

Risk Management Framework & Action Plan

Version 7.0
October 2024



Process for Policy Review and Update

- Revision History

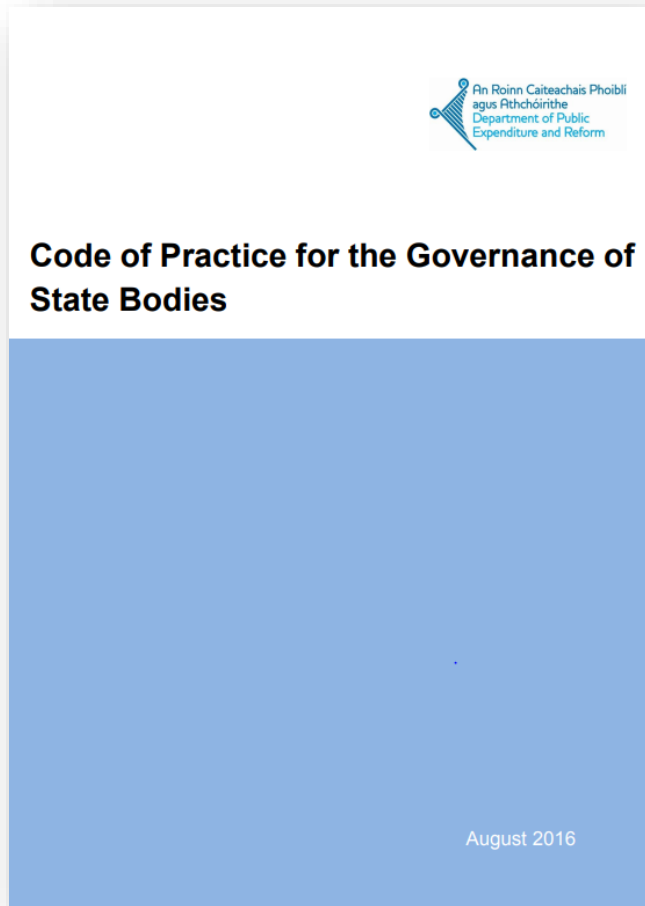
Version	Date	Description	Prepared	Reviewed
1.0	15/12/2017	For Board Approval	Noel Beecher	Board approved
2.0	26/04/2019	For ARC & Board Approval	Noel Beecher	Approved by ARC & Board
3.0	7/05/2020	For ARC Approval	Noel Beecher	ARC approved
3.1	15/05/2020	For Board Approval	Noel Beecher	Board approved
4.0	07/05/2021	For ARC Approval	Noel Beecher	ARC approved
4.0	21/05/2021	For Board Approval	Noel Beecher	Board approved
5.0	09/09/2022	For ARC Approval	Noel Beecher	ARC approved
5.0	16/09/2022	For Board Approval	Noel Beecher	Board approved
6.0	08/09/2023	For ARC Approval	Noel Beecher	ARC approved
6.0	15/09/2023	For Board Approval	Noel Beecher	Board approved
7.0	25/10/2024	For ARC Approval	Noel Beecher	ARC approved
7.0	15/11/2024	For Board Approval	Gerard Cuddihy	Board approved

- Next Review Date: October 2025

- Approvals

Position		Name	Date
Corporate Risk Manager	Annual Review	Gerard McBrien	10/09/2024
Chief Risk Officer & Head of Governance	Annual Review	Noel Beecher	10/10/2024
ARC	Annual Review	ARC	25/10/2024
Board	Annual Review	Board	15/11/2024

Code of Practice for the Governance of State Bodies

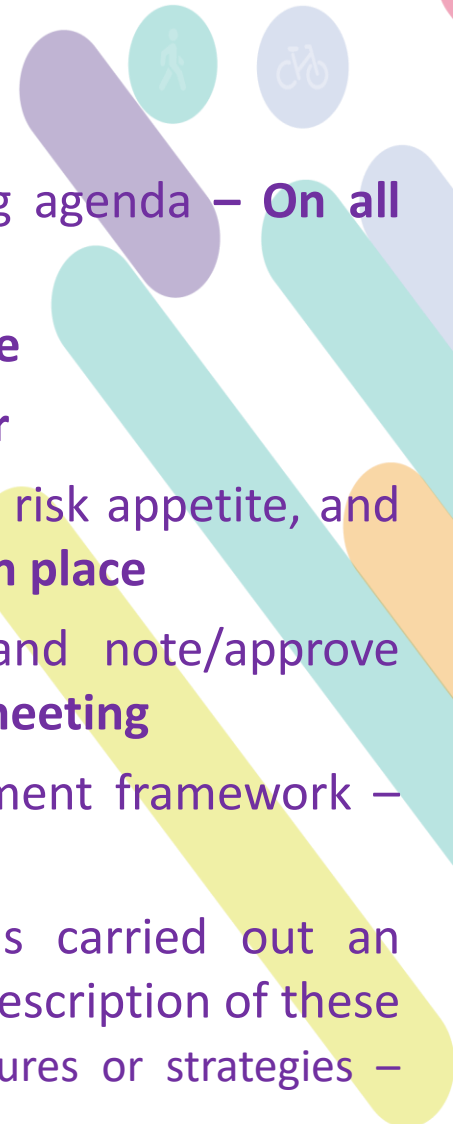


The Code

- Documents issued by Department of Public Expenditure and Reform
- Effective from the 1st of September 2016
- Greater emphasis on Risk Management
- Resulted in new disclosures in the Annual Report and Financial Statements
- Placed emphasis on all internal controls not just financial controls

2016 Code Obligations

- Audit and Risk Committee - **In place since 2016**
- Risk management a standing item on the Board meeting agenda – **On all Board Agenda's**
- Risk management experience/ expertise on Board – **In place**
- Chief Risk Officer to be put in place – **In place Noel Beecher**
- Approve the risk management policy, set the State body's risk appetite, and approve the risk management plan and risk registers – **All in place**
- Review management reporting on risk management and note/approve actions as appropriate – **Reviewed at every Board & ARC meeting**
- Require external review of effectiveness of risk management framework – **Completed in Q4 2023 by IPA**
- Confirmation in the annual report that the Board has carried out an assessment of the State body's principal risks, including a description of these risks, where appropriate, and associated mitigation measures or strategies – **Confirmed annually at the February Board meeting**



Code of Practice

The code states that the Board's oversight of risk management should include:

Consider establishing a Risk Committee or including it in the charter of the Audit Committee

(Done)

Approving the Risk Management Policy, set the State body's risk appetite, approve the risk management business plan and corporate & strategic risk register at least annually

(Done, on-going annual review)

Include risk management expertise in the competencies of at least one director, or obtain expert advice externally.

(Done)

Reviewing management reporting on risk management and note/approve actions as appropriate

(Done, on-going review)

Appointing a Chief Risk Officer or empower a suitable management alternative, and provide for a direct reporting line to the Board

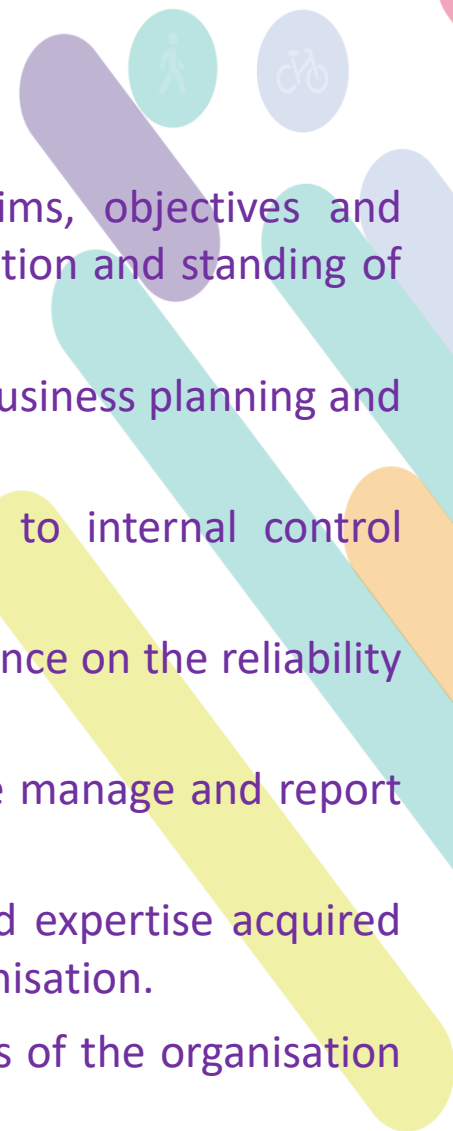
(Done)

Requiring external review of effectiveness of risk management framework on a periodic basis

(Done, on-going annual review)

Risk Management Principles

1. All risk management activity will be aligned to corporate aims, objectives and Authority priorities, and aims to protect and enhance the reputation and standing of the Authority.
2. Risk analysis will form part of the Authority's strategic planning, business planning and investment/project appraisal procedures.
3. Risk Management will be founded on a risk-based approach to internal control embedded in day-to-day operations.
4. The approach will be to inform and direct the work to gain assurance on the reliability of the Authority's systems.
5. Managers and staff will have a responsibility to identify, evaluate manage and report on risks.
6. The NTA will foster a culture of best practice, lessons learnt and expertise acquired from risk management activities for the benefit of the entire organisation.
7. Risk management policy will be applied to all operational aspects of the organisation both external and internal.



Risk Management Framework

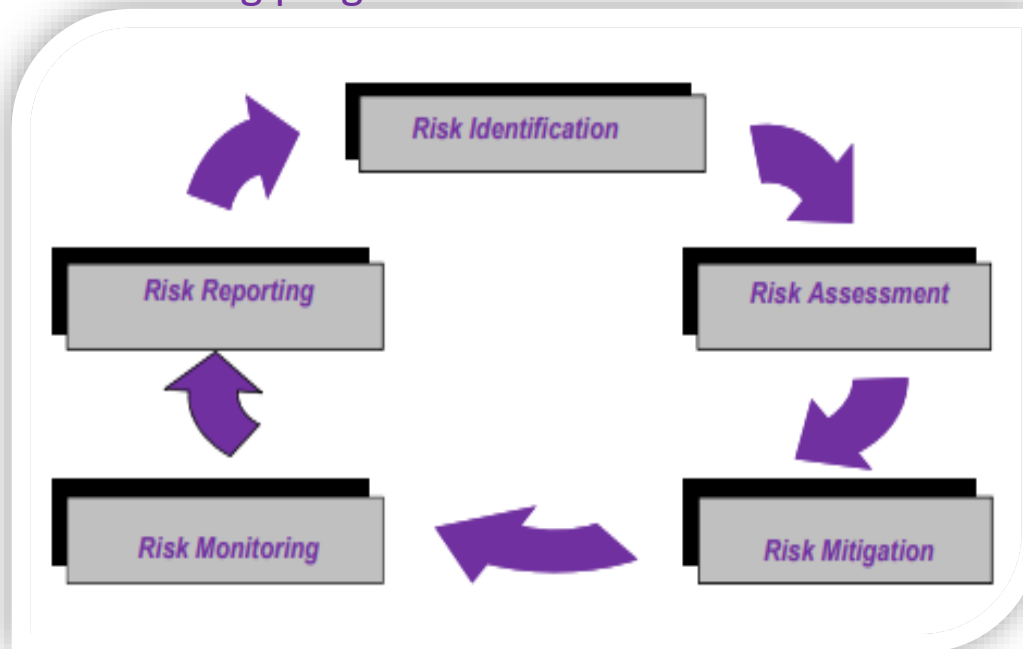
The table sets out the components of the Authority's Risk Management framework



- The Board approves the risk management framework and monitor its effectiveness.
- The Board reviews material risk incidents and note or approve management's actions, as appropriate.
- The Audit and Risk Committee mandate includes risk management.
- Management have various responsibilities however they ensure that Risk Management is embedded in the Authority.
- The Chief Risk Officer (CRO) is responsible for advising the Board on risk management strategy and has developed appropriate policies, procedures, and systems.
- The CRO provides preparations on risk registers and provides assistance to Heads of Departments and staff by providing advice and support.

Risk Management System

- Risk is uncertainty of outcome, whether positive opportunity or negative threat of actions and events. It is the combination of likelihood and impact, including perceived importance.
- Risk Management is all the processes involved in identifying, assessing, and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.



Risk Management System

Dealing with Risk

The 5 T's

Transfer
Outsource to specialists and/or increase insurance cover

Treat
Reduce by improving processes and controls or introduce new controls

Tolerate
In order to avoid the cost of trying to reduce risk or in anticipation of expected benefit through more risk

Take
The risk is accepted as it is seen as an opportunity in line with agreed risk tolerances and risk appetite.

Terminate
Activities that are the source of the risk are terminated

Risk Management System

Risk Matrix

Risk Matrix

		6	12	18	24	30
Likelihood	VH ≥80%	5	10	15	20	25
	H 60%-80%	4	8	12	16	20
	M 40%-60%	3	6	9	12	15
	L 20%-40%	2	4	6	8	10
	VL ≤20%	1	2	3	4	5
		VL	L	M	H	VH
Impact (Financial, Reputation)						

VH - Very High, H - High, M - Medium, L - Low, VL - Very Low

Risk Reporting Scale:

0 - 3 = Green 4 - 9 = Yellow 10 - 17 = Amber 18 - 23 = Red 24+ Black

- Risk mapping is a simple and useful method for assessing risks identified. It involves plotting risks on a matrix or map against relevant criteria.
- Likelihood scoring is based on the expertise, knowledge, and experience of the individuals scoring the likelihood from 1 indicating that there is a remote possibility of it occurring and 5 indicating that it is almost certain to occur. In assessing likelihood, it is important to consider the nature of the risk. The likelihood of a particular risk materialising depends upon the effectiveness of existing controls.
- To determine the impact each risk area should be assigned descriptors over 5 levels ranging from negligible or insignificant to substantial or catastrophic.
- Risk Urgency is covered in the next slide.
- The risk score is determined by taking the likelihood by the impact by the risk urgency i.e. Likelihood of High (4) by Impact of Very High (5) by risk urgency of Immediate (1.2) which is a risk score of 24

Black: Critical - Issues that require immediate attention of management.

Red: Serious - Issues that require constant attention of management.

Amber: High - Issues that need frequent review.

Yellow: Medium - Issues that need to be reviewed from time to time

Green: Low - Issues that need to be reviewed from time to time.

Risk Urgency

The risk urgency assessment weighting is a multiplier of the risk rating based on a review to determine the timing of actions that need to happen determined by the timeframe of the risk occurring. There are different factors to consider to effectively carry out risk urgency assessments as follows:

- **Timeframe of risk:** when could the risk occur;
- **Time available:** to mitigate a risk it may only be useful if it is implemented within a certain timeframe;
- **Warning signs of risk:** the warning signs of risks are also called risk triggers. This can help identify if a certain risk requires urgent responses; or
- **Risk rating:** this is the numeric rating based on the impact and likelihood of risk. Higher rated risks may occur sooner.

Once the urgency of a particular risk is determined it shall be categorised based on the timeframe of the risk occurrence from immediate within 1 month to long term greater than 36 months. The risk rating based on the impact and likelihood is multiplied by the time weighting factor, rounding up to the nearest whole value to give the risk severity score for residual risk only.

Timeframe	Time period in months	Time weighting factor
Immediate	within 1 month	1.2
Short Term	1 month to 12 months	1
Medium Term	13 months to 36 months	0.7
Long Term	greater than 36 months	0.5

Risk Appetite

Risk Appetite Matrix

		M	C	O	H	H
Likelihood	VH ≥80%	M	C	C	O	H
	H 60%-80%	M	M	C	C	O
	M 40%-60%	A	M	M	C	C
	L 20%-40%	A	M	M	M	C
	VL ≤20%	A	A	A	M	M
		VL	L	M	H	VH
Impact (Financial, Reputation)						

- The amount of risk that the Authority is prepared to accept, tolerate, or be exposed to at any point in time.
- The overarching risk strategy is to manage all risks that would prevent the achievement of the vision and strategic objectives while accepting that risk cannot be totally eliminated.
- When completing a risk assessment risk appetite should be used as a guide to the amount of risk the Authority is willing to accept in achieving the expected outcome.
- Risk appetites are based on the selected primary risk sub-category a risk owner selects when they are assessing a risk.

Black: Hungry - The Authority is eager to be innovative and to choose options that have high risks and rewards.

Red: Open - The Authority is open to risks while considering all the potential options.

Amber: Cautious - The Authority is willing to select options that are safe and have a low degree of risk.

Yellow: Minimal - The Authority prefers to select options that are ultra-safe and have a low degree of risks.

Green: Averse - The Authority is averse to take risks. Avoidance is a key decision, but recognises that the complete elimination of this risk is outside of its control

Risk Management Report.....

Risk Report

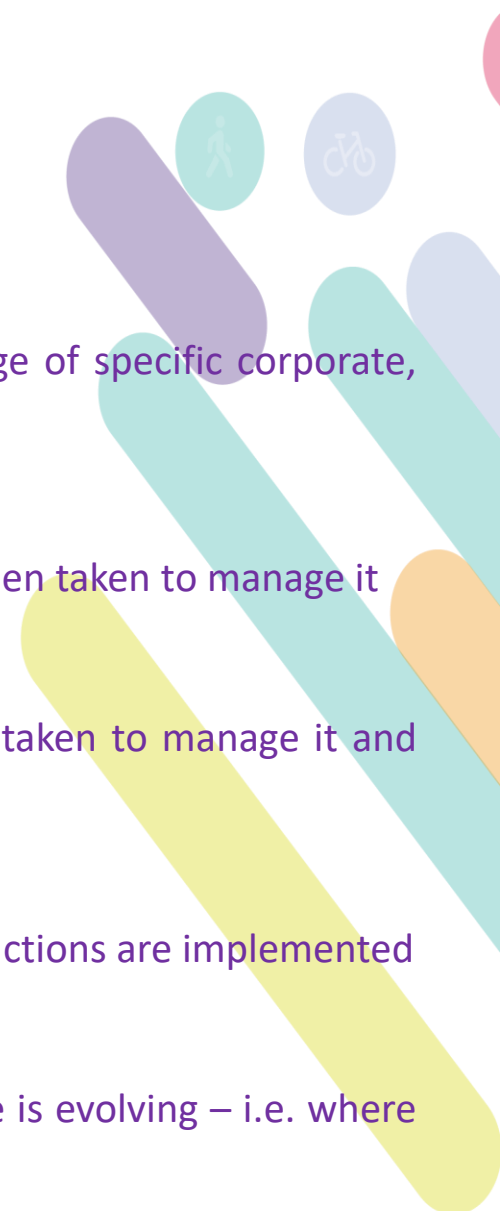
- Significant risks
- Risk Events
- Deviations in tolerances
- Trends
- New risks
- Emerging risks
- Horizon scanning
- High Impact, low likelihood risks



Risk Management System

Risk Reporting

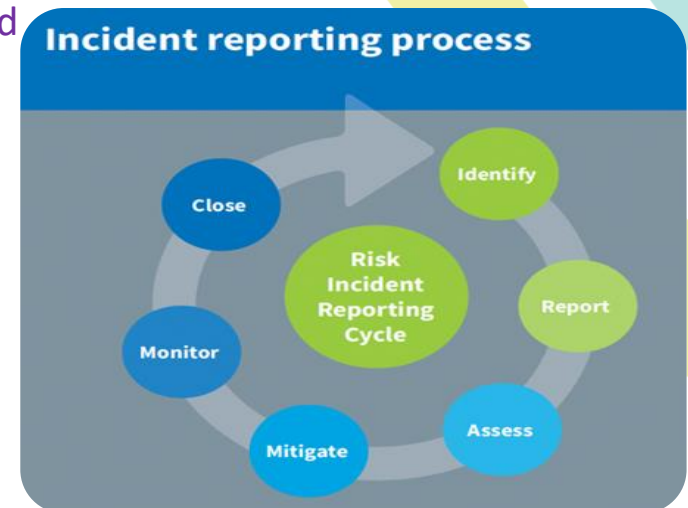
- **Risk Register**
The documented and prioritised overall assessment of the range of specific corporate, unit and section risks faced by the Authority
- **Inherent Risk**
The exposure arising from a specific risk before any action has been taken to manage it
- **Residual Risk**
The exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective
- **Target Risk**
Risk that an activity would pose with controls in place and after actions are implemented
- **Risk Trend**
This is a qualitative analysis which indicates how the risk climate is evolving – i.e. where it is improving, stable or deteriorating



Risk Management System

Risk Incidents & Near misses.

- An **incident or risk events** includes any errors, process failures, etc. which has impacted on the delivery of NTA services.
- A **near-miss** includes any errors, process failures, etc. which could have impacted on the delivery of NTA services.
- Any incident, suspected or confirmed, should be reported at the earliest opportunity.
- The incident reporting form, available on Transportal should be emailed directly to the relevant Departmental Head and the Chief Risk Officer at ARC@nationaltransport.ie.
- The Incident & Near-Miss Report should be completed as soon as possible following the occurrence of any incident or near miss that has been rated as 3 moderate or higher.
- The above process is to be followed when an incident is identified, that is not covered by any other Authority policies, namely, Health & Safety, Data Protection Breaches, Fraud and Protected Disclosures as these types of breaches shall be dealt with as set out in their own policy.
- The following process will be followed for all risk incidents and near misses:
 - ✓ Risk Incident Assessment and Investigation
 - ✓ Risk Incident Mitigation and Monitoring
 - ✓ Risk Incident Closure
 - ✓ **Reporting** - A near-misses and incident log will be a standing item on all Audit & Risk Committee agendas.



Risk Management System

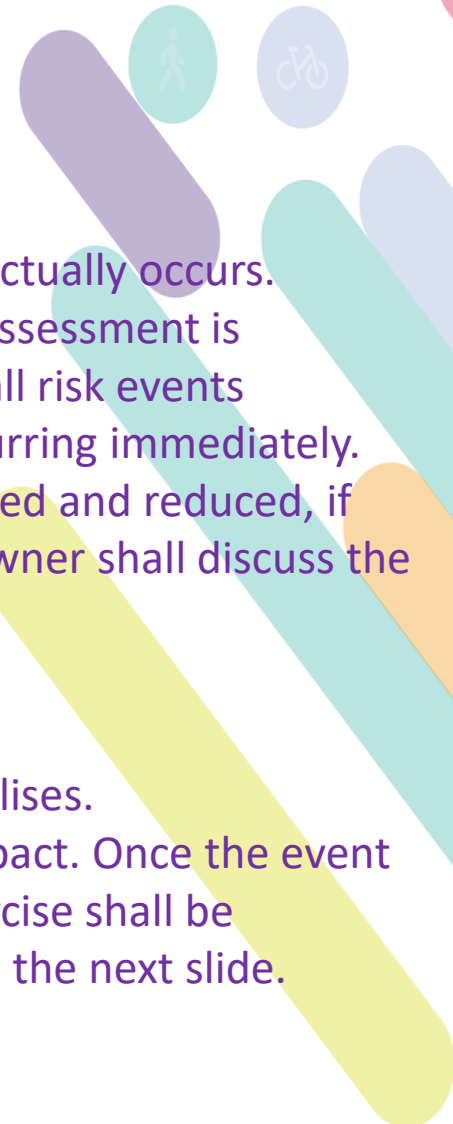
Risk Events

Risk Materialisation

- Materialisation occurs when the event that was thought possible actually occurs.
 - When a risk materialises, the probability element of the risk assessment is removed as the consequences predicted have occurred. Not all risk events materialising may result in the consequence occurring or occurring immediately. This may still provide scope for the consequence to be managed and reduced, if the risk that materialised is identified immediately. The risk owner shall discuss the materialised risk with their manager and the CRO.

Risk Crystallisation

- Crystallisation occurs when the consequence from the risk materialises.
 - Once a risk crystallises the focus shall be on managing the impact. Once the event has been fully managed and concluded a lessons learned exercise shall be completed. The steps when a risk event happens is covered in the next slide.



Risk Management System

Risk Events cont.

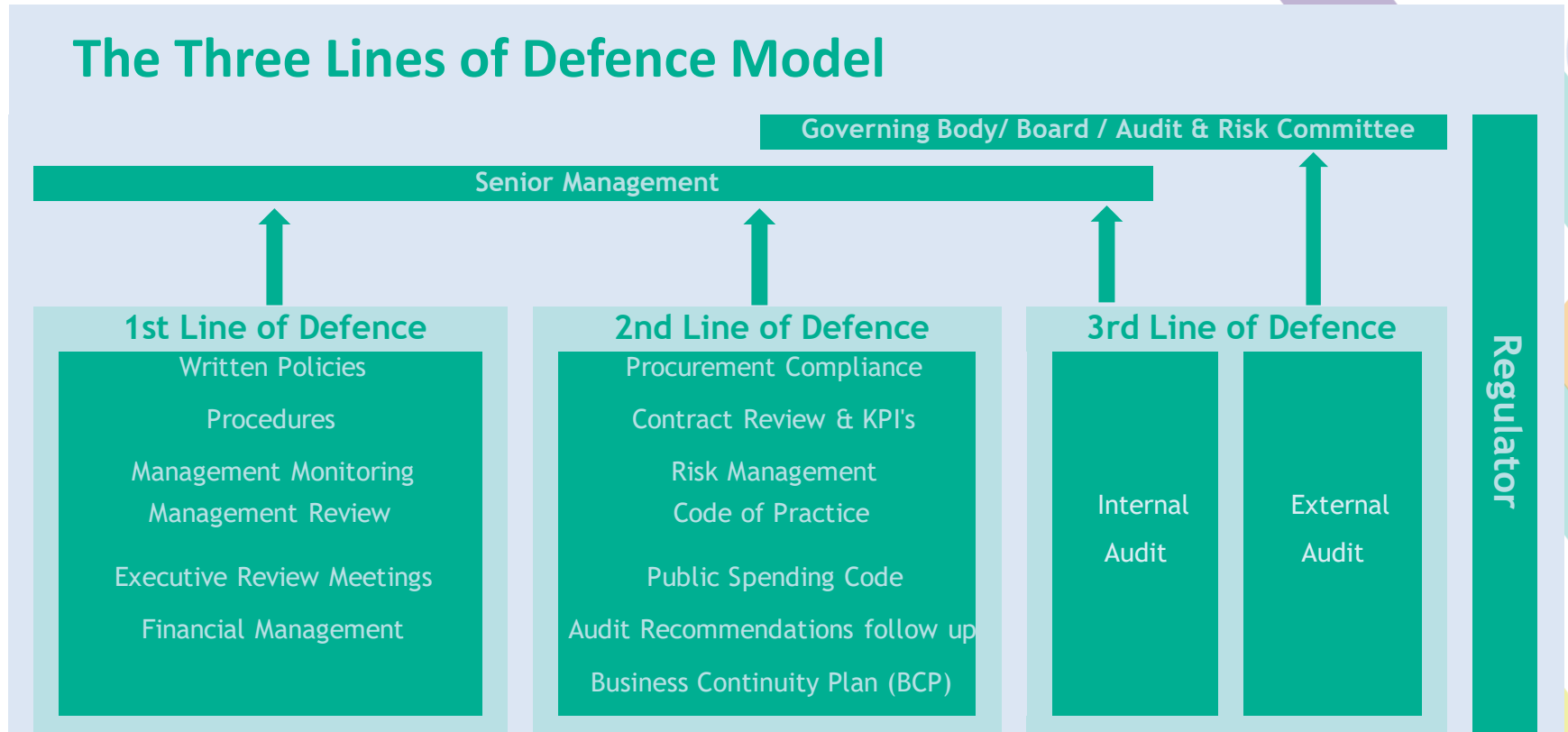
Risk Crystallisation

- There needs to be predetermined criteria or questions that form the basis of the lessons learned exercise. These questions shall identify deficiencies that caused a materialisation of the risk and any deficiencies identified shall be addressed as a matter of priority.
- Specifically, at a minimum, the following shall be considered:
 - How and why the incident occurred;
 - The identified vulnerabilities;
 - The impact on the delivery of business services;
 - Whether the risk controls, decisions and recovery processes and communications were appropriate; and
 - The speed of recovery and whether the impact tolerances are adequate.
- The lessons learned exercise shall give details of the risk and define effective remediation measures applied to redress any deficiencies. The relevant internal communication of the lessons learned exercise will promote an effective culture of learning and continuous improvement in the Authority. Depending on the significance of the event the lessons learned report may be shared with the ARC and Board.



3 Lines of Defence Model

- Assurance Map



Process in place

Processes includes the following are in place;

- Risk on Agenda of all Board and ARC meetings
- Corporate risk register reported to each meeting of the Board and ARC
- Risk Owners identified as Directors / Heads of Business and Functions
- Operational risk register to be updated for all Business Units two times a year with CRO
- Heads of Function, Directors approve operational risk reports
- CRO to ensure awareness of compliance with appropriate legislation, guidelines and best practice
- Risk Training provided as part of induction and annually to all staff
- Continue to enhance Risk Reporting to the Audit & Risk Committee Meeting



2024/25 Proposed Action Plan

- Staff training
 - ☐ Follow up training to be provided to all staff in Q4 2024 in Q2 2025
 - ☐ Risk Management is now part of the induction pack for new personnel
 - ✓ Provide training on the Enterprise Risk Management System Camms Risk in Q4 2024
- Assist, train and support Risk Owners in their use of Enterprise Risk Management System Camms Risk
- Continue to embed all Operational, Corporate and Strategic Risk Registers in the Enterprise Risk Management System Camms Risk
- Assist project managers to migrate projects over €20 million in costs or for projects that are a key strategic objective for the delivery of the NTA's Strategy onto the Enterprise Risk Management System Camms Risk
- Other Governance issues:
 - Have RSM UK assurance report to provide management with an assurance as to the adequacy and effectiveness of the controls operating within various systems and also to provide a summary of the internal audit activities undertaken in 2024 by the end of 2024
 - Deliver the Audit & Risk Committee annual report issued to the Board by the Committee Chair to comply with the requirements of the Code and provides a wider perspective on the work of the Committee for 2024 in February 2025
 - Deliver the overall Assurance Letter to Department of Transport from RSM UK, to provide an independent professional opinion on the adequacy and effectiveness of control over the 2024 internal audit programme in relation to applications and over the robustness of the management activity by end of Q1 2024
 - Ensure continued compliance with the Code of Practice for Governance of State Bodies and the Audit & Risk Committee Terms of Reference throughout the year of 2024

