this must start at the top!**

# Regulation 26 – Risk Management Procedures

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

26 (2)- The registered provider shall ensure that there are systems in place in the designated centre for the assessment, management and ongoing review of risk, including a system for responding to emergencies.

# Fundamentals of Risk Management

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

## What is Risk?

- Risk can be defined as an **uncertainty of outcome**, whether a positive opportunity or a negative threat.
- A risk may prevent or delay the achievement of an organisation or unit's goals or objectives.
- **A risk is not certain** – its likelihood and impact can only be estimated.

## What is Risk Management?

- The primary purpose of risk management is to **identify potential hazards** that may be experienced through our work, while **assessing** and **reducing** their risk of occurring to an **acceptable level**. It is a key activity which should take place on an ongoing basis within your organisation.
- A risk management strategy helps an organisation achieve its **strategic and operational objectives** by **managing and mitigating** the risks which have the **potential to affect the achievement** of those objectives.

## The Importance of Risk Management

- Effective Risk Management helps to create a **culture of accountability** and promote **responsible decision-making** throughout the Organisation.
- By linking business goals to risks, it **supports strategic thinking** and **alignment to business goals** across all levels.
- Effective risk management establishes **clear roles and responsibilities.**
- It supports **continuous improvement** as mitigation actions and control measure are identified to bring the risk within a tolerable level.

**Risk Management Guidelines for Government Departments and Offices (DPER, 2016):**

Organisations face **internal and external factors and influences** that make it **uncertain** whether and when the **extent to which they will achieve or exceed their objectives**. The effect that this uncertainty has on the organisation objectives is "risk".

# Fundamentals of Risk Management

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

The risk management cycle includes the following steps:

## 1. Objectives:

- Here consideration is given to the potential risks associated with an activity aligned to the business or corporate plan.

## 2. Risk Assessment:

- We identify the risks and uncertainties associated with our objectives and analyse the risk's impact and likelihood and mitigate them as appropriate.

## 3. Challenge and Evaluate Controls:

- We ask questions like are the controls effective? Do they help contain the risk? Do we need additional controls? and/or what other actions should be considered to improve those controls? Are the controls regularly reviewed?


Risk Management Cycle

# Fundamentals of Risk Management

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

### 4. Take Action:

- We take action for risks where controls are weak or absent or where the risk exceeds its assigned appetite. We are mindful of the cost versus the benefit of these changes and depending on Board defined risk appetite, the action taken may include tolerating, treating or eliminating the risk

### 5. Monitor and report:

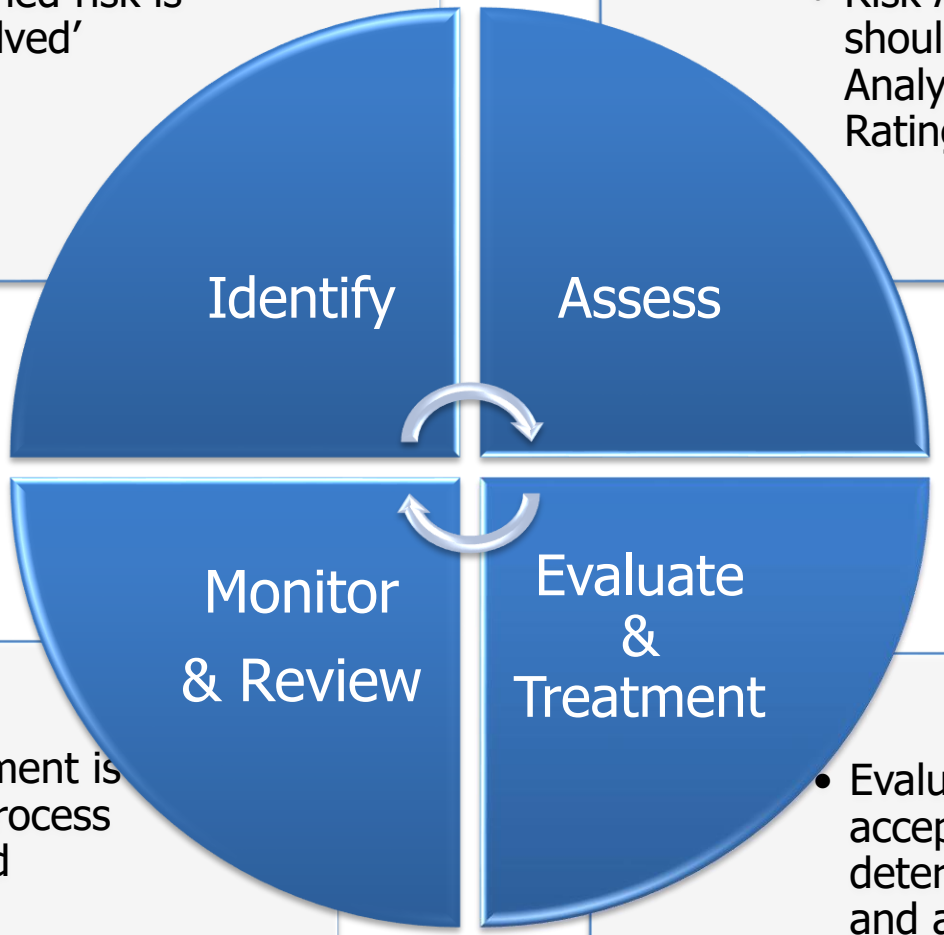
- All risks should be monitored, reviewed, actioned, recorded and reported as appropriate on a regular basis. Reviewing all risks and monitoring of internal control weaknesses, gaps and failures regularly should be a standing agenda item at team and management meetings.


Risk Management Cycle

# Risk Management Cycle

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

- 'A well identified risk is a risk half solved' (Prince2)




- Risk Assessment – should include Risk Analysis & Risk Rating
- Risk Management is an iterative process that is applied repeatedly
- Evaluation of risk acceptability should determine treatment and action

# Risk Categories

| Risk Category | Description |
|---|---|
| **Strategic** | Risks arising from identifying and pursuing a strategy, which is not clearly defined, or is based on outdated or inaccurate data due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change) that fails to support the delivery of strategic commitments, plans or objectives. |
| **Financial** | Risk arising from not managing resources in accordance with requirements and/or constraints (e.g. lack of funding) resulting in failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting. |
| **Operational** | Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes and / or ICT systems resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance with statutory functions and/or poor value for money. |
| **Reputational** | Risks arising from adverse events, ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations. |
| **Compliance / Legal / Governance** | Risks arising from<br>i. Non-compliance with laws and regulations, internal policies or prescribed best practices.<br>ii. Risks arising from a contract and / or a claim being threatened or made (including proceedings issued, a defence to a claim or a counterclaim) or some other legal event occurring<br>iii. Risks arising from ineffective or disproportionate governance structures impacting decision-making and / or performance |
| **People** | Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and / or non-compliance with relevant employment legislation / HR policies resulting in negative impact on performance. |
| **Project Delivery** | Risks that programmes and projects are not aligned with objectives and do not successfully and safely deliver requirements and Intended benefits (innovation, time, budget and quality). |

# Risk Management Cycle

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

# The Fundamentals of Risk Management

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

**1. Establish the context**

- To identify risks effectively, there must be a thorough understanding of organizational business plan objectives, operational functionality, organizational culture .

**2. Risk Assessment**

- **Risk Identification** – is a key responsibility for all Boards, Directors, Heads of Business Areas, Managers and their teams. Risks may be identified from a variety of sources both internal and external to the organisation
- **Risk Analysis** - is a process used to evaluate the risk you have identified and to estimate the level of risk attached to it. The risk is scored by multiplying (Impact x Likelihood) = Risk Score.
  - Inherent Risk Score – The Risk Score in the absence of any control
  - *Residual Risk Score* – The Risk Score after controls have been applied
  - *Target Risk Score* – The Risk Score anticipated when actions are completed, and controls are working effectively. This risk score should be aligned with your organisations risk appetite.
- **Risk Evaluation** – considers the outcome of the risk analysis in order to determine whether or not the calculated level of risk is acceptable. This will be informed by the organisations risk appetite.

# The Fundamentals of Risk Management

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

**3. Risk Treatment**

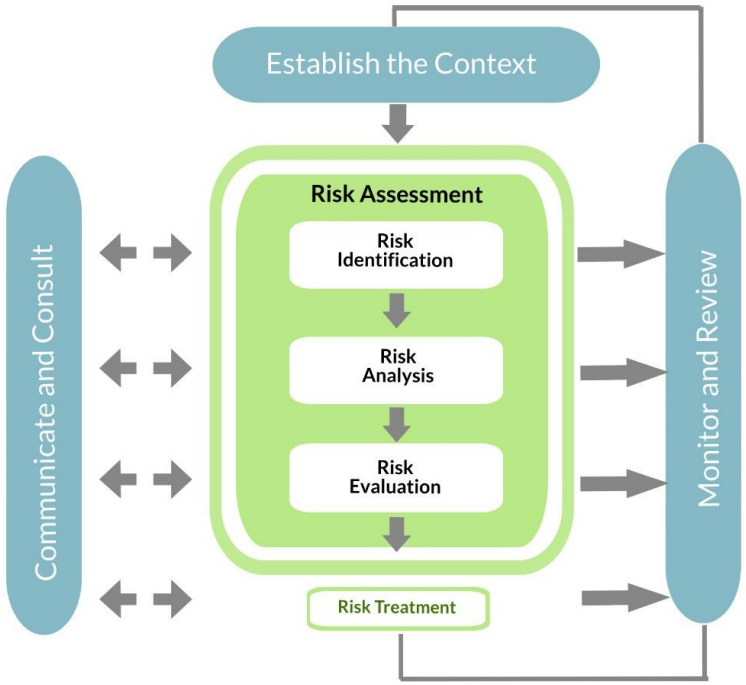
- Refers to the choices available to handle a specific risk. Risks can be controlled depending upon the type of risk response: Treatment, Tolerance, Transfer or Terminate

**4. Controls**

- In terms of risk, is what is done to prevent this risk from occurring what is needed to be done to reduce its likelihood of occurring or minimising its impact if it was to occur

**5. Monitor and Review**

- All risks should be monitored, reviewed, actioned, recorded and reported as appropriate on a regular basis. Reviewing all risks and monitoring of internal control weaknesses, gaps and failures regularly should be a standing agenda item at team and management meetings.



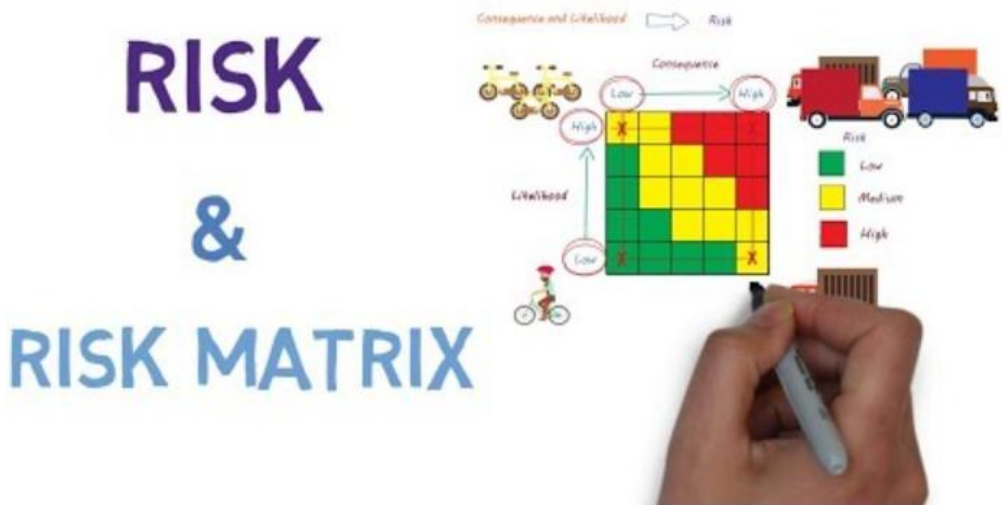

Risk Management Process

EY

# Risk Matrix & Risk Registers

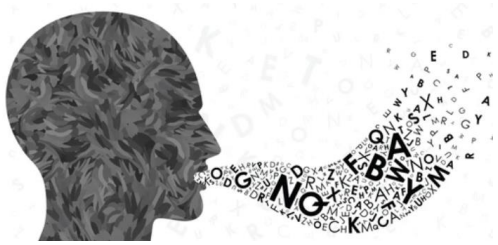
The purpose of risk registers is to capture and maintain information on all the risks relating to the organisation's activities.

Where the level of residual risk is within the risk appetite for that category, the risk is managed by the appropriate management level.




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

# The Language of Risk Management…

- **Worry**… is a form of self-torment, best described as 'what-if' thinking. Anticipates problems and things not going to plan/going awry (loss of control).
- **Concern** …on the other hand, is a calculated consideration and assessment of actual danger and is more fact-based and geared toward problem-solving.
- **Issue** …is an event, condition or situation that has already happened and has impacted or is currently impacting.
- **Hazard** …A hazard is a potential source of harm or adverse effect- e.g. something that can cause harm
- **Risk** …a risk as an *uncertain event* or condition that, if it occurs (based on probability – high/low), can have a positive or a negative effect. Can pose opportunities and threats to the organizations objectives.

# Risk Tolerance & Risk Appetite


**Risk tolerance** is the level of risk that an organization can accept per individual risk, whereas risk appetite is the total risk that the organization can bear in a given risk profile, usually expressed in aggregate.

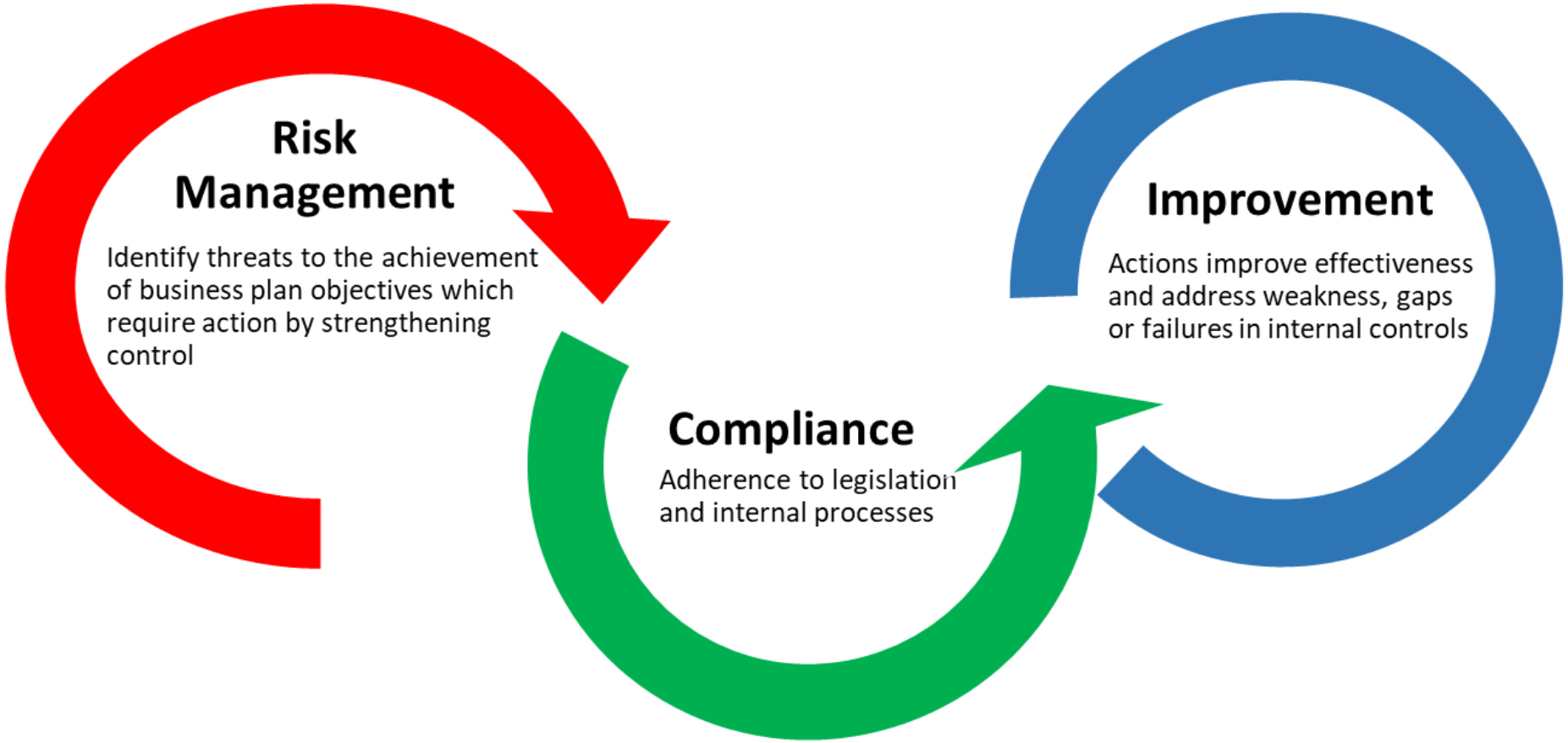
**Risk appetite** can be defined as 'the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives'.

Organisations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time.

Risk appetite and tolerance need to be high on any Board's agenda and is a core consideration of an effective risk management approach.

# Risk, Compliance & Improvement

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte



# The Fundamentals of Risk Management

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

**Code of Practice for the Governance of State Bodies - Risk Management Principles:**

## Requirements of the Board includes:

- The Audit and Risk Committee to give an independent view in relation to risks and risk management systems
- Risk management is a standing item on the Board meeting agenda;
- At least one Board member has risk management experience/expertise
- Appoint a Chief Risk Officer, or empower a suitable management alternative
- Approve the risk management policy, set the State body's risk appetite, and approve the risk management plan and risk register at least annually;
- Review Managements reporting on risk management and note/approve actions as appropriate;
- Request that an external review to assess the effectiveness of the risk management framework on a periodic basis; and
- Confirm in the annual report that the Board has carried out an assessment of the organisation's principal risks

# Internal v External Influences on Corporate Governance & Risk Management

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte


Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

# Internal

- Personality Power
- Knowledge Power
- Sanction Power
- Political Power
- Personality Power
- Interpersonal Power
- Representative Power
- Networking Power
- Societal Power

# External

- Shareholder Perspective
- Prospect of Litigation
- Leglislation & Regulation
- Litigation
- Charismatic Chairman
- Media Pressure
- Influence of External Auditors
- Threat of Takeover
- Risk to Reputation

# Internal v External Risk

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

**Internal Risk**

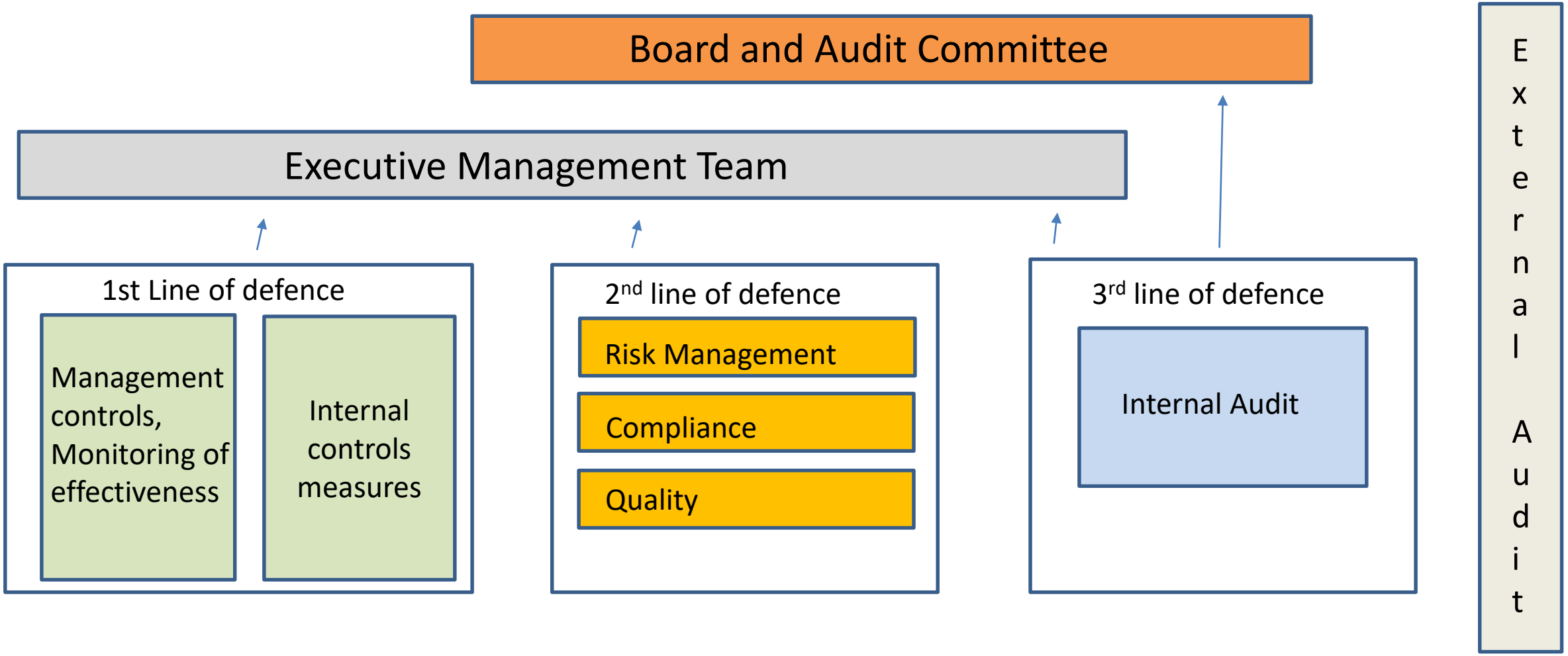
- Staffing & Resource
- Governance & Management
- Legal/Compliance
- IT/ICT
- Stakeholders
- Strategic & Operational Business Planning
- Human Resource Management
- Knowledge & Skills Management
- Change/Process Management

**External Risk**

- Stakeholders - Residents/Families/Public
- Reputational
- Political
- Regulatory
- Economy
- Sector Changes
- Legal Remit
- National Landscape
- Changing Demands/Expectations

# Three lines of defense model helps to clarify risk responsibilities

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte



# Three Lines of Defense Model

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

**1. First line of defense**

**Own and manage** risk and control. In the first line of defense, line management are responsible for identifying and managing risks directly. They own the risk and optimize controls to highlight any inefficiencies and gaps.

**2. Second line of defense**

**Monitor** – risk, control and compliance functions are put in place by management to work alongside the first line to help ensure that risk and control are effectively managed. The second line is essentially a management and/or oversight function that owns many aspects of the management of risk.

**3. Third line of defense**

**Provide independent assurance** to the Board and the Executive Management Team concerning the effectiveness of management of risk and control (internal audit). As such, the third line is an assurance not a management function, which separates it from the second line of defence.

# Risk Culture eats Strategy for Breakfast…

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

An organisation's risk culture determines the way risks are identified, understood, discussed, and acted upon in the organisation.

Culture is about behaviour – what you do, not just what you say.


There is no single accepted definition of what culture or risk culture is and similarly no regulator will attempt to impose cultural standards/norms on any provider – there is no one size fits all.

However it is essential that organisations and their employees have a solid understanding as to the behaviours that are expected of them in their employment.

It needs also to be understood that regulators are looking for organisations to understand what they generally expect to see as indicators of positive culture/risk management culture within the providers that they regulate.

# Risk Culture eats Strategy for Breakfast…

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

A *sound* risk culture consistently supports appropriate risk awareness, behaviours and judgements about risk-taking within a strong risk governance framework.

A sound risk culture bolsters effective risk management, promotes sound risk-taking, and ensures that emerging risks or risk-taking activities beyond the organisations risk appetite are recognised, assessed, escalated and addressed in a timely manner.

A culture of **Risk Ownership & Accountability** must be understood and promoted.

The best approach is likely to be one where the ownership of risk is in the frontline, supplemented by strong oversight and control from the second line and assurance from the third line.

Embedding risk culture involves ingraining the belief that “risk is everyone’s responsibility.”

# Risk and Blame

"High blame" approaches to risk management operate on a win/lose approach to governance and risk.

Positive Risk Management only functions effectively if all incentives to hide information about our errors and mistakes are removed, so that near misses and failures can be fully analysed and discussed in order to prevent major accidents and failures.

# Trust and Risk

A trustworthy organisation is one that operates effectively, acts with due concern for the interests of its stakeholders and conducts itself according to the principles of honesty, integrity and fairness: that is, with high ethical standards.

Trust, honesty and fairness: The key people involved in the application of good governance and risk management must be trustworthy and honest and treat others fairly at all times.

Trust is a cornerstone of successful risk management.

Trust in those who manage and provide services is paramount. It is the factor that often leads to the greatest successes ; but in contrast, breaches of trust almost always lead to the most spectacular failures.


# Current Challenges to Effective Risk Management

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

- We sometimes can think we know it all when it comes to risk…….we don't.
- Risk Management is rhetoric heavy and can be seen as overtly conceptual/technical…..then we need to simplify it.
- Risk is subjective
- Risk can be emotive
- **Risk is a tool…..not a rule**
- Inconsistent application of risk management

- Governance is a balance between performance and conformance BUT effective risk management has to be both
- Risk (and its brother Quality) can often be viewed as sitting in a disconnected space away from the busy operational space – this prevents understanding and is a barrier to 'buy in' and a strong risk culture.

# Conclusion

Ciara McShane

Interim Deputy Chief Inspector

# Key Points to Remember

The board and senior management of an organisation should be developing, implementing and embedding risk culture right across all services creating the right  “tone from the top”.

This ‘tone from the top’ must be consistently reinforced throughout all levels of the organisation.

The Board/Directors, the Executive & Senior management are responsible for reinforcing the ‘tone at the top’, driving a culture of compliance and ethics and ensuring effective implementation of strong corporate governance and risk management in the delivery of safe, high quality care and support to residents.

# Thank You.

Health Information and Quality Authority
An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

George's Court, George's Lane
Smithfield, Dublin 7
D07 E98Y

T: 01 814 7400
W: www.**hiqa.ie**
**E: info@hiqa.ie**