Risk Management

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 Agency and various risk committees.

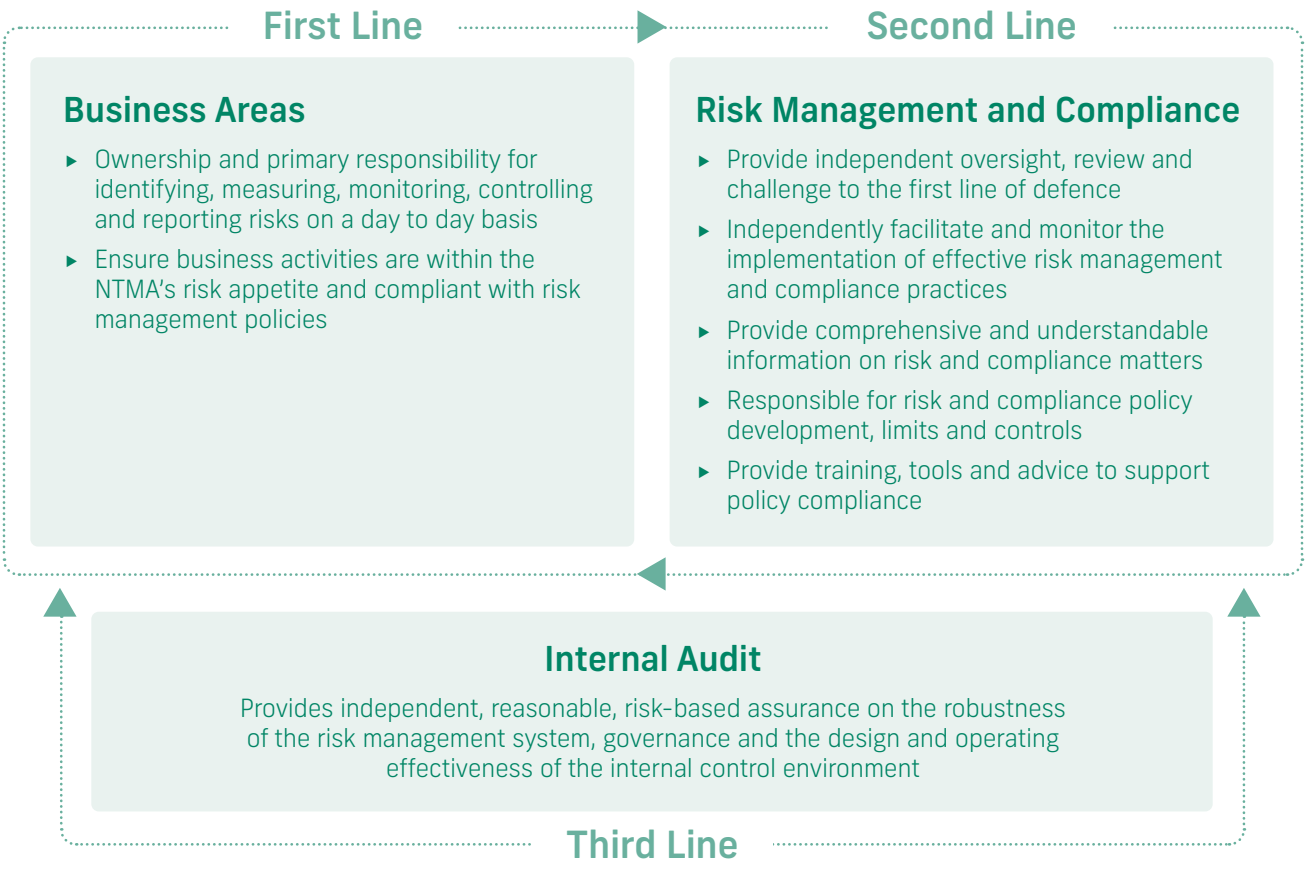
Framework, Policy and Appetite

The Agency has a formal risk management and governance framework in place, designed to support the proactive management of risk. The Agency's Risk Management Policy and Framework and Risk Appetite Framework together set out its risk appetite, its risk management structures and processes and details the roles and responsibilities of staff in relation to risk. The Agency has ultimate oversight and accountability in relation to risk management and provides direction by approving the Risk Management Policy and Framework and the Risk Appetite Framework. Thereafter, the Agency assures itself on an ongoing basis that executive management is responding appropriately to risks.

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

Governance

The Audit and Risk Committee (the ARC) assists the Agency in the oversight of the Risk Management Framework including monitoring adherence to risk governance and risk appetite with the objective of ensuring that risks are properly identified, assessed, managed and reported. An executive-level Enterprise Risk Management Committee (ERMC) oversees the effective management of risk and compliance by reviewing and/ or approving key risk frameworks and policies, monitoring the organisation's risks and controls and monitoring the overall risk profile and principal/strategic risks. 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.



Risk Assessment

Risk assessment processes are designed to provide assurance 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 both their strategic and emerging risks as part of their periodic risk register presentations to the ERMC and the ARC.

Strategic Risks

The Agency oversees a formal, top-down assessment of its strategic 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 to address any emerging risks as early as possible.

Risk	Description and Potential Impact	Mitigation
 **Geopolitical and Macro Financial Risk**	The risk that adverse macro-economic conditions, unpredictable geopolitical or regulatory developments could negatively impact the NTMA's ability to achieve its objectives including difficulties in accessing investment opportunities; 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.	Ongoing monitoring and reporting of market and macro-economic trends, implications, key market risk indicators and emerging regulatory developments including horizon scanning and stress testing; Where specific risks are identified as part of the ongoing monitoring and reporting, tailored action plans are developed, assigned to responsible owners, and actively monitored to support timely completion; 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; Flexible annual funding plan for the Exchequer, annual investment plan for Social Insurance Fund (SIF) Investment Portfolio, and the diversified long-term investment strategies for ISIF, FIF, and ICNF reviewed and approved by the Agency; NDFA monitors project counterparty risks and macroeconomic risks. Changes to inflation provisions are now included in new PPP and Exchequer funded contracts; The Financial Stability Group (FSG) is a forum for senior officials from the Department of Finance, the Central Bank of Ireland and the NTMA which meets regularly to review and prepare for potential risks to Irish financial stability.

Risk Management (continued)

Risk	Description and Potential Impact	Mitigation
 **Market and Investment Risk**	The risk that (i) NTMA will incur losses or higher funding costs due to adverse movements in market variables or (ii) actual investment performance deviates materially from the expected outcomes of relevant investment strategies.	Active management of the national debt maturity profile. The current profile reduces exposure to volatility in funding costs in the short- to medium-term; All investments are governed by Investment and Market Risk policies which are subject to regular reviews by the appropriate NTMA governance committee; Monitoring of emerging risks and regular stress testing of portfolios is undertaken to model resilience in adverse scenarios, with appropriate escalation to risk committees; Diversified investment strategies for ISIF, FIF and ICNF are in place which are reviewed and approved by the Agency, subject to Ministerial consultation; All new ISIF Irish Portfolio investment proposals are subject to separate first and second line review and assessment prior to Investment Committee/Agency submission; 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; Ongoing first and second line monitoring and reporting on ISIF's Irish and Funding Portfolios and FIF and ICNF's Portfolios (including quarterly portfolio reviews, KRIs and Red, Amber, Green (RAG) status reporting) to the relevant NTMA governance committees and regular engagement between the first and second lines of defence; Annual reviews conducted of each existing investment in the Irish Portfolio, including an assessment of performance against original targets and presented to an ISIF governance committee; Regular communications with existing ISIF Irish Portfolio investees and ISIF Funding Portfolio, FIF and ICNF investment managers, as well as the relevant custodians; Monitoring and reporting against agreed statutory benchmark.

Risk	Description and Potential Impact	Mitigation
 **Liquidity and Counterparty Credit Risk**	Liquidity and Counterparty Credit Risk respectively represent the risk that the NTMA will (i) have insufficient cash to meet its obligations as they fall due or (ii) suffer financial loss arising from the failure of a financial market counterparty to meet its contractual obligations.	Active management of the national debt maturity profile. The current profile reduces exposure to volatility in funding costs in the short- to medium-term; Active liquidity 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; Counterparty credit proposals are subject to independent first- and second-line review and assessment prior to submission to Counterparty Credit Risk Committee for approval; Monitoring of emerging risks and regular stress testing of portfolios is undertaken to model resilience in adverse scenarios 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); Ability to raise short term funding by reopening the Treasury Bill programme and increasing Euro Commercial Paper; Flexible annual funding plan for Exchequer, annual investment plan for SIF, and diversified long-term investment strategies for ISIF, FIF, ICNF and SIF are in place, reviewed and approved by the Agency.

Risk Management (continued)

Risk	Description and Potential Impact	Mitigation
 **NTMA Sustainability and Climate Risk**	The risk that the NTMA fails to take the necessary actions to integrate sustainability and climate action (as appropriate) into its business decisions in the context of delivering on its mandates to Government and delivering an environmentally sustainable organisation in line with its Climate Action Strategy.	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. Assessment of ESG score across all proposed investments and ongoing assessment and engagement on investee transition risks (including emissions) across both the Irish and Funding Portfolios; ESG approach includes divestment and exclusion of certain categories (e.g. fossil fuel activities) from ISIF's, FIF's and ICNF's Portfolios under the applicable strategies; Issuance of sovereign green bonds, where proceeds are allocated to eligible green projects as outlined in the National Development Plan (NDP), which contribute to carbon emission reductions. Active role in the development of European green bond market and standards; NewERA actively works 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; Any new projects being procured by the NDFA include green procurement plans. NTMA corporate procurements also include the provision for green procurement requirements where appropriate; KRIs in place to monitor year-on-year reduction in emissions; Equity, Diversity and Inclusion (EDI) and Wellbeing strategies are in place.

Risk	Description and Potential Impact	Mitigation
 **Cyber Security Risk**	The risk of the NTMA or its third-party service providers, counterparties, investees or stakeholders being the subject of a successful cyber-attack/ social engineering attempt that may result in failure to execute critical processes; leakage of sensitive information leading to data breaches and system integrity issues; system outages or malware.	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 FSG; Regular ICT upgrades and patching of systems to maintain systems and security so they remain up-to-date; 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; Guidelines regarding the use of Generative AI are incorporated into the IT User Security Policy, which applies to all NTMA employees; Regular simulated 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, 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 Management (continued)

Risk	Description and Potential Impact	Mitigation
 **Third Party Risk**	The risk of failure by an NTMA third party service provider, counterparty, investee or stakeholder to successfully deliver on its contractual obligations or act in a manner consistent with the NTMA's expectations and/or requirements.	Third Party Risk Policy in place, with supporting procedures and guidance. The policy requirements include criticality assessment, due diligence, risk assessment, written agreements, ongoing 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 internally in accordance with authorities delegated from the Chief Executive 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 adapted in terms of the frequency and focus in response to the risk profile of the third party; Annual attestation required from business units/ corporate functions by ICT to support appropriate visibility and oversight of systems in use; Risk-based oversight of third-party data processors by Data Protection Officer; A Generative AI Governance Framework for third party products has been implemented to support appropriate oversight and governance.

Risk	Description and Potential Impact	Mitigation
Business Disruption and 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), severe weather events and/or geopolitical incidents, ineffective change management or an ineffective response to disruption.	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 maintain systems and security so they 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; 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.

Risk Management (continued)

Risk	Description and Potential Impact	Mitigation
 **Process and Change Risk**	The risk of inadequate or failed internal processes, the occurrence of fraud or processes that do not appropriately balance robustness with flexibility and as such are not sufficiently agile and adaptable to support a dynamic workplace or change delivery, in response to an evolving environment, emerging technologies (e.g. AI) or changing/new mandates.	Risk and control assessment processes help to provide assurance that 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; Enhanced oversight, governance and support in place for key strategic projects; Various projects and initiatives ongoing 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; Enterprise Risk Management system in place supporting risk and control assessments, operational event reporting and KRIs; Automation, control and monitoring of payment processes; A Generative AI Governance Framework for third party products has been implemented to support appropriate oversight and governance.

Risk	Description and Potential Impact	Mitigation
 **People, Behavioural and Conduct Risk**	The risk of: (i) Failure to recruit, retain, (adequately) reward and develop a sufficiently skilled, diverse, engaged, resilient and adaptable workforce; and/or (ii) Failure to maintain ethical and positive workplace behaviours in a manner consistent with relevant laws, regulations, policies, expectations and the Code of Conduct of the NTMA.	A People Function Strategy is in place and is regularly revised; Continued investment in staff through: - 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; 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; Tone from the top set by the Agency including NTMA values integrated into the Corporate Strategy; Compliance training, communication and advice provided to all relevant internal stakeholders to support and maintain a positive culture of risk and compliance; A range of People Function and Compliance policies, codes and procedures help to support best practice in people management and upholding ethical standards; Regular mandatory training required to be completed by all employees; 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 and assurance testing is conducted.