

Risk Management Framework & Action Plan



Version 5.0
September 2022

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

- Next Review Date: September 2023

- Approvals

Position		Name	Date
Corporate Risk Manager	Annual Review	Gerard McBrien	24/08/2022
Chief Risk Officer & Head of Governance	Annual Review	Noel Beecher	31/08/2022
ARC	Annual Review	ARC	09/09/2022
Board	Annual Review	Board	16/09/2022

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

Code of Practice for the Governance of State Bodies

August 2016

2016 Code Obligations

- Audit and Risk Committee;
- Risk management a standing item on the Board meeting agenda;
- Risk management experience/ expertise on Board;
- Chief Risk Officer (Noel Beecher);
- Approve the risk management policy, set the State body's risk appetite, and approve the risk management plan and risk registers;
- Review management reporting on risk management and note/approve actions as appropriate;
- Require external review of effectiveness of risk management framework; and
- 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.

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)

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

(Done)

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

(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)

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

(Done, on-going review)

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 organisational 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 components of the NTA Risk Management framework:

**The
Board**

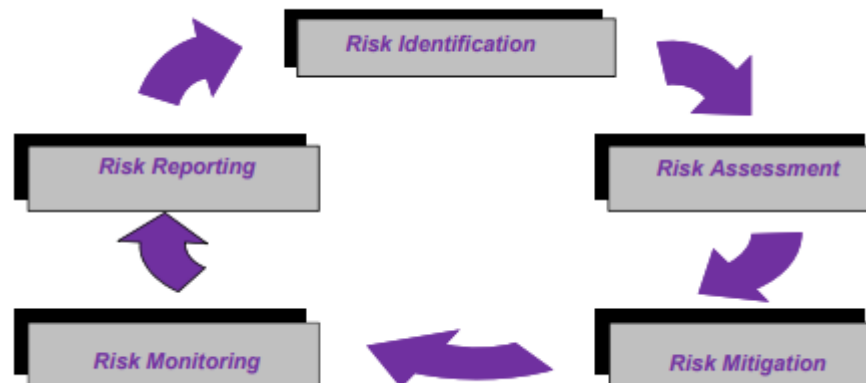
**Audit and Risk
Committee**

**NTA Management
and Staff**

Internal Audit

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

Terminate
Activities that are the source of the risk are terminated

Take
The risk is accepted as it is seen as an opportunity

Risk Management System

Risk Matrix

- 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 Matrix

Likelihood	VH ≥80%	11	16	20	23	25
	H 60%-80%	7	12	17	21	24
	M 40%-60%	4	8	13	18	22
	L 20%-40%	2	5	9	14	19
	VL ≤20%	1	3	6	10	15
		VL	L	M	H	VH
Impact (Financial, Reputation)						

Risk Reporting Scale:

0 – 3 = Green 4 – 10 = Yellow 11 – 19 = Amber 20+ = Red

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

Amber: High - Issues that need constant monitoring by management.

Yellow: Medium - Issues for frequent review

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

Risk Appetite

Risk Appetite Matrix

- 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.

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

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.

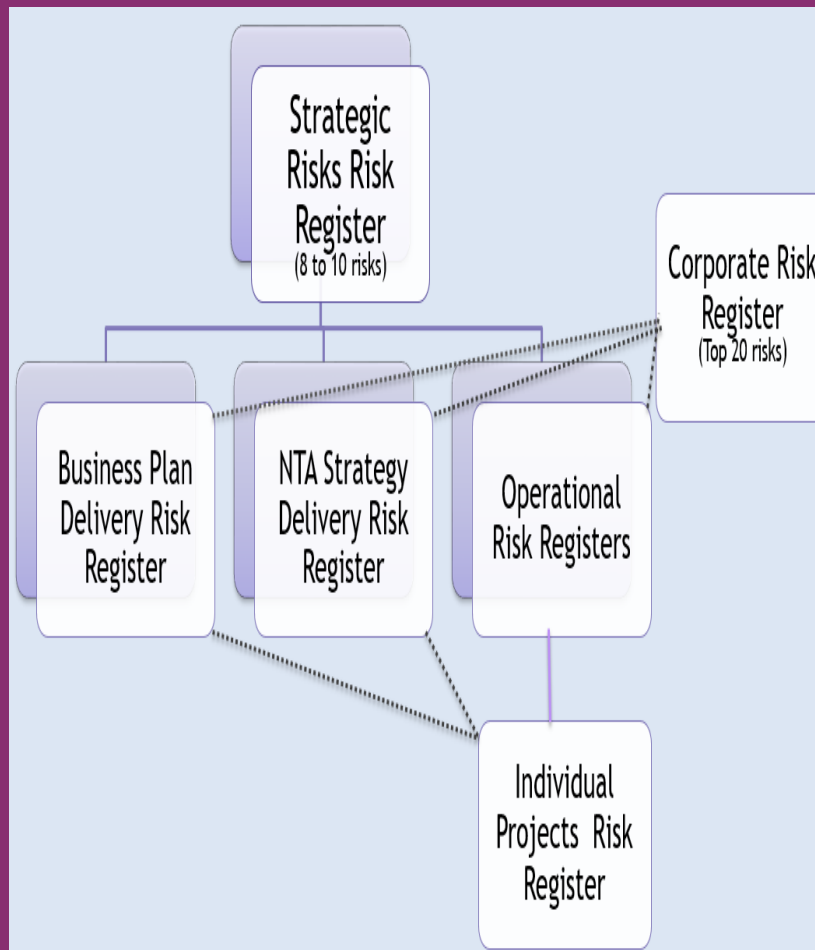
Amber: Cautious - The Authority is willing to select options that are safe and have a low degree of risk.

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

Green: Adverse - 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 Hierarchy

- Within the Authority a Risk Hierarchy exists. Each register is separate however risks do feed up and down through the hierarchy
- The Strategic Risk Register is the 9 risks identified by the ARC and Board in Q2 2022, all risks within the Authority should be linked back to one of these 9 Strategic Risk
- Project registers are for individual specific projects;
- Operational registers are in place from all 27 business units in the NTA;
- The Corporate register is a combination of risks from the NTA Statement of Strategy, the Business Plan, Operational risks and risks management identify. The register is no more than 20 risks at any one time and only includes amber or red risks.



Risk Management Report.....

Risk Report

- Significant risks
- Risk Events
- Deviations in tolerances
- Trends
- New risks
- Emerging 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 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.

Integration with established business processes

Underpins strategy

Complements existing
systems & processes

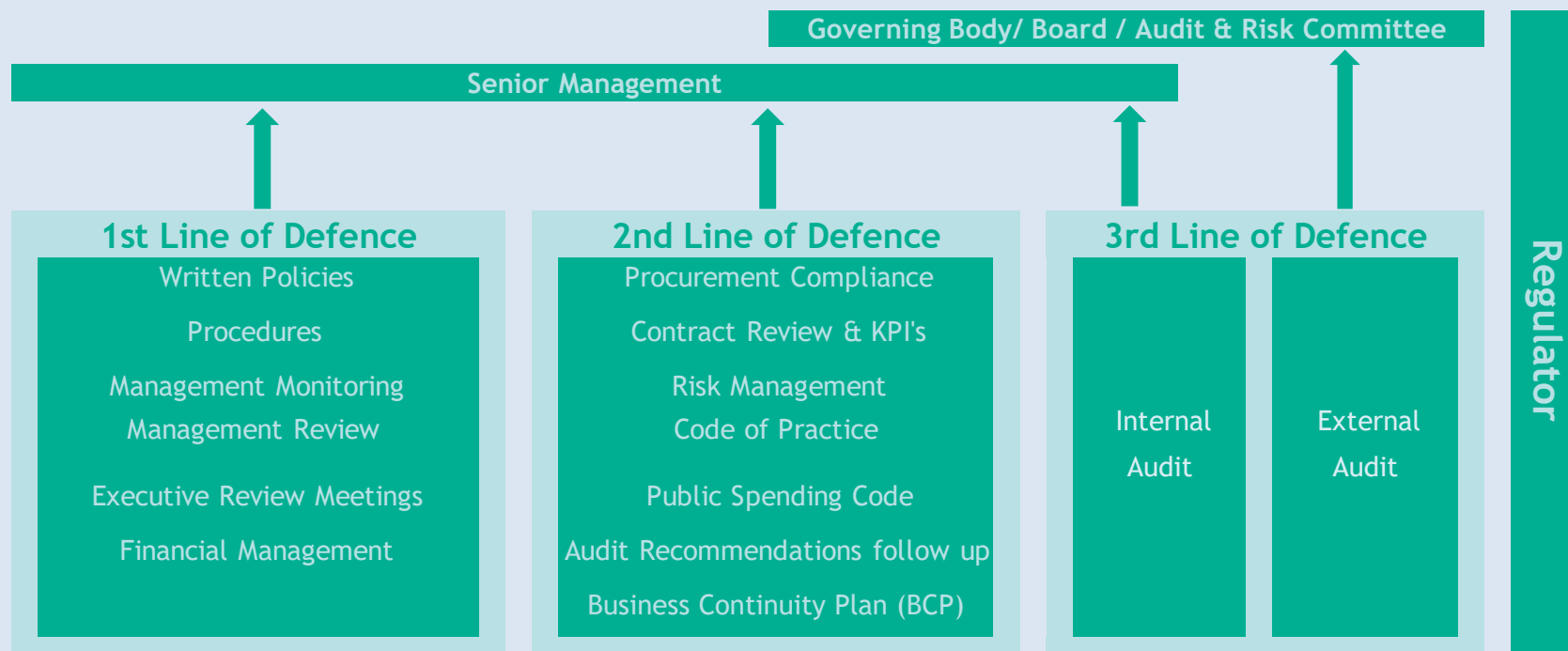


Uses existing
data

Best Practice - 3 Lines of Defence Model

- Assurance Map

The Three Lines of Defence Model



Process in place

Process includes the following are in place;

- Risk on Agenda of all Board and ARC meetings

Corporate risk register reported monthly and strategic risk register reported bi-annually to 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 sign off on 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

2022 Proposed Action Plan

- Staff training
 - ✓ Follow up training to be provided to all staff in Q2 2023
 - ✓ Risk Management is now part of the induction pack for new personnel
- Put in place a Risk Management System to facilitate comprehensive management of all risks within a package
- Once a Risk Management System has been rolled out, all Operational, Corporate and Strategic Risk Registers will review Risk Appetite against this risk and ensure that risk it within its acceptable risk tolerances
- Other Governance issues:
 - Deliver the overall Capital Assurance Letter to Department of Transport from RSM UK, to provide an independent professional opinion on the adequacy and effectiveness of control over the 2021 capital grant spend in relation to applications and over the robustness of the management activity by end of Q1 2023
 - 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 2022 by the end of 2022
 - 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 2022 in February 2023
 - 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 2022