Risk Assurance Services LLP

# Transport for the North

## Risk Maturity Review

## Final Report 3.22/23

## 17 October 2022

RSM

# Contents



RSM

# Executive Summary

## Background

As part of the approved internal audit plan for 2022/23, we have undertaken an advisory review to assess Transport for the North's ('TfN's) risk maturity status.

TfN faces a wide range of risks at all levels across the organisation, and hence risk management is integral to the achievement of its strategic objectives. TfN revised its Risk Management Strategy in September 2022 to incorporate a clearly defined risk appetite, a new '5x5' risk scoring matrix, in addition to setting out the responsibilities and accountabilities of key staff, committees and the TfN Board with respect to risk management. According to the Risk Management Strategy, TfN defines its risk appetite as 'cautious', which is defined by the Orange Book (2021) as:

*"A preference for safe options that have low degree of risk and only limited potential for benefit. Willing to tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant benefit and/or realise an opportunity."*

TfN currently use the Predict Risk Management System for the recording of risk-related information (this includes TfN's project, functional and corporate risk registers). The Predict Risk Management System allows a complete record of all risks, controls, and actions and is automated such that risk owners are assigned to risks and notified when risks are due for review.

At the time of our review (September 2022), the Group had a total of 25 risks recorded on its corporate risk register. Of these 25 risks, six risks had 'red' ratings (very high), 12 risks had 'amber' ratings (high), seven risks had 'yellow' ratings (medium). Further to this, the risk register includes two opportunities, that were rated 'medium' and 'high' in line with the scoring matrices outlined in the Risk Management Strategy.

As part of our review, we conducted focus meetings with a Risk Champion, a member of the Senior Management Team (SMT) and the Chair of the Audit and Governance Committee. We have integrated feedback from these conversations into our findings throughout this review.

The new Risk Manager has continued to further embed the Predict Risk Management system. In our 2021/22 audit, it was noted that TfN did not define its assurance sources in terms of defined assurance mechanisms. We also noted that an 'Assurance Framework' was being developed by TfN to set-out the structures and processes that would support the delivery of the organisation's Investment Programme. This is recognised as an area of development by the Risk Manager. Our Risk Advisory team has been in contact with TfN to provide continued support and advice on the evolving of the Board Assurance Framework.

RSM

# Executive Summary

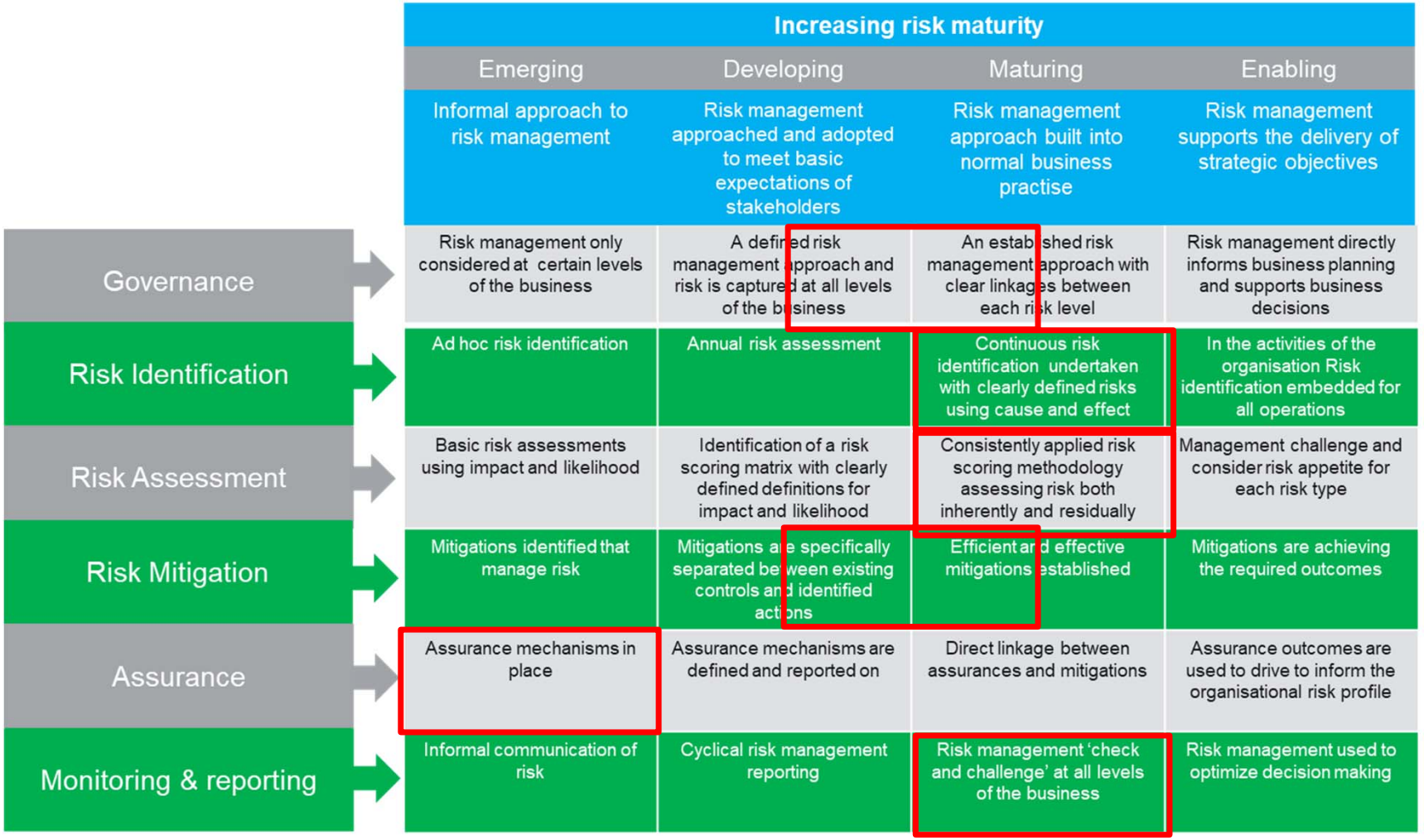
## Conclusion

No formal assurance opinion has been provided in this report due to the advisory nature of the review. However, this review includes an assessment of where TfN sits on the spectrum of RSM's risk maturity matrix (see below). Through our work we were able to confirm that the TfN has established processes in place for the identification and assessment of both current and inherent risk, and for the reporting of this risk information to the Operating Board, Audit and Governance Committee and TfN Board members. This includes improvements to the way in which risk-related information is recorded and reported.

However, whilst clearly established risk management processes are in place, we have included four management actions in this report which are designed to support the ongoing developments in this area. These actions include developing a Board Assurance Framework, utilising the Predict Risk Management System to its full potential and performing deep dives into risk areas that sit outside of the agreed risk appetite. These should further enhance and develop TfN's risk management framework, and work towards the 'enabling' risk maturity level (as outlined on the risk maturity matrix).

RSM

# Risk Maturity Assessment



| | Increasing risk maturity | | | |
|---|---|---|---|---|
| | Emerging | Developing | Maturing | Enabling |
| | Informal approach to risk management | Risk management approached and adopted to meet basic expectations of stakeholders | Risk management approach built into normal business practise | Risk management supports the delivery of strategic objectives |
| Governance | Risk management only considered at certain levels of the business | A defined risk management approach and risk is captured at all levels of the business | An established risk management approach with clear linkages between each risk level | Risk management directly informs business planning and supports business decisions |
| Risk Identification | Ad hoc risk identification | Annual risk assessment | Continuous risk identification undertaken with clearly defined risks using cause and effect | In the activities of the organisation Risk identification embedded for all operations |
| Risk Assessment | Basic risk assessments using impact and likelihood | Identification of a risk scoring matrix with clearly defined definitions for impact and likelihood | Consistently applied risk scoring methodology assessing risk both inherently and residually | Management challenge and consider risk appetite for each risk type |
| Risk Mitigation | Mitigations identified that manage risk | Mitigations are specifically separated between existing controls and identified actions | Efficient and effective mitigations established | Mitigations are achieving the required outcomes |
| Assurance | Assurance mechanisms in place | Assurance mechanisms are defined and reported on | Direct linkage between assurances and mitigations | Assurance outcomes are used to drive to inform the organisational risk profile |
| Monitoring & reporting | Informal communication of risk | Cyclical risk management reporting | Risk management 'check and challenge' at all levels of the business | Risk management used to optimize decision making |

RSM

# Key Findings

## Governance

TfN has a Risk Management Strategy document, which provides details of roles, responsibilities and high-level processes relating to the risk management activities, including the scoring framework and risk appetite employed at TfN. The Risk Management Strategy document was reviewed and approved by the Audit and Governance Committee on 21 September 2022 and is available for staff to access on the TfN SharePoint.

Roles and responsibilities of the groups that oversee the risk management activities are also stated in the relevant terms of reference (these include the Operating Board and the Audit and Governance Committee). However, we noted through review of the TfN Board terms of reference that responsibilities with respect to risk management are not clearly defined. Through discussions with the Risk Manager, we were informed that this is because responsibility has been delegated to the Audit and Governance Committee. As we were able to observe the Audit and Governance Committee discharging this delegated responsibility in practice, and it is clearly defined in the Audit and Governance Committee terms of reference, we do not consider this to be an issue and have not raised a management action in this area. It was further noted that the delegated responsibility is clearly defined within the Risk Management Strategy.

All staff receive mandatory risk management training as part of the induction process. This training package was being redeveloped at the time of our review to incorporate the changes that have been made to the Risk Management Strategy. Additional training has been developed for Risk Champions at TfN, which outlines the changes made to the Risk Management Strategy, in addition to the roles and responsibilities of Risk Champions with respect to risk workshops and risk conversations with responsible owners within their functional areas. Both training packages were being redeveloped at the time of our review and delivered to relevant staff. As such, we did not test compliance with these training packages.

## Risk Identification

All risk registers are recorded on the Predict Risk Management System (including corporate, functional and project level risk registers). Each risk register is divided into sub-categories with individual risks outlined. Access restrictions are established to prevent unauthorised amendment of risks and a list of all users is retained by the Risk Manager.

Each functional area has a designated Risk Champion who manages the functional risk register and the project risk register. The Risk Manager acts as the Risk Champion for the corporate risk register. Risk Champions hold monthly risk workshops with risk owners in their department and review each risk. These workshops act as a ‘check and challenge’ and focus on review of the wording of the risk, the current risk rating and whether this is appropriate, the controls (ongoing ‘business as usual’ activities), mitigating actions (measures taken to reduce the possibility of the risk event occurring) and fallback actions (how to minimise the impact after the event) for each risk and if all risks have been considered. We selected a sample of five risk registers and tested to ensure three risk workshops had occurred in the last three months (September, August and July). Testing identified no exceptions.

RSM

# Key Findings

However, through our walkthrough of the Predict Risk Management System, we identified that a 'progress' update section is available, which allows users to add comments to each risk. The Risk Manager identified that Risk Champions should be populating this progress tab following each workshop to detail what was discussed and the result of those discussions, however from a review of the system, it was noted that this is not being fully utilised. This would be in line with good practice, as it demonstrates a clear audit trail of discussions and that each risk is being considered in the context of the current environment to ensure it is appropriate. At present, there is a risk that scrutiny of risks is not being fully captured and hence we have raised a management action below.

The Risk Manager further chairs a Risk Champion forum on a monthly basis, which allows discussion regarding arising issues across TfN and sharing of good practice. Through review of agendas from February, April and May 2022 we identified discussion surrounding key risk themes and feedback from monthly risk reviews.

**Management action 1:**
Risk Champions will ensure all areas of the Predict Risk Management System are utilised, including:

- Progress update – the progress function will be utilised to record decisions made during monthly risk workshops regarding each risk; and
- The basis for assessment – the basis for assessment box will be completed to record the rationale for the current risk score. (Please refer to next section for details)

**Priority:** Low
**Responsible owner:** Daniella Della-Cerra Smith, Risk Manager
**Implementation Date:** 31 May 2023
*(Progress against this management action has already started, however we have set an implementation date to allow the control to be fully embedded)*

## Risk Assessment and Risk Appetite

TfN uses a 5x5 risk scoring methodology which is built into the Predict Risk Management System to ensure all risks are scored using a consistent methodology. Each risk owner must score their risks utilising an assessments of 'probability' and 'impact' using a defined scoring system (guidance is provided in the Risk Management Strategy to support the risk assessment scores). Impact is scored against five impact areas (external relationships, financial, quality, reputation, and time), with the highest scoring impact multiplied by the probability score to get the overall risk score. Each risk is assessed both in terms of its 'initial score' and its 'current score', and a target risk score is included, which records the risk score TfN wishes to achieve utilising controls and mitigating actions.

The Predict Risk Management System includes a 'basis for assessment' tab, which should be utilised to record the rationale behind the risk score assigned. We selected a sample of five risks (across the corporate risk register, the functional risk registers and project risk registers) and tested to ensure the 'basis for assessment tab' had been completed. Testing identified that in 5/5 cases, no basis for assessment had been included for the risk. Where this is the case, the rationale behind the risk rating is not clearly noted, such that when the risk is reviewed, the rationale cannot be challenged or critically assessed. Please refer to management action one above.

RSM

# Key Findings

A high-level risk appetite statement is included in the Risk Management Strategy, which defines TfN's appetite as 'cautious', with risks with a current risk score of 14 or above being outside of the risk appetite. Through review of the corporate risk register, we identified that in 19/27 cases, the current risk score falls outside of the risk appetite. Where a risk falls outside the risk appetite, the following measures are established:

- The risk will have a 'fallback plan' in the Predict Risk Management System – the Risk Manager informed us that this control was recently implemented and hence not all risks have fallback plans at the time of this review. This is a work-in-progress and hence we did not complete sample testing in this area;
- The risks will be drawn out in reporting to Operating Board, the Audit and Governance Committee and the TfN Board; and
- The risks will be reviewed on a monthly basis as part of the risk workshop, with a focus on the mitigating actions and whether any further actions can be put in place.
- However, aside from the above measures, no further measures are put in place for risks that fall outside of TfN's risk appetite. Whilst we appreciate that the risk rating for these risks are outside of the control of TfN, management may wish to consider putting some additional measures in place to provide the Audit and Governance Committee and the TfN Board with additional assurance regarding the control of areas that fall outside the risk appetite. Through our work, we often observe risk deep dives being conducted into a sample of risks that fall outside of the risk appetite.

These deep dives are concerned with looking at the controls and mitigating actions established by TfN to control the risk, but also the fallback plans that have been established should the risk be realised, and aim to provide the Committee with assurance that the risk is being appropriately handled. Deep dives have previously been considered by the Audit and Governance Committee and should be recommenced in line with good practice. It is acknowledged that there is a requirement to re-focus on risk appetite, recognising the current economic climate and financial constraints.

**Management action 2:**
The Audit and Governance Committee will perform a deep dive into a chosen risk from the corporate risk register in November 2022. Following this, a programme of risk deep dives will be agreed with the Audit and Governance Committee for 2023. Deep dives will include risks that fall outside of TfN's risk appetite, emerging risk areas, or risks that are showing volatility in risk rating. These deep dives will focus on the controls, actions and fallback plans established to mitigate the risk to TfN and provide assurance that the risk is appropriately scored and controls are operating effectively.
**Priority:** Low
**Responsible owner:** Daniella Della-Cerra Smith, Risk Manager
**Implementation Date:** 28 February 2023

RSM

# Key Findings

## Risk Mitigation

The risk register includes details of the existing internal controls relevant to each risk, in addition to mitigating actions (measures taken to reduce the possibility of the risk event occurring) and fallback actions (how to minimise the impact after the event). Each control and action is assigned to a risk owner and is assigned a review date (which is set in line with the monthly risk workshops) and an implementation date. The Predict Risk Management System notifies all owners when actions are due for implementation and actions are reviewed as part of the risk workshops. The Risk Manager reviews a dashboard produced from the Predict Risk Management System on a weekly basis, which details all outstanding actions that have not been reviewed or implemented by their target date (there were no outstanding actions at the time of our review). The mitigating actions and controls are additionally detailed in the corporate risk register which is presented to the Audit and Governance Committee.

## Assurance

TfN do not currently have a function in place to allow for effective assurance mapping in line with the three lines of assurance model. Where this is the case, the TfN Board and Audit and Governance Committee cannot easily assess the assurance mechanisms in place for each risk area and hence effectively identify and assess TfN's vulnerable risk areas.

In the absence of more specific assurance information it may be difficult for the reader to have a clear understanding of how the mechanisms in place provide assurance over the effectiveness of the related controls. Additionally, the absence of documented timings/dates may make it difficult for the reader to understand the timeframes involved and this might have an impact of the reader's ability to monitor the effectiveness and relevance of the assurances and whether these are positive or negative.

**Management action 3:**

a) TfN will establish a Board Assurance Framework, which will include the main areas of risk for TfN and where TfN gets assurance in each area. This Board Assurance Framework will provide for cyclical assessment of controls and the provision of assurance and will be clearly detailed within the Risk Management Strategy.

b) The Risk Manager will work alongside Risk Owners for the key corporate risks to ensure the Board Assurance Framework is embedded and applied for all assurance areas.

**Priority:** Medium
**Responsible owner:** Daniella Della-Cerra Smith, Risk Manager
**Implementation Dates:**
a) 31 March 2023
b) 31 October 2023

RSM

# Key Findings

## Monitoring and Reporting

The Operating Board is responsible for the implementation of the Risk Management Strategy. This includes the receipt of the corporate risk register on a quarterly basis, in addition to the escalation of functional and project level risks on a judgemental basis. Through review of meeting minutes and papers from 22 February, 17 May and 6 September 2022 we identified that a risk update and copy of the corporate risk register was presented and discussed. Through discussions with the Risk Manager, we were informed that functional and project risks are escalated to the Operating Board where appropriate. Through review of the Risk Management Strategy, the process for escalation states that only very high or high risks will be escalated, and this will be done on an ad hoc basis. TfN should clearly define when these risks should be escalated to reduce the risk that key risk areas are not escalated or deescalated as appropriate.

Further to this, the Audit and Governance Committee meet on a quarterly basis and receive TfN's corporate risk register. Through review of meeting minutes and papers from 10 June 2022, 14 July 2022 and 21 September 2022 we identified that a risk update, and copy of the corporate risk register was presented at each meeting. Through review of meeting minutes, we identified scrutiny of the corporate risk register, including whether 'loss of knowledge' and the 'severance process' should be included, and whether Key Performance Indicators (KPIs) from the Business Plan 2022/23 could be included. These suggestions have been subsequently actioned by the Risk Manager and presented to the Audit and Governance Committee. This demonstrates the 'check and challenge' principle at Committee level.

The oversight of the risk management framework is delegated to the Audit and Governance Committee by the TfN Board and hence, the TfN Board receive the corporate risk register and a risk update on a bi-annual basis. Through review of the meeting minutes from 29 September 2021 and 30 June 2022 we identified receipt and discussion of the risk update and corporate risk register.

We additionally obtained a sample of five papers from the two meetings above to ensure that the relevant risk had been considered. Through our review, we noted that a section is included in all TfN Board reports titled 'Risk Management and Key Issues'. In the sample of five reports, all included a narrative on risk, with two reports referencing a specific risk reference from the corporate risk register, one referencing the risk by description and two papers referencing that a risk assessment had been carried out. As risk had been considered in each paper, we do not consider this to be an issue.

**Management action 4:**

The Risk Management Strategy will be amended to include the factors that will be considered when escalating risks to the Operating Board. This could include risks that exceed the TfN risk appetite or could be driven by strategic themes outlined within the Business Plan.

**Priority:** Low

**Responsible owner:** Daniella Della-Cerra Smith, Risk Manager
**Implementation Date:** 31 December 2022

RSM

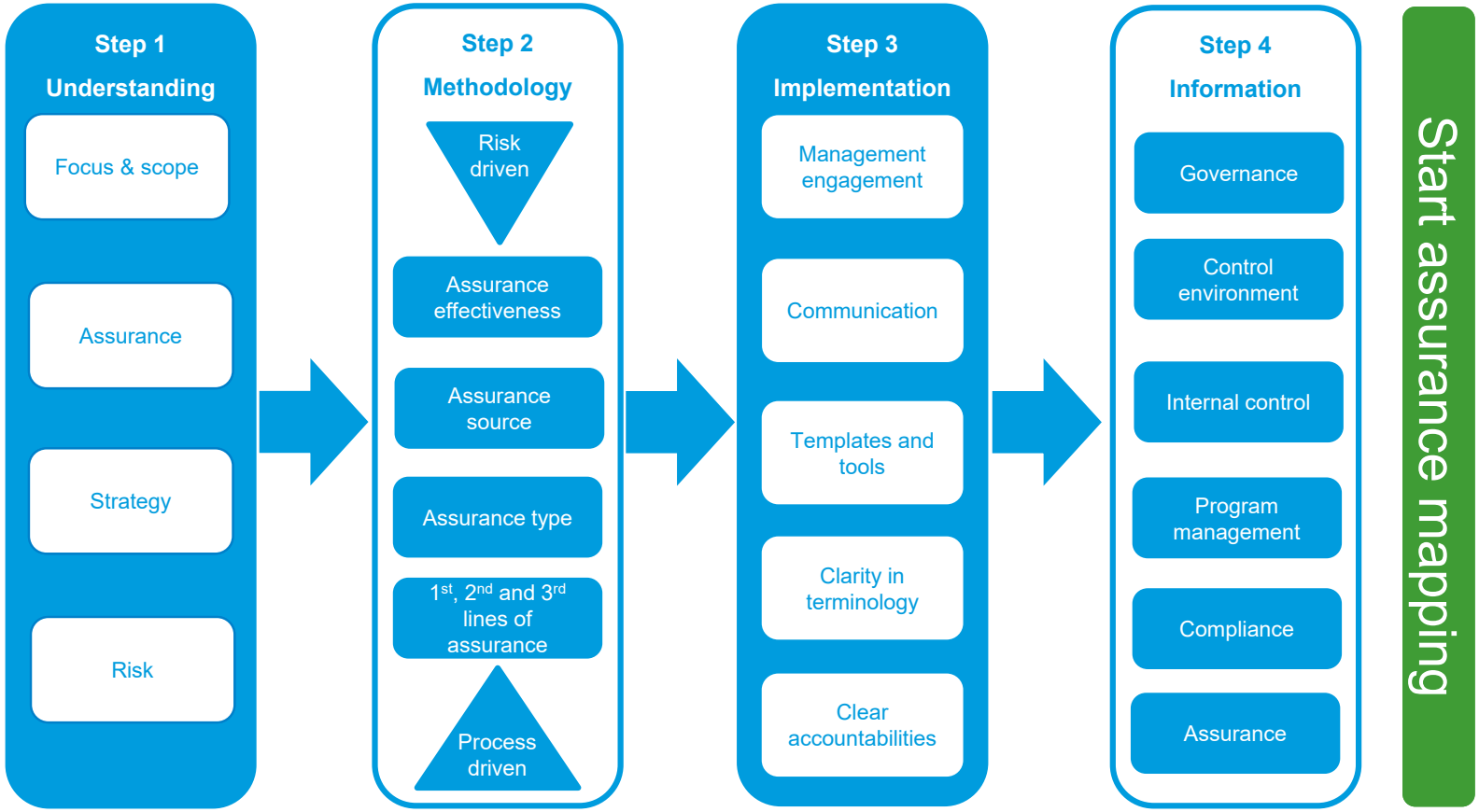
# Key Findings

## Good practice to consider

We noted the following area of good practice for TfN to consider:

- From a good practice point of view, the corporate risk register should contain 10-12 of the keys risks facing the organisation, that will stop TfN from achieving its corporate objectives. A higher number than this can become unwieldly and harder to prioritise and report, leading to the TfN Board and Audit and Governance Committee not being able to digest such an amount of information. Whilst we have not raised a management action to address this, management may wish to consider the existing risks to ensure that they meet the definition of a corporate risk and are truly strategic in nature, whilst considering the ability to achieve its objectives.
- Once the Board Assurance Framework has been embedded and applied, TfN may wish to incorporate wider risks outside the key corporate risks into the framework.

# Appendix A: Assurance mapping – the key steps



# Appendix B: Detailed scope

| | |
|---|---|
| **Objective of the area under review:** | There is an effective risk management framework in place at TfN that is fit for purpose. |
| **Areas for consideration** | **Information Gathering**<br>• Desktop review of key documents i.e. risk registers, risk reports and risk management strategy.<br>• Conduct meetings with Risk Champions to gain an insight into the views and understanding of risk management.<br>**Analysis, Interpretation, Check, Challenge and Conclusion**<br>• Comparison of outcomes from above with best / leading practices (based on RSM experience) and UK standards.<br>• Virtual check and challenge meeting to discuss outcomes with TfN management.<br>• Agree risk maturity assessment and identify where TfN wants to be in the future.<br>• Agree areas for development.<br>**Develop improvement road map**<br>Formulate actions to accommodate areas for development, with priorities, coupled with expected outcomes. |
| **Limitations to scope** | • This is an advisory review, as such no formal opinion will be provided;<br>• We will not seek to verify the accuracy of information provided to the Board and Senior Management;<br>• We do not endorse a particular means of managing information to the Board and Management. It remains the responsibility of the Board and Management to agree and manage information needs and to determine what works most effectively;<br>• Any testing undertaken during the audit will be performed on a sample basis only;<br>• The audit will not involve a comprehensive review of the minutes and papers and will not consider the appropriateness of decisions made;<br>• Our audit is focused on controls surrounding the Risk Management process only. No other process or services undertaken by the organisation will be considered;<br>• We will not comment on whether individual risks are appropriately managed, or whether TfN has identified all of the risks and opportunities it faces;<br>• We will not comment on the appropriateness of risk assessment scores/ gradings assigned by management to identified risks;<br>• We do not endorse a particular means of risk management. It remains the responsibility of the Board and Management to agree and manage information needs and to determine what works most effectively for the organisation;<br>• Conclusions will be based on our assessments made through discussions with management, assessment of the current framework of controls and review of relevant documentation made available; and<br>• Our work does not provide absolute assurance that material errors, loss or fraud do not exist. |

RSM

| | | | |
|---|---|---|---|
| **Debrief held** | 11 October 2022 | **Internal audit Contacts** | Lisa Randall, Head of Internal Audit<br>lisa.randall@rsmuk.com / 07730 300 309 |
| **Draft report issued** | 14 October 2022 | | |
| **Responses received** | 17 October 2022 | | |
| **Final report issued** | 17 October 2022 | | Alex Hire, Senior Manager<br>alex.hire@rsmuk.com / 07970 641 757 |
| | | **Client sponsor** | Paul Kelly, Finance Director |
| | | **Distribution** | Paul Kelly, Finance Director |



RSM