Risk Management

Overview

The NTMA considers that risk management is a fundamental element of corporate governance and is essential to achieving its strategic and operational goals. The NTMA is subject to the Code of Practice for the Governance of State Bodies (2016) ("the Code") which provides guidance for the application of good practice in corporate governance for both commercial and non-commercial State bodies. The NTMA maintains a formal risk management framework underpinned by a strong risk culture and tone from the top, which is overseen by the NTMA Board and various risk committees.

Framework, Policy and Appetite

The NTMA Board sets the Risk Management Policy and Framework and the Risk Appetite Framework. The Risk Management Policy and Framework defines the standards for risk management across the organisation. It includes the objectives, structures, governance, policies, responsibilities and processes that support the effective and integrated management of risk, consistent with the NTMA's risk appetite.

The NTMA has defined its risk appetite for its key risk categories within the Risk Appetite Framework. Risk exposures are monitored through the use of key risk indicators (KRI) and limits as appropriate. The Risk Management Policy and Framework and Risk Appetite Framework are reviewed at least annually to ensure that they remain relevant and up-to-date.

Governance

The Audit and Risk Committee ("the ARC") assists the NTMA Board in the oversight of the Risk Management Framework including monitoring adherence to risk governance, risk appetite and ensuring risks are properly identified, assessed, managed and reported. An executive-level Enterprise Risk Management Committee ("ERMC") oversees the effective management of risk and compliance and monitors the organisation's overall risk profile and principal risk exposures. The NTMA's approach to risk management is based on the "three-lines-of-defence" model, set out below, and is designed to support the delivery of its mandates by proactively managing the risks that arise in the course of the NTMA pursuing its objectives.

Three Lines of Defence Model

First Line

Business Areas

- Ownership and primary responsibility for identifying, measuring, monitoring, controlling and reporting risks on a day to day basis
- Ensure business activities are within the NTMA's risk appetite and compliant with risk management policies

Second Line

Risk Management and Compliance

- Provide independent oversight, review and challenge to the first line of defence
- Independently facilitate and monitor the implementation of effective risk management and compliance practices
- Provide comprehensive and understandable information on risk and compliance matters
- Responsible for risk and compliance policy development, limits and controls
- Provide training, tools and advice to support policy compliance

Internal Audit

Provides independent, reasonable, risk based assurance on the robustness of the risk management system, governance and the design and operating effectiveness of the internal control environment

Third Line

Risk Assessment

Risk assessment processes are designed to ensure that material risks are identified, that the NTMA manages its risk within its agreed risk appetite, and that the management of risk is monitored within clearly defined and delineated roles and responsibilities.

Individual business units and corporate functions maintain risk registers in which their key risks and controls are recorded and responsibility for the operation of controls is assigned. These registers are reviewed twice yearly by the respective business units and corporate functions and the controls therein are attested by the control owners. The review:

- Identifies or re-confirms and classifies the risks to the business;
- Assesses the inherent and residual risk impact and likelihood;
- Identifies existing controls and assesses their effectiveness;
- Identifies proposed treatments and controls;
- Allocates owners for any agreed action plans; and
- Reports on the implementation of measures and controls to address the residual risks.

Business units present principal risks from their risk registers to the ERMC and the ARC at least annually.

Strategic Risks

The NTMA Board oversees a formal, top-down assessment of its strategic/principal risks at least annually, the purpose of which is to identify and mitigate the key risks to the execution of NTMA mandates from an organisation-wide perspective and, in particular, to address any emerging risks as early as possible.

Risk	Description and Potential Impact	Mitigation
Macro, Financial and Market Risk	The risk that extraneous risks such as adverse macro-economic conditions, unpredictable geopolitical or regulatory developments and/or market volatility could negatively impact the NTMA's ability to achieve its objectives. Possible consequences include a deterioration of the fiscal position leading to increased funding requirements, difficulties in accessing funding or investment opportunities, deterioration of debt sustainability, increased debt service costs, re-financing risk, increased cost and/or delay of infrastructure delivery, unsatisfactory economic impact or sub-optimal investment returns and/or potential reputational damage.	Flexibility and diversity in the funding strategy, the funding plan and the investment strategy and portfolios, which can be amended as required through appropriate processes and governance channels; The National Debt's current maturity profile reduces exposure to volatility in funding costs in the short to medium term; Funding plan and KPIs are approved and reviewed by the NTMA Board; Diversified ISIF Global and Irish Portfolios; Active liquidity, market and counterparty credit risk management, governed by policies that are reviewed and approved annually with appropriate risk monitoring and reporting to risk governance committees. Asset and liability portfolios are managed in accordance with Agency-approved risk appetite and monitored daily against policy limits; On-going monitoring and reporting of market and macro-economic trends, implications and key market risk indicators including horizon scanning and stress testing; On-going monitoring and reporting of emerging regulatory developments; Where specific risks are identified (e.g. the Russian invasion of Ukraine), tailored action plans are put in place and monitored; NDFA monitoring project counterparty and macroeconomic risks.

Risk	Description and Potential Impact	Mitigation
Investment Risk	The risk that actual investment performance deviates materially from the expected outcomes of relevant investment strategies. Possible consequences include: I. Financial losses or sub-optimal returns; and/or II. Unsatisfactory economic impact; and/or III. Reputational damage.	NTMA Board approved ISIF investment strategies for Global and Irish Portfolios in place; All new ISIF Irish Portfolio investment proposals are subject to review by first and second line and NTMA governance committee reviews prior to Investment Committee/NTMA Board submission; Investments are governed by investment, liquidity, market and counterparty credit risk policies which are subject to regular reviews by the appropriate governance committee; Appropriate strategies, governance structures, policies and processes are capable of being adapted as required, facilitated through: • The ability to re-prioritise and re-direct resources • use of various sources of expertise (staff, external secondees, advisors) and • the availability and agility of key governance committees; On-going first and second line monitoring and reporting on ISIF's Irish and Global portfolios (including quarterly portfolio reviews, KRIs and RAG status reporting) to the relevant governance committees and regular engagement between the first and second lines of defence; Regular communications with Global Portfolio investment managers and existing investees on the Irish Portfolio.
Liquidity Risk	The risk that, over a specific time horizon, the NTMA will have insufficient cash to meet its obligations as they fall due. Possible consequences include failure to access funding, the inability to fund the State and the inability to fund investments resulting in reputational damage and/or the NTMA being unable to achieve its objectives.	Full year Exchequer surplus for 2022 led to robust opening cash balances in 2023 and a reduced funding requirement; Funding plan and KPIs are approved and reviewed by the NTMA Board; NTMA Board approved ISIF Global Portfolio Strategy is in place and regularly monitored to ensure adequate liquidity; Flexibility and diversity in the funding strategy, the funding plan and the investment strategy and portfolios, which can be amended as required through appropriate processes and governance channels; Active management of the debt maturity profile; A Liquidity Risk Policy, which includes appropriate limits and liquidity buffers, is in place for the Exchequer and ISIF; Regular stress testing of portfolios to model resilience in adverse scenarios; Monitoring (including horizon scanning) and reporting of liquidity risk exposures is performed with appropriate escalation to Risk Committees; Structural supports in the EU available to Ireland in the event of an unanticipated deterioration in market conditions (e.g. EU Recovery Fund).

Risk	Description and Potential Impact	Mitigation
NTMA Climate Risk	The risk that the NTMA fails to take the necessary actions to integrate climate action (as appropriate) into its business decisions in the context of delivering its mandates to Government and delivering an environmentally sustainable organisation in line with its Climate Strategy. Possible consequences are reputational damage and/or the NTMA being unable to achieve its objectives.	NTMA Climate Action Strategy, informed by the Government's Climate Action Plan, in place, monitored and reported on; ISIF Climate and Sustainable and Responsible Investment Strategies in place, which seek opportunities to invest €1bn over five years in climate positive investments, integrate climate action across all investments and assess and engage on investee transition risks (including emissions) across both the Irish and Global Portfolios; Active divestment and exclusion of fossil fuel assets from ISIF's Global Portfolio; Issuance of sovereign green bonds, where proceeds are allocated to eligible green projects as outlined in the National Development Plan, which contribute to carbon emission reductions. Active role in the development of European green bond market and standards; NewERA actively work with the relevant Government Departments in relation to actions assigned to NewERA in the Government's Climate Action Plan; Various NTMA corporate initiatives including the Green Team and the Sustainability Group are in place; KRIs in place to monitor year-on-year reduction in emissions and completion of NTMA Actions within the Climate Action Plan; Any new projects being procured by the NDFA include green procurement initiatives; State Savings digitalisation programme to reduce waste and move to sustainable and efficient processes including digital correspondence, EFT payments and paper reduction.

Risk	Description and Potential Impact	Mitigation
Cyber Security Risk 	The risk of the NTMA or its third parties being the subject of a successful cyber-attack/social engineering attempt. Possible consequences include a failure to execute critical processes, leakage of sensitive information, data breach, system integrity issues, system outages or malware, which may lead to business disruption, financial loss and/or reputational damage.	Monitoring, testing and reporting of ICT traffic, ICT security, cyber threat landscape and expert external advice on emerging trends and cyber threats, including engagement with the National Cyber Security Centre, industry peers and the Financial Stability Group; Regular ICT upgrades and patching of systems to ensure systems and security remain up-to-date; Cyber Security Framework in place based on the National Institute of Standards and Technology ('NIST') Framework; ICT security requirements are incorporated and assessed as part of system/service procurement and selection. Third party cloud services are subject to an assessment and approval process; Third Party Risk policy in place, with supporting procedures and guidance covering ICT involvement in assessing the adequacy of third party information security measures; IT Security Committee in place focusing on ICT security matters. IT Security Operations Committee in place which oversees the implementation of the NTMA ICT Cyber Security Management Framework in protecting NTMA information and systems, both on-premises and in the cloud; End user ICT security policies in place with mandatory cyber security staff training, and regular cyber awareness communications via email and intranet; Simulated spear-phishing campaigns and training for employees; Annual third party cyber security posture assessment tracking maturity and benchmarking the NTMA against the industry; Data protection policy and related procedures, periodic training and risk based monitoring in place; Enhanced cyber security focused KRIs regularly monitored at function and organisational level; Regular audits and external reviews of cyber security.

Risk	Description and Potential Impact	Mitigation
Third Party Risk	The risk of failure by an NTMA third party service provider, counterparty, or stakeholder to successfully deliver on its contractual obligations or act in a manner consistent with the NTMA's expectations and/or requirements. Possible consequences include interruption to critical operations and/or financial loss and/or reputational damage.	Third Party Risk Policy in place, with supporting procedures and guidance. The policy requirements include criticality assessment, due diligence, risk assessment, written agreements, on-going monitoring, oversight and reporting of critical third party arrangements undertaken as required depending on the nature of the third party service/product; Dedicated procurement team and procedures in place for managing the tendering process for relevant third party services; Third party contracts approved by internal management and reviewed by legal advisers, where appropriate; Technical ICT advice provided as part of the tendering process for new technology services, where appropriate; Regular communications with third parties which is adapted in terms of the frequency and focus in response to the risk profile of the third party; Third party service oversight subject to periodic internal audit review; Annual attestation required from units/functions by ICT to ensure appropriate visibility and oversight of systems in use; Risk-based oversight of third party Data processors by Data Protection Officer.
Business Disruption and ICT Resiliency Risk	The risk of business disruption or inadequate resilience due to technology failure (e.g. software, hardware or network issues), failure to appropriately upgrade/augment existing technology, a loss of critical services (e.g. utilities) or ineffective change management. Possible consequences include poor operational performance, fragmented collaboration services, financial loss, reputational damage and/or the NTMA being unable to achieve its objectives.	Alternative working arrangements available (including remote working capabilities) to cover various business disruption scenarios and alternative processes in place (or established) for key business processes/activities, including regular testing of the alternative processes; Regular ICT upgrades and patching of systems to ensure systems and security remain up-to-date; ICT Steering Committee in place to oversee strategic ICT projects and ICT architecture and an ICT Project Management Office ('PMO') in place, resourced with experienced project managers; Experienced ICT Service Desk Team, with an increasing focus on timely and clear communications; ICT Change Advisory Board ('CAB') in place with formal review of key risk assessments and approval of upcoming changes; Contingency planning: alternative processes in place (or established) for key business processes/activities, and regular testing of alternative processes; An active business continuity management ('BCM') plan and programme, with regular testing of plans and scenarios including communication tools and BCM training rolled out to all NTMA employees; Defined crisis management and incident response teams in place; Use of certain cloud based systems with simplified Software Development Life Cycles and more efficient access to upgrades.

Risk	Description and Potential Impact	Mitigation
Process Risk	The risk of inadequate or failed internal processes, or that processes do not appropriately balance robustness with flexibility and as such are not sufficiently agile and adaptable to support a dynamic workplace or to respond to an evolving environment, circumstance, or mandate. Possible consequences include financial loss, business disruption, breach of legal/regulatory requirements and/or reputational damage.	Risk and control assessment processes help to ensure control measures are adequate and re-evaluated to address evolving risks; Alternative processes in place (or established) for critical business processes/activities, and regular testing of alternative processes; Appropriate operational risk and compliance policies are in place, supported by guidance documents, procedures and staff training; Various projects and initiatives on-going across the NTMA to increase process automation and flexibility to achieve efficiencies and enhanced effectiveness; Operational event reporting process in place with key actions identified and monitored. Events are subject to second line and risk committee review and challenge, and periodic trend analysis; Second line corporate functions available to support and challenge material process changes as required; Oversight committees in place with scope to react to changes in the environment or processes; KRIs in place, including indicators regarding operational events and process issues, and reported to the relevant risk governance committee; Regular risk-based internal audits and external audits and resolution of agreed audit actions; Appropriate use of internal and external professional advice; Enterprise Risk Management system in place supporting risk and control assessments, operational event reporting and KRIs; Automation, control and monitoring of payment processes.

Risk	Description and Potential Impact	Mitigation
People and Behavioural Risk	The risk of failure to (i) recruit, retain and develop a sufficiently skilled, diverse, engaged, resilient and adaptable workforce and/or (ii) to maintain ethical and positive workplace behaviours in a manner consistent with relevant laws, regulations, policies, and expectations. Possible consequences include an adverse impact to the NTMA's ability to execute its mandates, financial loss, business disruption and/or reputational damage.	A HR Strategy is in place and is regularly revised; Continued investment in staff through a Learning and Development (L&D) programme with a focus on leadership and management skills, and regular staff communications; The NTMA operates a structured recruitment and selection process; Workforce planning, assessing capacity within teams, identifying redeployment requirements and succession planning in place; Retention rates are monitored and reported and succession planning is undertaken; Measures focused on maintaining employee wellbeing and strong engagement in the hybrid working environment and regular staff engagement surveys and staff communications; Annual resources budgeting, performance reviews and L&D requirements processes in place; Compliance training, communication and advice provided to all relevant internal stakeholders to support and maintain a positive culture of compliance; A range of HR and Compliance policies, codes and procedures help to ensure best practice in people management and upholding ethical standards; Key internal controls and anti-fraud measures are in place; KRIs in place focused on staff retention, recruitment, inclusion and diversity; Regular risk-based internal audits, external audits and Second Line monitoring.