CalQRisk
Manage the effect of uncertainty on objectives

Risk Management Fundamentals for Housing Associations

Trainer: Gerard Joyce

March 24th, 2022

Outline

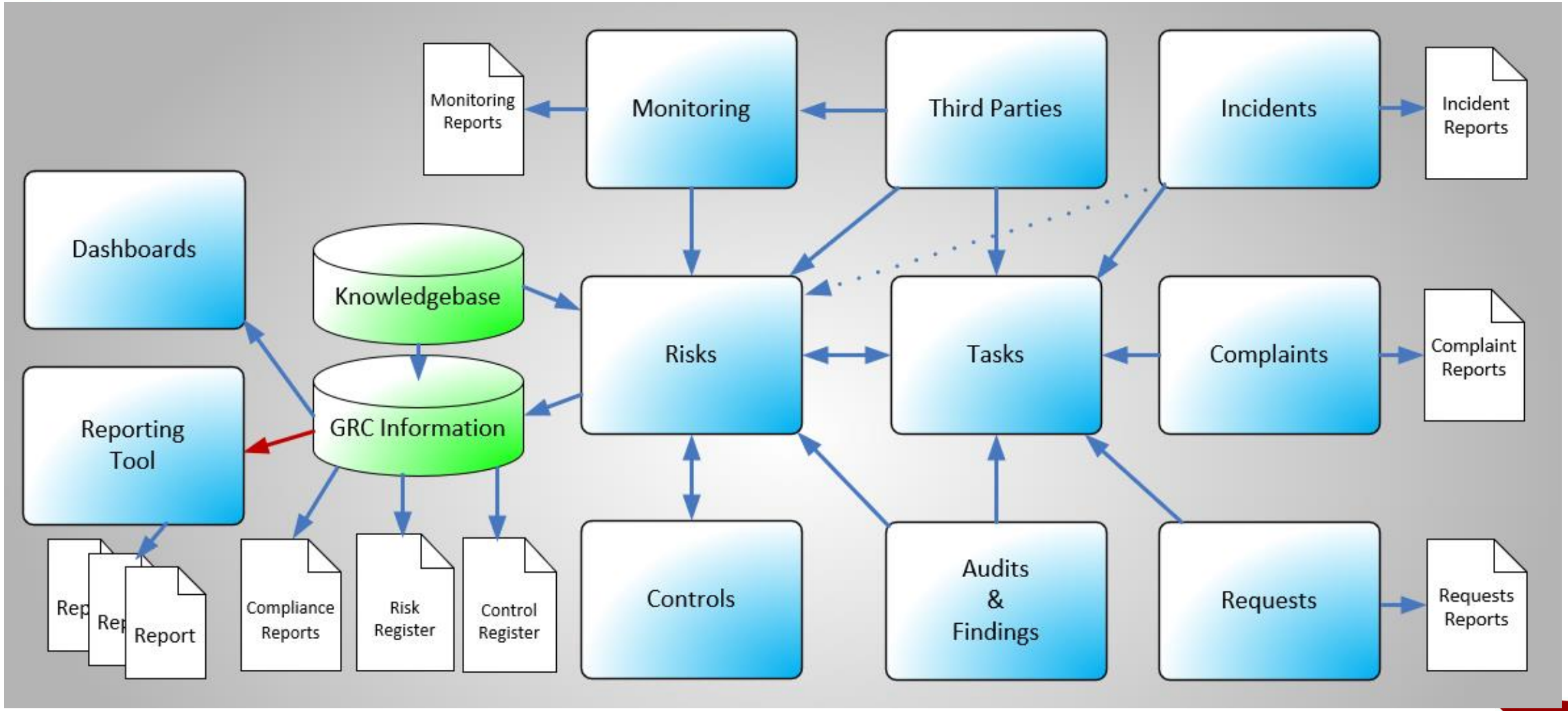
CalQRisk
Manage the effect of uncertainty on objectives

1. Trainer
2. Objectives
3. Why Do Risk Management?
4. What is Risk Management?
5. The Risk Management Framework and Process
6. Risk Criteria / Risk Appetite
7. Roles and Responsibilities

Trainer- Gerard Joyce

- Participated in the development of ISO 31000: International Risk Management Standard.
- Chairman of the Irish Risk Management Mirror Committee
- Co-founder of CalQRisk

CalQRisk Platform



Objectives for this Session

- Know what Risk Management involves
- Be Familiar with the Risk Management Process
- Understand the roles of individuals with respect to risk
- Know what to look for to ensure that risk is being managed effectively

Why Do Risk Management?

CalRisk
Manage the effect of uncertainty on objectives

Because*:*

- Objectives
- Focus
- Forward Looking
- Process Identifies Opportunities
- Better / Informed Decision Making
- Improved Performance
- Effective Governance Demands It

What is Risk Management?

- Coordinated activities to direct and control an organisation with regard to risk (ISO Guide 73)
- the co-ordinated activities designed and operated to manage risk and exercise internal control within an organisation. (Orange Book)

What is Risk?

- The Effect of Uncertainty on Objectives (ISO 31000 / Guide 73)
- Risk is the effect of uncertainty on objectives. Risk is usually expressed in terms of causes, potential events, and their consequences: *(Orange Book)*

Risks are not Events!

Governance and Risk Management

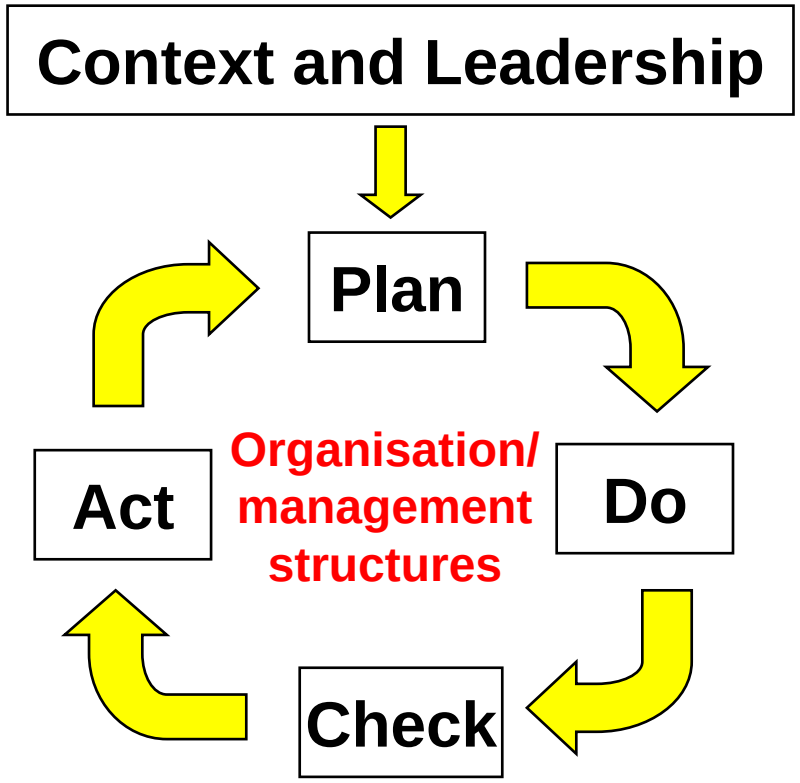
- Corporate Governance
  - to facilitate effective, entrepreneurial and prudent management that can deliver the long-term success of the company (UK Corporate Governance Code)

- Risk Management
  - Looks forward, prevention and mitigation
  - Increasing likelihood of positive outcome
  - Dynamic, responsive to change
  - Aligned with Objectives

Compliance and Risk Management

- Compliance
  - With laws and regulations
  - Documentation of controls
  - Static, controls match regulations
- Risk Management
  - Non-compliance is a source of risk
  - Risk Management process can support compliance efforts

Risk Management System / Framework



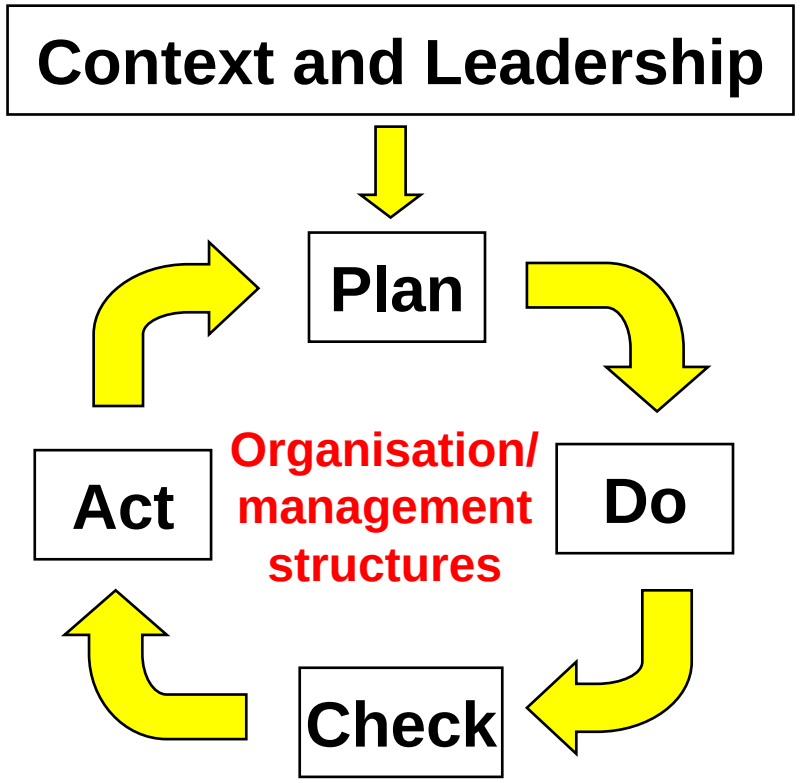
Context

- Objectives
- Scope
- Stakeholders
- Requirements

Leadership

- Policy
- Roles, Responsibilities, Authorities
- Resources

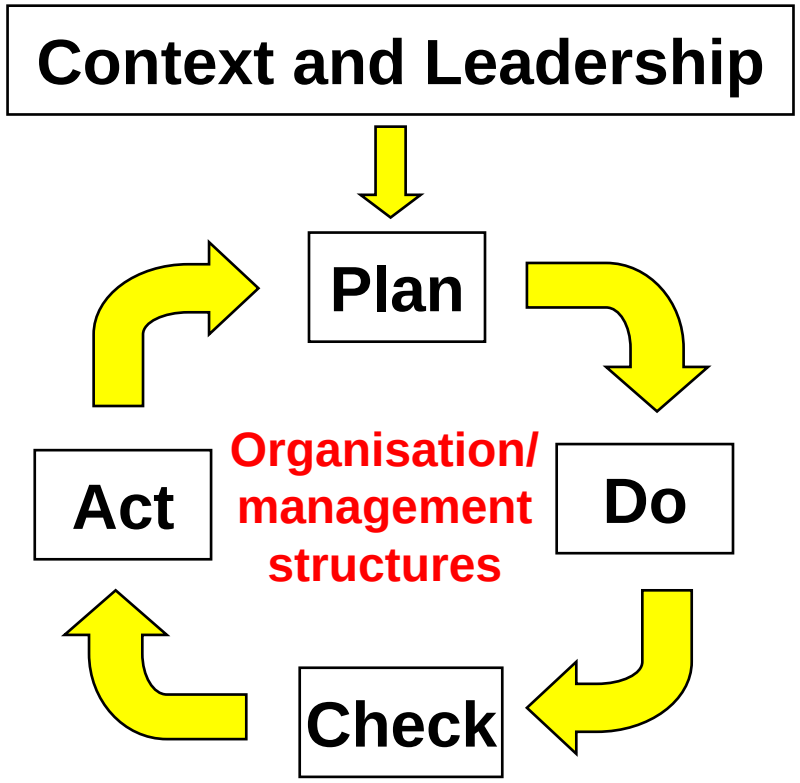
Risk Management System / Framework ctd



Plan

- Identify Threats & Opportunities
- Actions to address T&O
- Integrate into processes
- How to measure effectiveness
- Establish functional objectives
- Roles and Responsibilities
- Processes
- Training requirements
- Communication
- Documentation required
- How performance measured

Risk Management System / Framework ctd



Act
- Address non-conformity
- Identify causes
- Implement corrective and preventive actions
- Record actions taken

Do
- Implement processes
- Record results

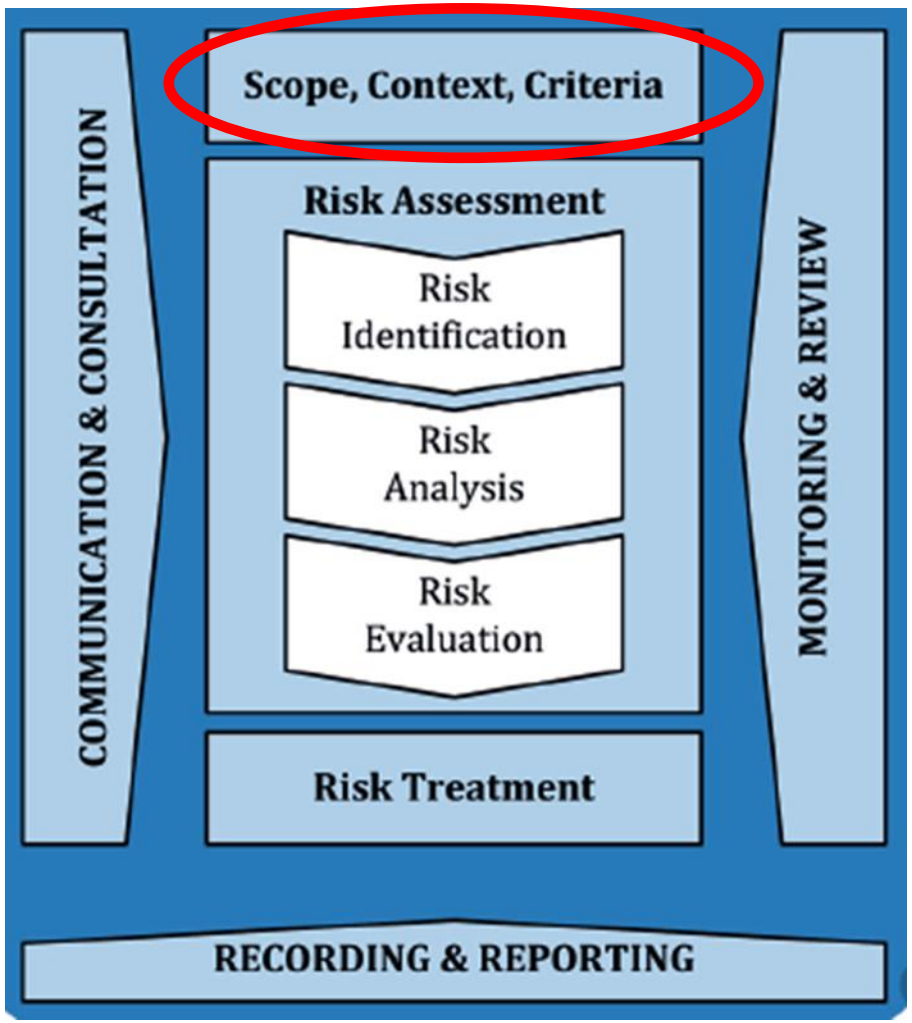
Check
- Monitor operation
- Evaluate performance
- Audit
- Review
- Opportunities for improvement

Risk Management Policy

Contents:

- Scope and Rationale
- Objectives
- Policy Statement
- Risk Appetite / Tolerance / Capacity
- RM Performance (How measured)
- Roles and Responsibilities
- Education and Training

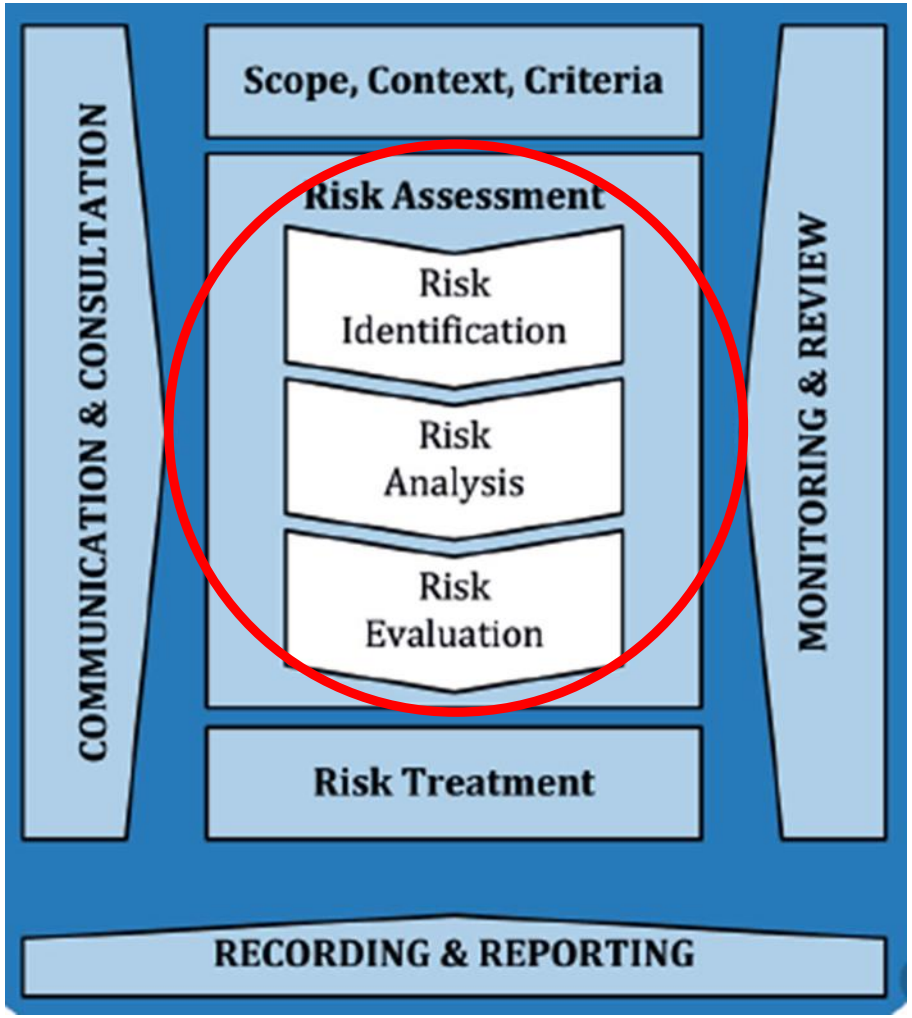
The Risk Management Process



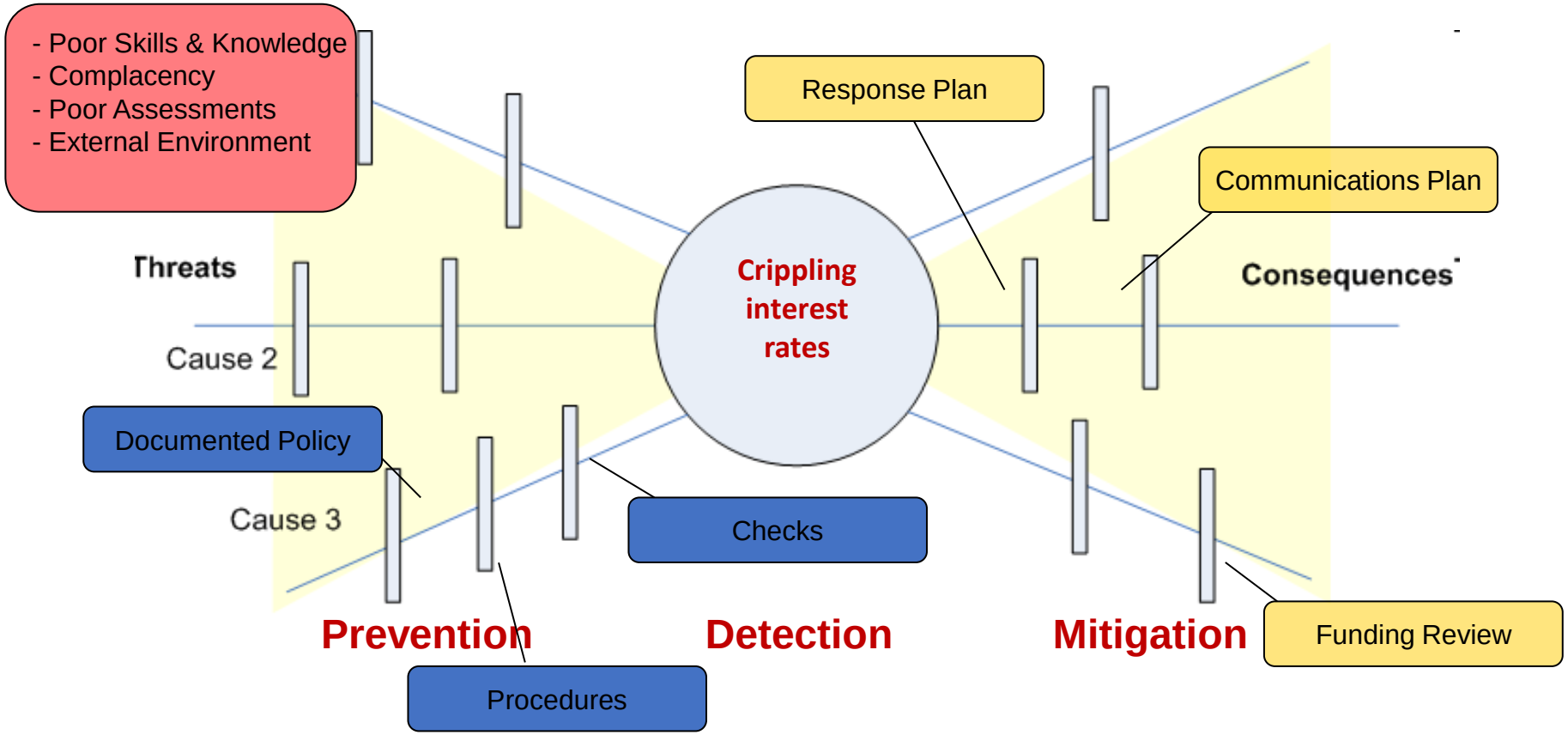
Establishing the Context

- the objectives of the organisation
- the internal and external environment (structure, housing stock, key third parties, standards and legal & regulatory requirements)
- the Risk Criteria used to evaluate the significance of risks
- the Risk Appetite as defined by the Board of Directors
- the stakeholders
- the scope of the risk assessment (Risk Assessment Framework)
- the Key Risk Indicators (KRIs)

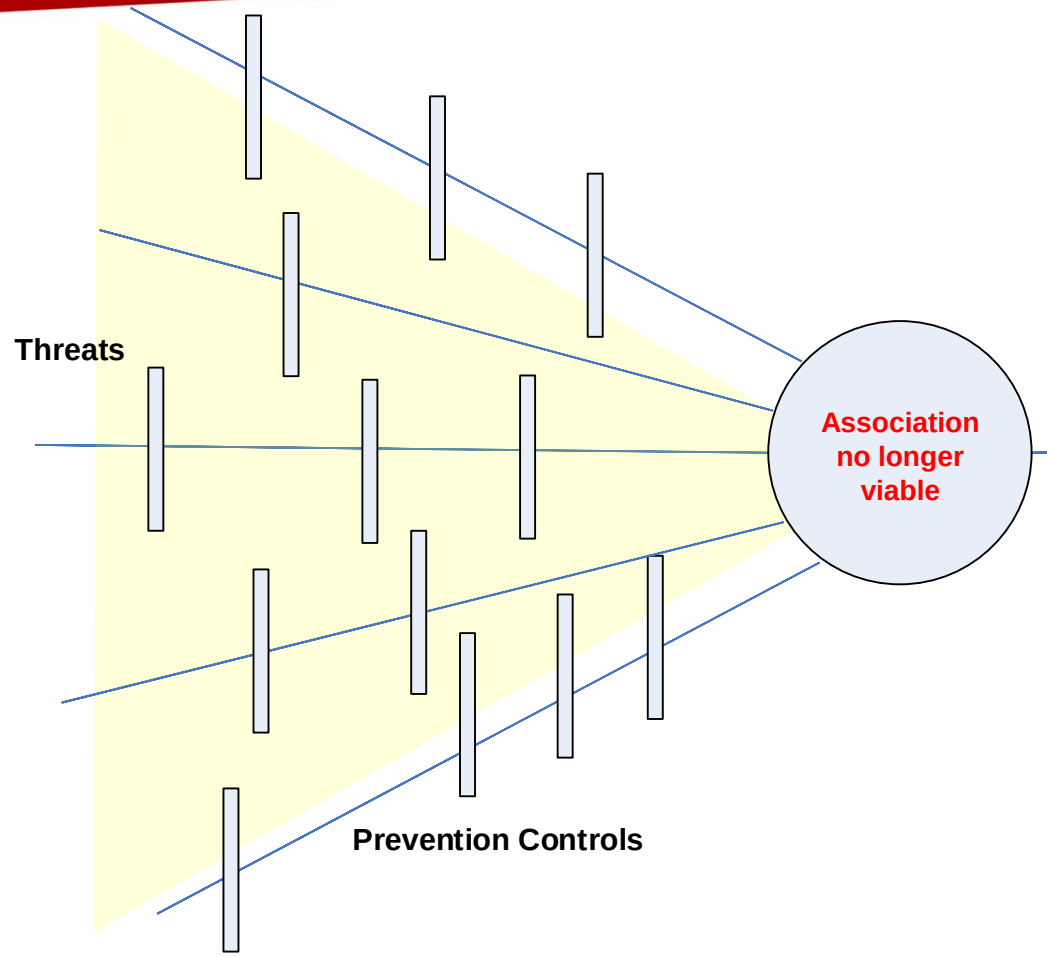
The Risk Management Process



Risk Assessment – Bow-Tie



From Objectives to Risks



Diversify into student accommodation

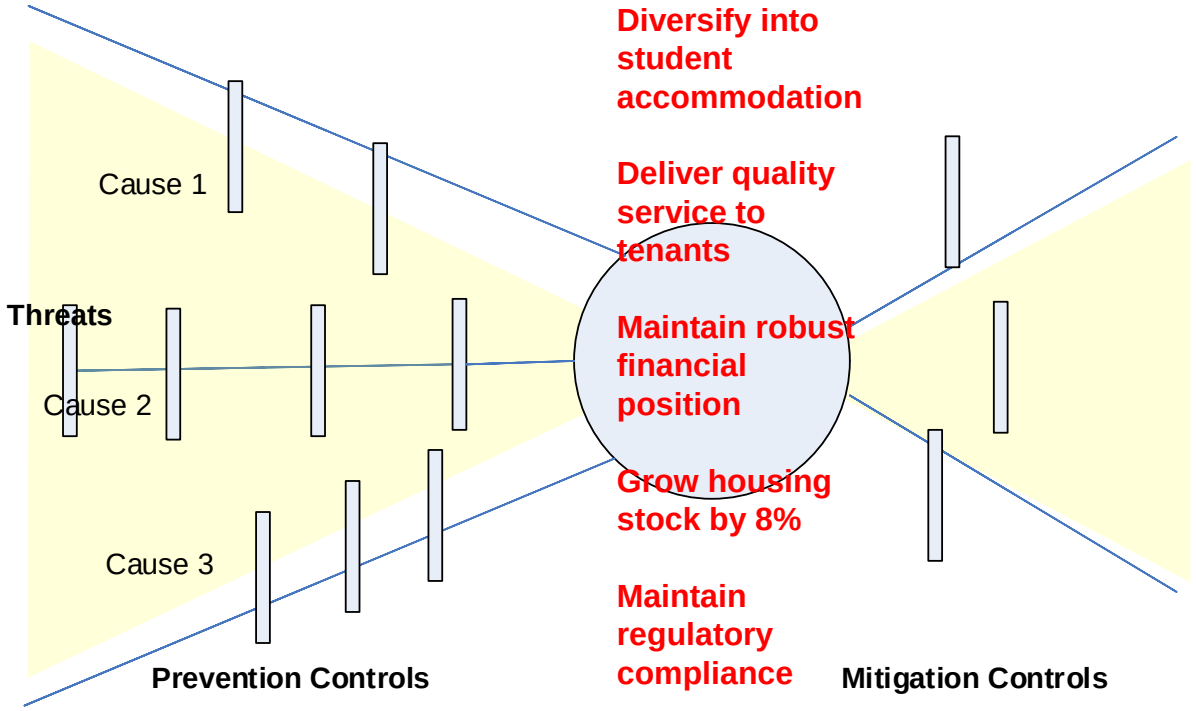
Deliver quality service to tenants

Maintain robust financial position

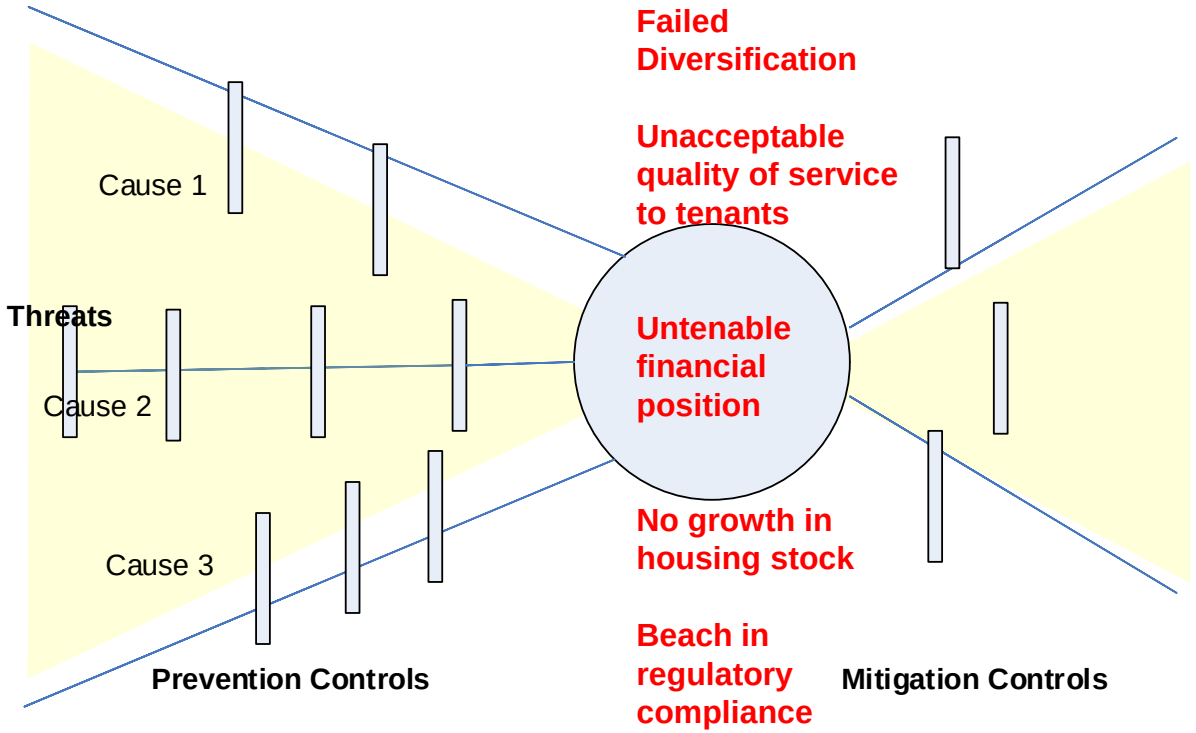
Grow housing stock by 8%

Maintain regulatory compliance

From Objectives to Risks

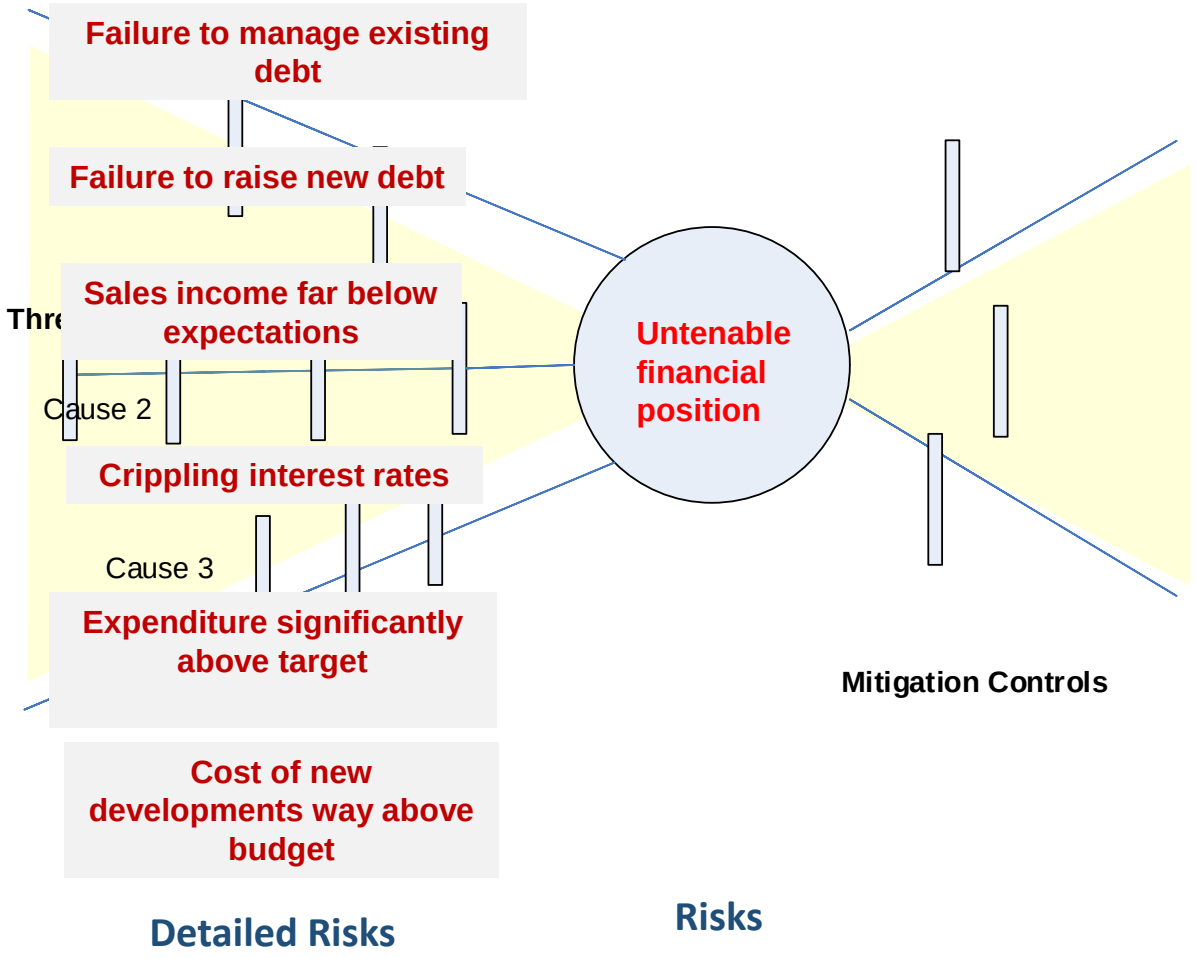


From Objectives to Risks

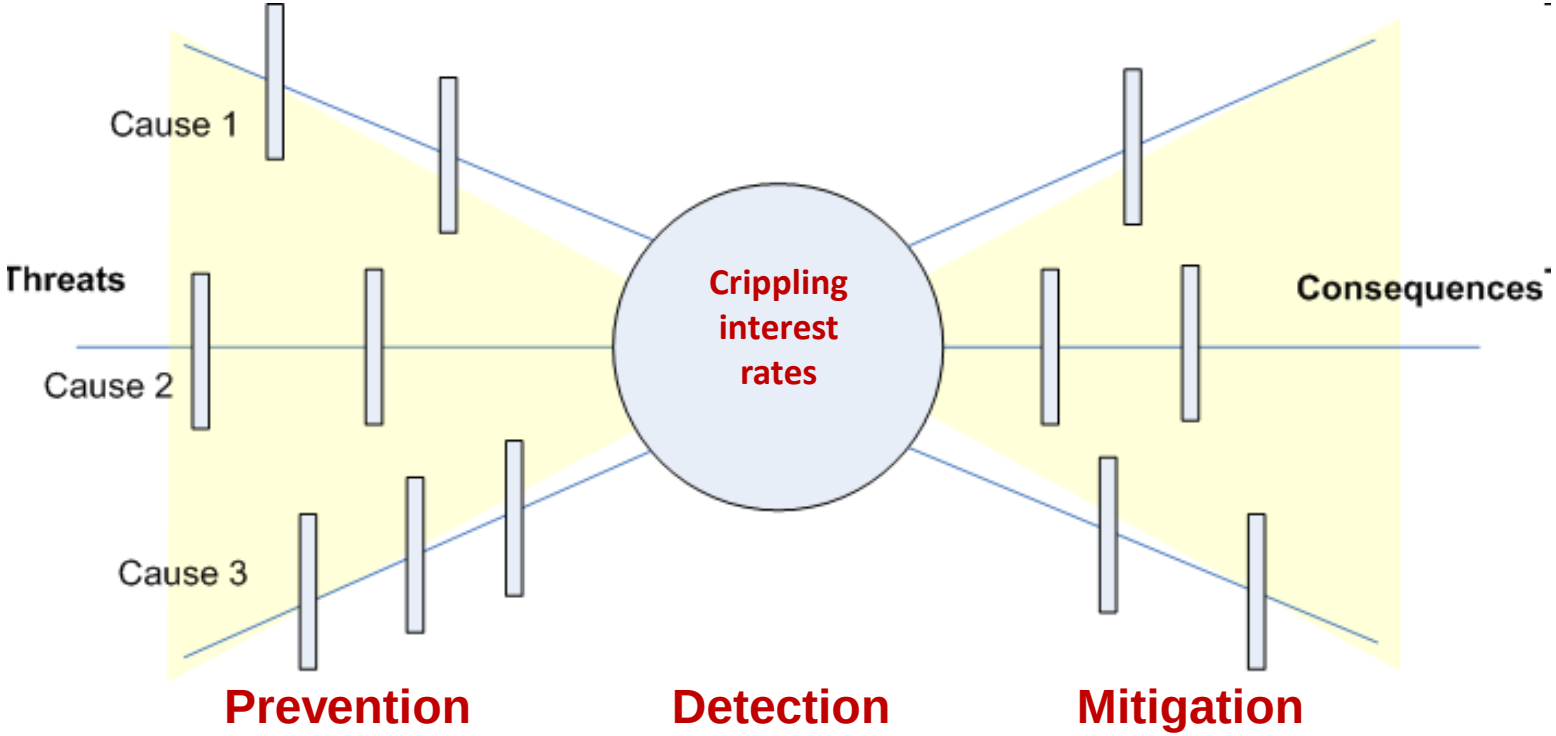


Risks

From Objectives to Risks



Risk Assessment – Bow-Tie



Definitions

Risk Appetite Amount and type of risk that an organization is prepared to pursue, retain or take. (ISO Guide 73)

Risk Criteria Terms of reference against which the significance of a risk is evaluated. (ISO Guide 73)

Inherent Risk Risk Present with No Controls

Residual Risk Risk Remaining after Risk Treatment

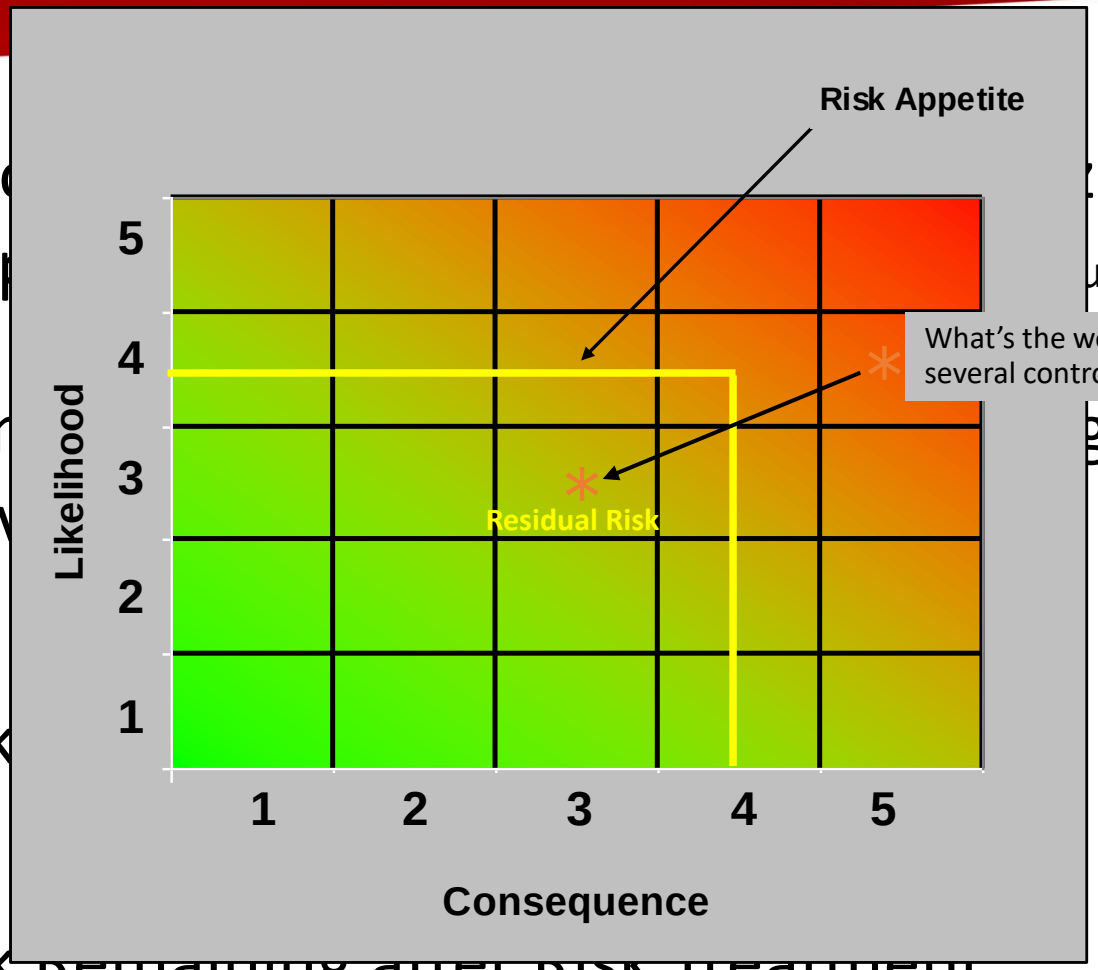
Definitions

Risk Appetite Amo…zation is prep…uide 73)

Risk Criteria Terr…gnificance of a risk is ev…

Inherent Risk Risk…

Residual Risk Risk Remaining after Risk Treatment



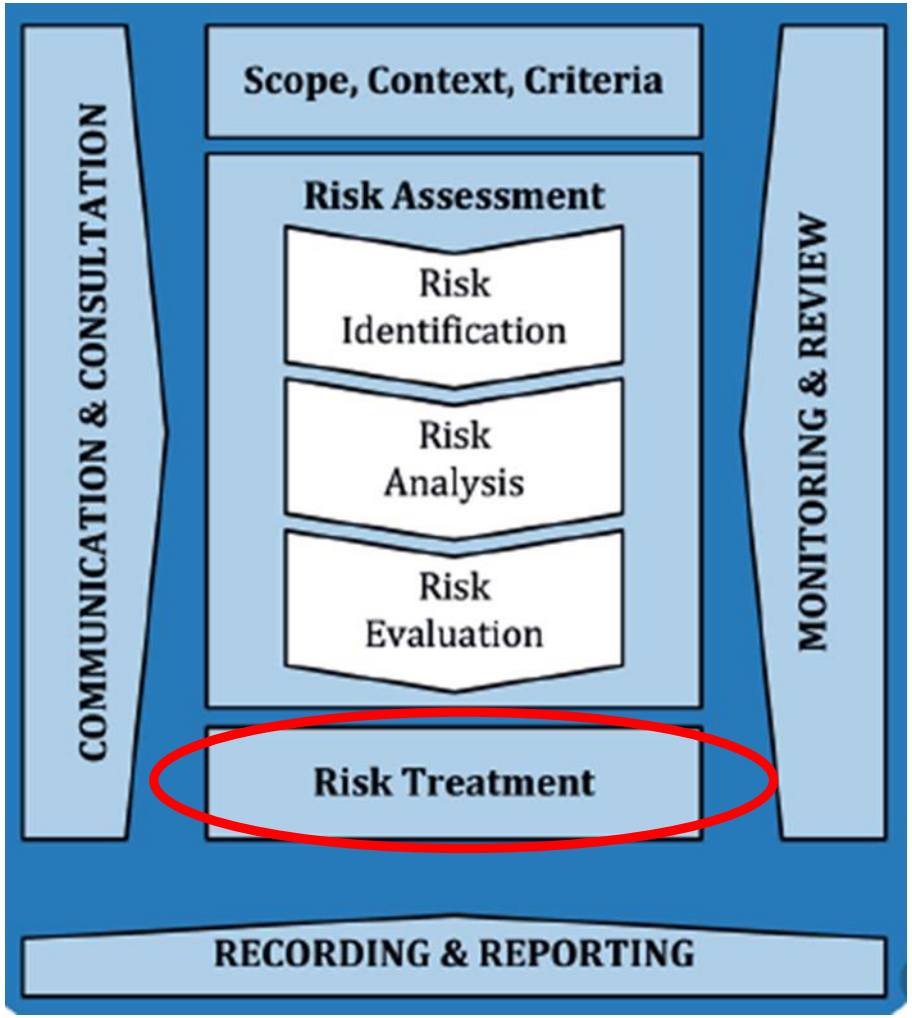
Risk Register

CalQRisk
Manage the effect of uncertainty on objectives

RISK REGISTER

Housing Association											23/03/2022
				Pre-Control				Post-Control			
Risk Nr	Category	Risk Description	Risk Owner	L	C	R	Controls	L	C	R	Additional Mitigation Options
83693	Data Protection-DP Governance	Inappropriate processing of personal data	Chris Hanlon	4	4	16	'- All purposes for which personal data is collected and processed have been communicated to and understood by all relevant personnel. '- All of the purposes for which the organisation is collecting the data are disclosed to the data subject in clear and plain language at the time of collection.	2.9	3.3	9.6	- There must be a documented policy in place that governs the purpose(s) for which the organisation collects and processes personal data. '- There should be one competent individual with responsibility for all of the organisation's data processing management activities. '- There should be an up-to-date, documented privacy notice / statement in place for each dataset and / or group of data subjects as necessary. '- There must be stringent procedures in place to ensure that personal information is never used for any purpose other than those disclosed to the data subject.
83703	Technology-Governance	Failure to detect and respond to a cybersecurity breach in a timely manner	Chris Hanlon	4	4	16	- There is a documented policy in place that addresses continuous monitoring and detection of unauthorised activity on the network. '- We keep up-to-date on known vulnerabilities for all IT related systems and services that we depend upon. '- Tools are deployed in the network that monitor the behaviour of attached systems and can detect unusual deviations from the expected. '- Malware detection software is configured to perform frequent scans of all files. '- Contact has been established with legal counsel who can provide appropriate assistance in the event of a data breach. '- Contact has been established with an IT forensics expert who can provide appropriate assistance in the event of a data breach.	2.6	2.7	6.9	'- The organisation should keep a record of all of the locations where sensitive information is stored. '- Tools should be put in place on the network that can detect signatures of known cyber attacks and patterns. '- Intrusion detection tools that can quickly detect and signal the presence of malicious activity on the network should be acquired and deployed.
82625	Legal & Regulatory-Charities Regulation	Non-compliance with NHF Code of Governance Principle 1: Mission and Values	Fiona Kiely	4	4	16	'- The board sets and actively drives the organisation's social purpose, mission and values and through these embed resident focus, inclusion, integrity, and openness and accountability within the organisation. '- The board leads the organisation in pursuit of achieving its social purpose. '- The needs and safety of the organisation's current and future residents and other customers are placed at the heart of the board's decision-making. '- The organisation has policies, frameworks and	2.2	2.3	5.2	'- The board must set the organisation's mission and values. '- The board must have access to insight into the views and needs of the organisation's residents and other customers (including insight into their concerns and complaints). '- The board must use insight into the views and needs of the organisation's residents and other customers to inform its decisions where appropriate. '- Where there is a material conflict of interest, any

Risk Treatment



Brakes Allow a Car to go Fast

Risk Treatment

Risk Control (Minimise Exposure)

- Terminate (Avoid)
- Treat (Reduce)
  - Pre-loss (Prevention)
  - Post-loss (Mitigation)

Risk Financing (Fund Losses)

- Tolerate (Retain)
- Transfer
  - Insurance
  - Contract

Risk Control

Reduce - Pre-loss – Prevention / Detection

- Policies, Procedures
- Education & Training
- Design
- Communication, Signage, etc
- Housekeeping, Supervision
- Maintenance, Review
- Target Hardening
- Alarms, Cameras, KRIs

Risk Control

Reduce - Post-loss – Mitigation

- Incident Response Procedure
- Education & Training
- Communications Plan

Risk Control - Example

Technology Loss Prevention / Mitigation

- Resiliency
- Redundancy
- Backup and Recovery Plan
- Anti-virus
- Firewall
- Access Control
- Change Control
- Acceptable Usage Policy

Risk Appetite

Amount and type of risk that an organization is prepared to pursue, retain or take. (ISO Guide 73)

- Set by the Board of Directors
- For all who make decisions in the organisation
- For those stakeholders who need assurance

Risk Appetite

- ISO31000: Amount and type of risk an organisation is willing to pursue or retain or take.
- FSB: The aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan.
- COSO: Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so.
- NACD: "Every Board should be certain that…the risk appetite implicit in the company's business model, strategy and execution is appropriate.
- UK CG code The board is responsible for determining the nature and extent of the principal risks it is willing to take in achieving its strategic objectives.

Risk Appetite – The What

- Desirable risks
- Undesirable risks
- Unavoidable risks
- Linkage to Strategic Objectives
- Limits

Risk Appetite – The How

CalQRisk
Manage the effect of uncertainty on objectives

We only allow Finance department staff to use the company credit card

Statements

- Start with each risk category or objective
- For each Objective clarify Primacy and Flexibility
- Desirable / Undesirable risks
- State what you will tolerate / not-tolerate

We will cancel any events or activities that we cannot deliver in compliance with our safeguarding obligations

Any employee / volunteer working with minors must be police vetted

Any expenditure greater than €5,000 will require Board approval

We will apply full public procurement compliance to all suppliers/third party providers

Limits

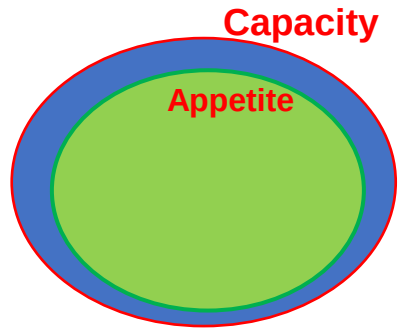
- Disaggregation of overall appetite
- Constraints
- Probably expressed in many policies already

Meeting our legal and regulatory obligations will take priority over other business objectives.

Our core systems will have a minimum uptime of 99.5% during operating hours (7 x 12). (Implies max 25 min downtime in any one week)

If you have zero-tolerance of non-compliance with legal obligations: Say it!

Risk Appetite – The How



Risk Capacity

is the maximum amount of risk which the organisation is technically able to assume before breaching constraints determined by capital, liquidity, borrowing capacity, regulations, reputation and operational environment.

Risk Management Capability

the ability to manage risk exposures within desired risk limits. (Understanding, measurement, skills & knowledge, controls and oversight, culture..)

Risk Criteria

Terms of reference against which the significance of a risk is evaluated. (ISO Guide 73)

- Defined by the Risk Officer
- Approved by the Board of Directors
- Must be consistent with the Risk Appetite
- Use “What Matters” to the organisation as the reference

Risk Criteria

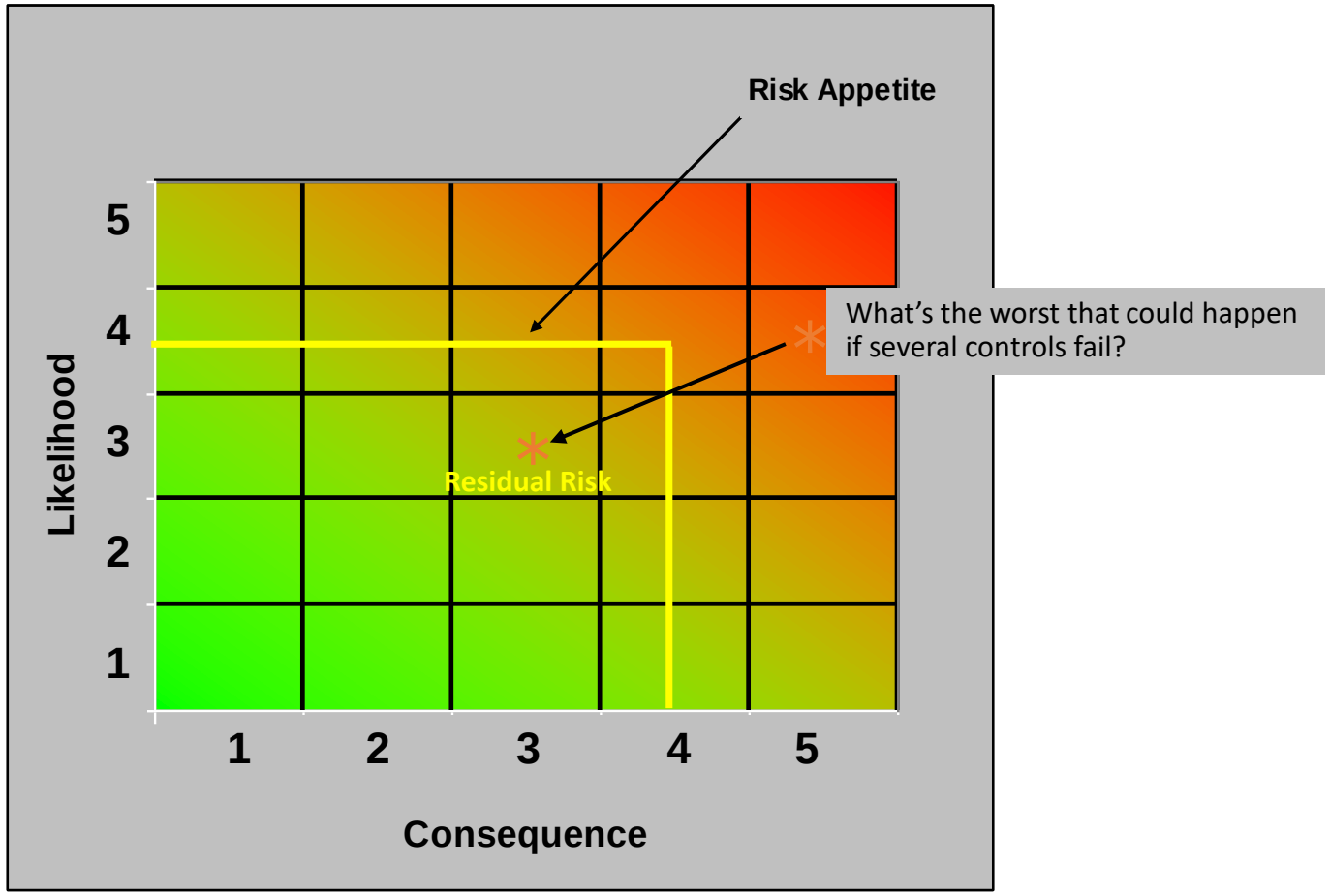
CalRisk
Manage the effect of uncertainty on objectives

Risk Criteria

CONSEQUENCES					
Criteria	5 Substantial	4 Significant	3 Moderate	2 Minor	1 Negligible
Profit	Loss > €3M	Loss €1M and €3M	Break Even	Profit of 5%	Profit > 5%
Customers / Service Users	Departure of 3 key customers	Departure of one key customer	Departure of 3 medium customers	Departure of 1 medium customer	Departure of 1 minor customer
Reputation	Sustained International Multi-Media adverse publicity	Once-off International Multi-Media adverse publicity	Once-off national Multi-Media adverse publicity	Negative comment in national press	< 3 substantiated complaints in a quarter
Approvals / Compliance	3 significant non-compliance issues found by CB	1 significant non-compliance issue found by CB	1 moderate non-compliance issue found by CB	Non-compliance found by internal audit and rectified quickly	Temporary non-compliance
People	Departure of 6 key individuals in one quarter	Departure of 3 key individuals in one year	Departure of 1 key individual	Departure of a line manager	Delay in recruiting for a key position

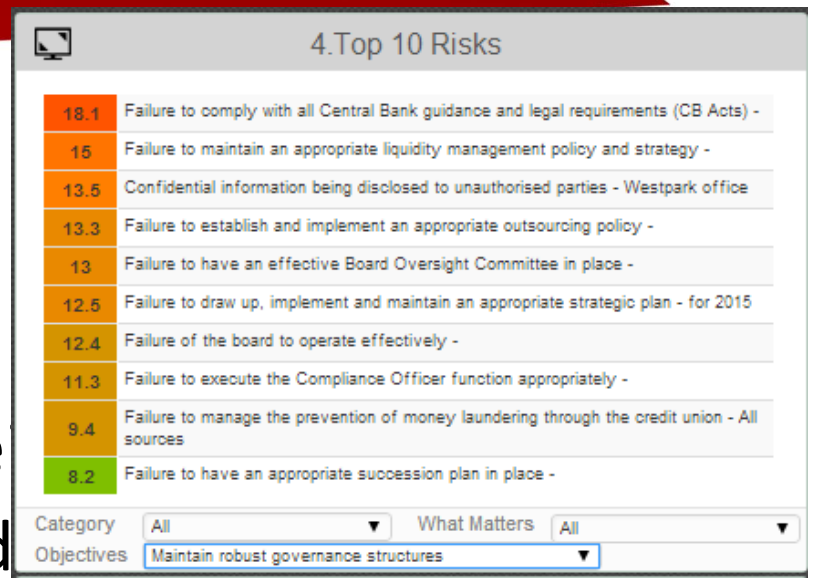
LIKELIHOOD				
5 Very High	4 High	3 Medium	2 Low	1 Very Low
Once per quarter or more frequent	Once per year	Once in 3 years	Once in 10 years	Once in 30 years or less frequent

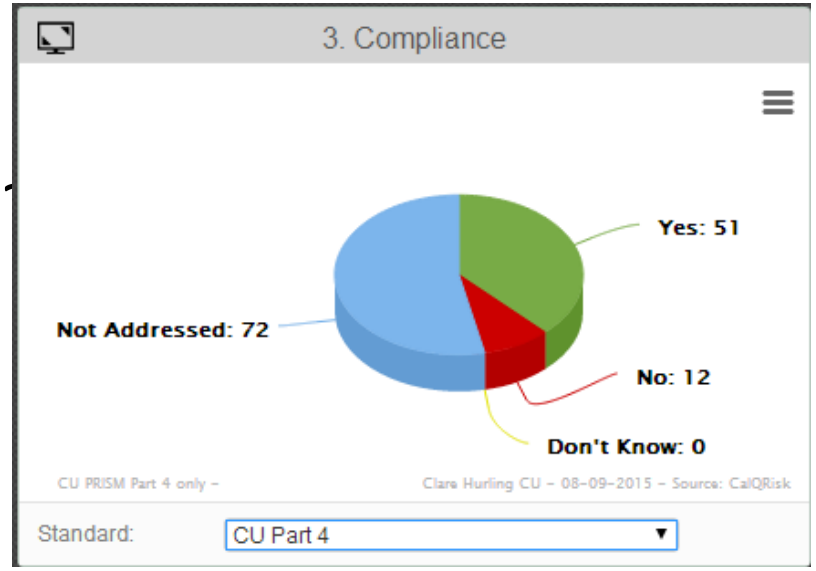
Risk Criteria



Reporting – What Boards Should Know

- What is the overall risk profile?
  - What are the Top 10 risks
- What is threatening the Objectives
- Are existing controls working / effective
- Have there been any near misses / incid
- Where are the gaps?
  - Confirmation of the overall compliance position
- What is being done to address the gaps
- Key Risk Indicators





Key Risk Indicators

Exposure Indicators

Changes in the nature of the business environment

- Investment return, unemployment rate, outstanding debt (Overdue), Key ratios (strengthening / declining)

Stress Indicators

Significant rise in the user of resources (people / material)

- Sick days, accidents, system downtime, complaints, loans made, helpdesk calls

Causal Indicators

Drivers of some key risks to the business

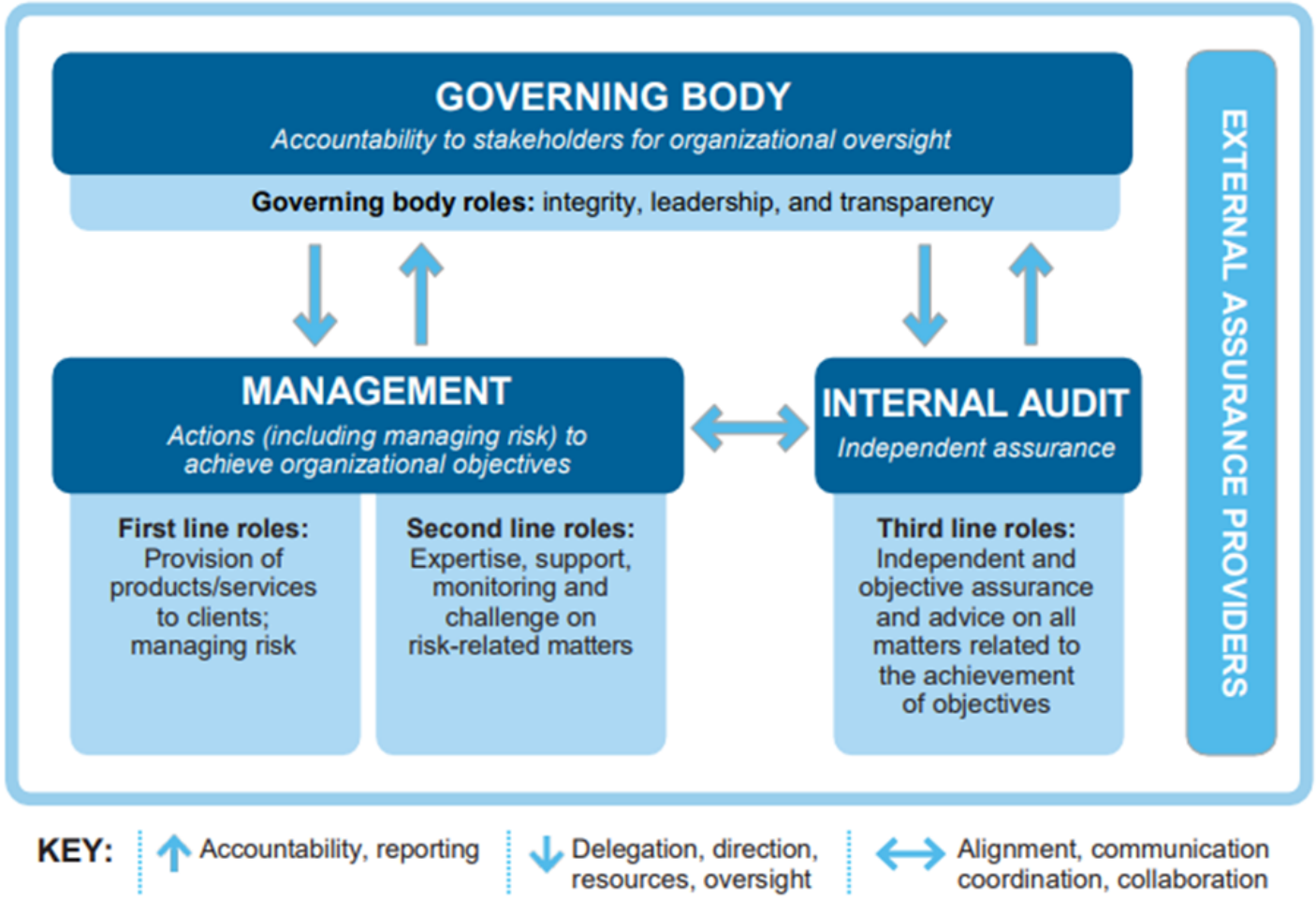
- Number of tenants, training completed, equipment age

Failure Indicators

Poor performance and failing controls

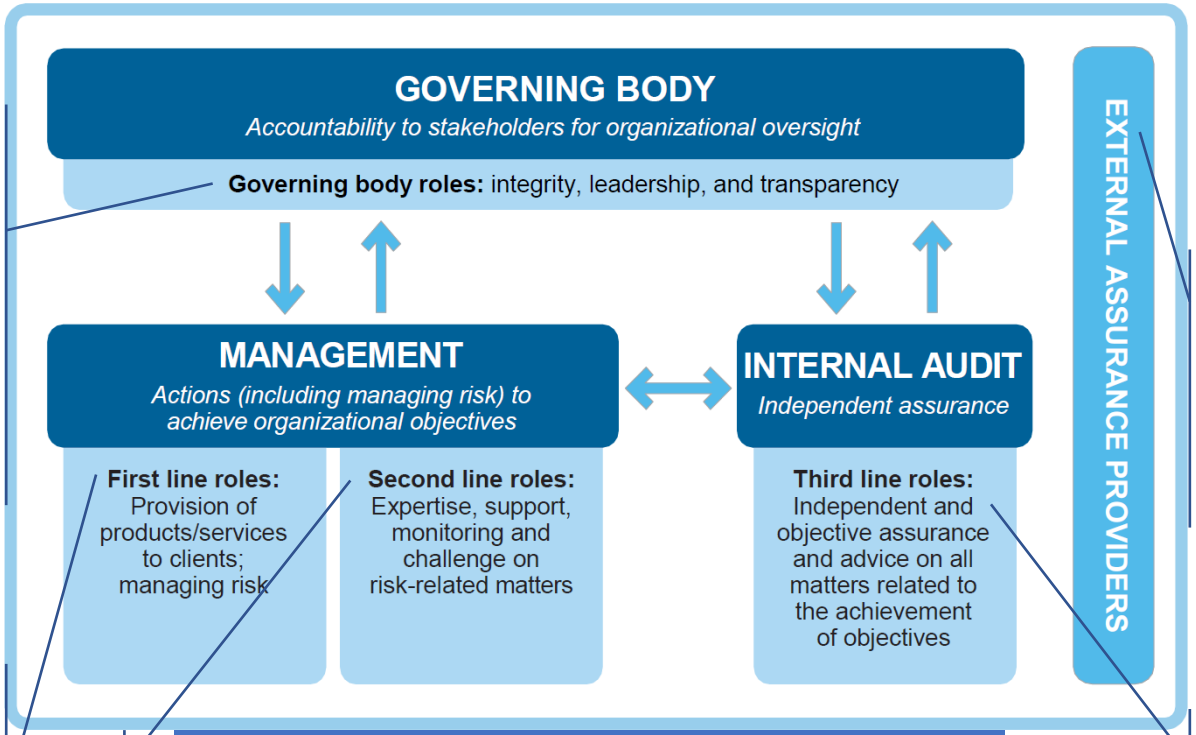
- Loan book, complaints, audit findings, data breaches, policy breaches, fraud

Three Lines Model



Who does what

4 Oversight
Define Objectives
Establish Structures
Provide Resources
Set Risk Appetite
Establishes Internal Audit



5 Expertise
e.g. Pen Testing
Satisfy reg requirements
Independence

1 The Doers
The Risk Owners
Identify and control risks
Implement Processes
Report on plans and outcomes
Ensure compliance

2 CRO, CCO
Expertise
Advise First Line
Challenge (respectfully)
Ensure Consistent Implementation
Monitoring
Reporting Adequacy and Effectiveness

3 Quality Control
Independent
Adequacy and Effectiveness
Advise

Questions & Answers

Thank You

gjoyce@linkresq.ie

Some Useful Sources of Information

IFAC	www.ifac.org
COSO	www.coso.org
RIMS	www.rims.org
CPA	www.cpacanada.ca
IRM	www.theirm.org