NIPEC Corporate Risk Register 2024-25

1. Purpose of this report

The purpose of this report is to ask Business Team to consider the draft Corporate Risk Register 2024-25 version 1.

All risks from 2023-24 have been included in the new version and members are asked to note the raised scoring of Risks 1 and 2.

2. Action Required

Business Team are asked to approve Version 1 of the 2024-25 Corporate Risk Register.

RISK 1	NIPEC is unable to fully achieve its business objectives as stated in the NIPEC Business Plan 2024-25				
Impact Score	**4 (Major)**	**Risk Owner(s)**	**Chief Executive/SMT**	**Date Added to Register**	**2nd May 2023**
Likelihood Score	**4 (Likely)**	**Risk Appetite**	**Cautious**	**Target Date Action Completion**	**March 2025**
Current Classification	**High (16)**	**Category**	**Performance**	**Target Score/ Classification**	**Low**
Controls	• Progress on corporate and professional objectives are reviewed by Council and the senior team as follows: - At Business and Professional Team meetings every 6 weeks; - Professional & Business Committee are responsible for monitoring progress on professional rag rated workplan objectives and providing assurance to Council on achievement of professional objectives; - Audit & Risk Committee are responsible for monitoring progress on corporate governance objectives and providing assurance to Council that these are being met; - A RAG rated professional workplan and corporate governance objectives update are presented to each Council meeting; • The Chief Executive monitors progress on individual objectives at 1:1 meetings which take place every 6 weeks; • NIPEC report progress on objectives at Sponsor Branch, Ground Clearing and Accountability meetings; • The Chief Executive reports progress/delays to the Chief Nursing Officer at their 1:1 meeting.				
Gaps in Control	• Limited use of Associates due to constraints in NIPEC Budget allocation / availability of slippage; • External factors, for example, no confirmed allocation; • NIPEC's Performance Management Framework to be reviewed and updated in terms of setting completion timelines for projects.				

Sources of Assurance	• Annual Report and Accounts; • Mid-year Assurance report and Assurance Maps; • Annual Quality report; • Performance Reports against Business Plan to NIPEC Council and Committees.
Gaps in Assurance	• Prioritisation of Projects for the 2024-25 year.
Impact of Risk	**Business Objective: Governance & Performance** Failure to achieve objectives in the current climate may result in NIPEC being unable to demonstrate value for money and our added value to the HSC system. It may also limit opportunities to participate in other areas of work.
Actions taken to date	**April 2024:** • Available resources (Associates) agreed and allocated to project leads; • Draft budget prepared and mitigations in place in relation to challenges of forthcoming budget forecast.
Future Actions	**May 2024 to March 2025:** • Senior planning day to be arranged to prioritise / weight projects; • Monitoring of progress objectives by BTM, PTM, Council and Committees; • Development of new NIPEC Performance Management Framework to include weighting of projects; • Monthly monitoring of budget and using slippage where available to increase capacity; • Finalise appointments of 2 project support officers and Committee Secretary; • Completion of Senior Team's appraisals and personal development plans; • Chief Executive to monitor progress of individual objectives at senior team 1:1 meeting; • Reporting of progress to Sponsor Branch, Ground Clearing & Accountability meetings; • Presentation of individual NIPEC projects to Council meeting to remain a standing agenda item.

RISK 2	Risk to NIPEC's ability to achieve financial breakeven due to a reduction in NIPEC's financial allocation for 2024-25				
Impact Score	**4 (Major)**	**Risk Owner(s)**	**Chief Executive/SMT**	**Date Added to Register**	**2nd May 2023**
Likelihood Score	**3 (Possible)**	**Risk Appetite**	**Cautious**	**Target Date Action Completion**	**March 2025**
Current Classification	**High (12)**	**Category**	**Performance & Reputational**	**Target Score/ Classification**	**Low (4)**
Controls	• NIPEC have prepared a draft 2024-25 budget based on a flat cash allocation; • Limited discretionary spend subject to confirmation of allocation for 2024-25; • Limits in place regarding use of NIPEC's Associate list based on funds being available; • Monthly budget monitoring meetings with BSO to track expenditure; • Submission of monthly Financial Monitoring Return (FMR) to DoH Finance; • BSO Annual Finance SLA.				
Gaps in Control	• Lack of confirmed allocation for 2024-25.				
Sources of Assurance	• Reporting of financial position to Business Team, A&RC and Council; • Presentation of Annual Report and Accounts to Audit & Risk Committee; • 'Clean' Annual Accounts for 2023-24; • Annual Financial Management Internal Audit and achievement of Satisfactory Assurance; • Quarterly assurance from BSO Finance that all objectives in SLA carried out.				
Gaps in Assurance	None identified.				

RISK 2	Risk to NIPEC's ability to achieve financial breakeven due to a reduction in NIPEC's financial allocation for 2024-25
Impact of Risk	**Business Objective: Finance & Governance** Failure to achieve financial breakeven may impact NIPEC's ability to deliver objectives, both from a financial and recruitment perspective. As financial breakeven is a mandatory requirement, failure to achieve it may damage NIPEC's reputation.
Actions taken to date	**April 2024:** • Preparation of a 2024-25 draft budget with implications of various savings scenarios included; • Regular updates to Senior Management Team and Business Team meetings; • Update to NIPEC Council at its March 2024 meeting; • Business Case submitted to NIPEC's Sponsor Branch requesting funding for the Ethnic Diversity Officers to March 2025.
Future Actions	**May 2024 to March 2025:** • Monthly budget meetings scheduled to take place with BSO Finance to monitor expenditure; • Submission of monthly FMR to DoH Finance; • Financial reports to be presented to Business Team, A&RC and Council meetings; • Use of NIPEC Associates to be monitored to ensure that NIPEC's budget does not become over/under-committed; • Ensure all NIPEC staff are regularly updated and fully aware of the budget position.

RISK 3	Failure by NIPEC to have a sufficiently tested organisational Business Continuity Plan in place to support ongoing delivery of services, including in the event of a cyber-security attack that results in the unavailability of systems that facilitate HSC services.				
Impact Score	**3 (Moderate)**	**Risk Owner(s)**	**Chief Executive/SMT**	**Date Added to Register**	**2nd May 2023**
Likelihood Score	**2 (Unlikely)**	**Risk Appetite**	**Cautious**	**Target Date Action Completion**	**March 2025**
Current Classification	**Medium (6)**	**Category**	**Performance & Reputational**	**Target Score/ Classification**	**Low (4)**
Controls	• A Council approved Business Continuity Plan is in place. It is a 'live' document and is reviewed at least annually; • NIPEC Chief Executive and Head of Corporate Services have a hard copy list of contacts in order that they can contact Council members and staff in the event of a cyber-attack and keep them up to date; • All NIPEC staff have remote access and can work from home in the event that James House offices become unavailable; • Business Continuity and Cyber-security training provided to Council members and staff; • All staff are required to complete Cyber-security e-learning programme; • NIPEC/Regional ALBs continue to be represented on regional Cyber Programme by Head of ITS; • To mitigate potential absence which may impact achievement of objectives, two Senior Professional Officers nominated for significant professional projects, one as the lead and one to shadow.				
Gaps in Control	• Personal contact details for key NIPEC staff maintained by BSO not up to date; • Training not attended or up to date; • Potential delays in communication by BSO ITS.				

RISK 3	**Failure by NIPEC to have a sufficiently tested organisational Business Continuity Plan in place to support ongoing delivery of services, including in the event of a cyber-security attack that results in the unavailability of systems that facilitate HSC services.**
Sources of Assurance	• BSO ITS SLA including Cyber-security; • Head of BSO ITS Annual Report shared with Council members; • Internal Audits of Business Continuity Planning; • BSO Annual Governance Statement; • Testing of NIPEC Business Continuity Plan.
Gaps in Assurance	• Testing of NIPEC's Business Continuity Plan not completed in James House; • Report on testing of BSO Business Continuity Plan to Council.
Impact of Risk	**Business Objective: Finance & Governance** Inability to deliver an appropriate level of service to our service users in the event of any disruption resulting in potential performance issues and reputational damage.
Actions taken to date	**March 2024:** • Business Continuity training attended by NIPEC Senior Staff and Council members; • NIPEC agreed the Internal Audit Plan for 2024-25 which includes an audit of NIPEC's Business Continuity arrangements.

RISK 3	**Failure by NIPEC to have a sufficiently tested organisational Business Continuity Plan in place to support ongoing delivery of services, including in the event of a cyber-security attack that results in the unavailability of systems that facilitate HSC services.**
Future Actions	**May 2024 to March 2025:** • Review of NIPEC's Business Continuity Plan to be undertaken and approved by BTM and Council; • Personal contact details from Council members and staff to be kept up to date and saved in hard copy for the Chief Executive and Head of Corporate Services for use in the event of a cyber-attack on HSC; • Internal Audit of NIPEC's Business Continuity arrangements to be completed and recommendations implemented; • Desk-top test of the current Business Continuity Plan to be completed in James House; • Further Business Continuity training session to be arranged for November 2024 for Council and the senior team; • Assurance to be sought from BSO that they hold personal contact details for NIPEC in the event of a cyber- attack so that information can be shared as to how staff will be paid, invoices paid and other key services will operate; • NIPEC to seek an assurance report from BSO on Business Continuity testing.

RISK 4	**Risk to the HSC network and organisations in the event of a cyberattack on HSC or a supplier/partner or organisation resulting in the compromise of the HSC network and systems or the disablement of ICT connections and services to protect the HSC and its data. The impact and residual risk on the ability of NIPEC to continue to deliver services may result in the inability to deliver the corporate objectives set down by sponsor branch.** N.B Note that this is a regional risk adopted by all HSC organisations.				
Impact Score	4 (Major)	**Risk Owner(s)**	Chief Executive/SMT	**Date Added to Register**	**1st April 2021**
Likelihood Score	4 (Likely)	**Risk Appetite**	Cautious	**Target Date Action Completion**	**March 2025**
Current Classification	**High (16)**	**Category**	Performance & Reputational	**Target Score/ Classification**	**Medium (9)**
Controls	• Regional Cyber Boards chaired by BSO; • HSC Cyber programme Board NIPEC represented by head of ITS; • NIPEC representation on DOH led Information Governance Advisory Group; • Risk Management Framework; • Information Governance Processes & monitoring; • Emergency Planning & Service Business Continuity Plans; • BSO ITS Disaster Recovery Plan; • Change Control processes; • Data Protection legislation.				
Gaps in Control	• Regular cyber security reports from BSO; • NIPEC reliant on BSO ITS for management of cyber security.				

RISK 4	**Risk to the HSC network and organisations in the event of a cyberattack on HSC or a supplier/partner or organisation resulting in the compromise of the HSC network and systems or the disablement of ICT connections and services to protect the HSC and its data. The impact and residual risk on the ability of NIPEC to continue to deliver services may result in the inability to deliver the corporate objectives set down by sponsor branch.** N.B Note that this is a regional risk adopted by all HSC organisations.
Sources of Assurance	• BSO SLA for provision of ICT; • Contract Management and Reviews; • Data Access Agreements/Memorandum of Understanding; • Supplier / Partner Frameworks; • DoH Information Governance Advisory Group; • HSC Cyber programme Board - NIPEC represented by head of ITS; • BSO Annual Governance Statement; • Regional cyber security training; • ALB Forum briefings by Head of Cyber Security.
Gaps in Assurance	• Regular written reporting from BSO ITS on cyber security developments.
Impact of Risk	**Business Objective Governance & Performance** Causing disruption to services. Unauthorised access to NIPEC information resulting in a breach of regulatory compliance, statutory obligations, and the potential for fines in addition to resulting reputational damage.

RISK 4	**Risk to the HSC network and organisations in the event of a cyberattack on HSC or a supplier/partner or organisation resulting in the compromise of the HSC network and systems or the disablement of ICT connections and services to protect the HSC and its data. The impact and residual risk on the ability of NIPEC to continue to deliver services may result in the inability to deliver the corporate objectives set down by sponsor branch.** N.B Note that this is a regional risk adopted by all HSC organisations.
Actions taken to date	• Service Continuity Plans reviewed, updated and tested against the impact of a cyber incident; • HSC wide Incident Response test in June 2023 - 60 people in attendance (ALB's represented by BSO); • HSC Cyber Security Team rolled out on-line training in 2022-23 for all HSC staff. Continues 2023-24.
Future Actions	• DoH Information Governance Advisory Group to develop an IG management plan in the event of Cyber incident; • DoH Regional IG working group to be established to take forward the review of data flows from HSC/Partner organisations; • Supplier frameworks to include Security and IG clauses, risk assessment and security management plans completed and approved by BSO Programme Board; • Consider development and use of legally binding arrangements; • Identify actions to support Partner/ Supplier Cyber Incident Recovery Planning (draft protocol paper shared with NIPEC). Seek written, evidenced assurances from supplier / partner on the secure transfer and storage of HSC data; • Further assurances to be sought on the management of Information Security by BSO ITS as discussed at A&RC in February 2024.

RISK 5	NIPEC is unable to give assurance of full compliance with the legislative requirements of Public Sector Bodies Websites and Mobile Applications (No. 2) Accessibility Regulations 2018.				
Impact Score	**3 (Moderate)**	**Risk Owner(s)**	**Chief Executive/SMT**	**Date Added to Register**	**2nd May 2023**
Likelihood Score	**3 (Possible)**	**Risk Appetite**	**Cautious**	**Target Date Action Completion**	**March 2025**
Current Classification	**Medium (9)**	**Category**	**Performance & Reputational**	**Target Score/ Classification**	**Low (4)**
Controls	• BSO ITS SLA; • Hosting of NIPEC Corporate and Careers' Websites on WordPress Framework; • BSO ITS audit of WordPress Framework; • Accessibility Statement on websites; • Website Governance Group.				
Gaps in Control	• None identified.				
Sources of Assurance	• BSO ITS SLA; • Internal Audit advisory report 2023-24 – will be reported to A&RC.				
Gaps in Assurance	• Accessibility Audit of websites to ensure full compliance of Accessibility Legislation 2018.				

RISK 5	**NIPEC is unable to give assurance of full compliance with the legislative requirements of Public Sector Bodies Websites and Mobile Applications (No. 2) Accessibility Regulations 2018.**
Impact of Risk	**Business Objective Governance & Performance** NIPEC would not meet its legislative obligations within the Accessibility Regulations and Disability Discrimination Act. This could impact on NIPEC's ability to show good public governance.
Actions taken to date	**March/April 2024:** • NIPEC received an advisory report from Internal Audit reviewing the implementation of recommendations from the 2021-22 Internal Audit of Websites; • NIPEC's Careers' Website transfer to WordPress completed and the site made 'live.'
Future Actions	**May 2024 to March 2025:** • Internal Website & Media Group to continue to monitor governance of the 2 websites; • Implementation of recommendations from Internal Audit advisory report; • Commission an accessibility audit of the 2 websites and implement recommendations.

RISK 6	Failure by NIPEC to have an up to date suite of Policies may cause inconsistency and misinterpretation and may fail to comply with Regional Policies.				
Impact Score	**3 (Moderate)**	**Risk Owner(s)**	**Chief Executive/SMT**	**Date Added to Register**	**26th February 2024**
Likelihood Score	**2 (Unlikely)**	**Risk Appetite**	**Cautious**	**Target Date Action Completion**	**March 2025**
Current Classification	**Low (6)**	**Category**	**Performance & Reputational**	**Target Score/ Classification**	**Low (4)**
Controls	• Policy grid maintained and updated; • Policies grid presented to each Audit and Risk Committee for noting; • Reviewed Policies sent to Business Team, Audit and Risk Committee and Council for approval; • Policies reviewed and updated regularly by Head of Corporate Services/Business Manager in accordance with Regionally reviewed Policies.				
Gaps in Control	• BSO HR Polices delayed due to strike action and regional frameworks; • Demand on capacity within the Corporate Team.				
Sources of Assurance	• Policies grid presented to Audit and Risk Committee; • Mitigations placed against each Policy; • Extension to 7 HR Policies granted by Council in March 2025.				
Gaps in Assurance	• NIPEC reliant on BSO for updates on regional Policies; • Limited capacity in the Corporate Team.				

RISK 6	**Failure by NIPEC to have an up to date suite of Policies due to capacity and demand can cause confusion and may fail to comply with new laws and legislation.**
Impact of Risk	**Business Objective: Finance & Governance** Failure to update NIPEC's Policies when required may cause inconsistency and misunderstanding and failure to comply with current legislation and laws.
Actions taken to date	**March/April 2024:** • Council approved extension of 7 HR Policies for a year pending regional review.
Future Actions	**May 2024 to March 2025:** • Head of Corporate Services and Business Manager to continue to update Policies as and when required or when new guidance or legislation is released; • Policies grid to be presented to each Audit and Risk Committee for monitoring; • Continue to liaise with BSO HR for updates on regional Policies.

Appendix A

HSC Regional Risk Matrix – with effect from April 2013
(updated June 2016 and August 2018)

Risk Likelihood Scoring Table			
Likelihood Scoring Descriptors	**Score**	**Frequency (How often might it/does it happen?)**	**Time framed Descriptions of Frequency**
Almost certain	5	Will undoubtedly happen/recur on a frequent basis	Expected to occur at least daily
Likely	4	Will probably happen/recur, but it is not a persisting issue/circumstances	Expected to occur at least weekly
Possible	3	Might happen or recur occasionally	Expected to occur at least monthly
Unlikely	2	Do not expect it to happen/recur but it may do so	Expected to occur at least annually
Rare	1	This will probably never happen/recur	Not expected to occur for years

	Impact (Consequence) Levels				
Likelihood Scoring Descriptors	**Insignificant (1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Almost Certain (5)	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
Likely (4)	**Low**	**Medium**	**Medium**	**High**	**Extreme**
Possible (3)	**Low**	**Low**	**Medium**	**High**	**Extreme**
Unlikely (2)	**Low**	**Low**	**Medium**	**High**	**High**
Rare (1)	**Low**	**Low**	**Medium**	**High**	**High**

Appendix B

Setting the Risk Appetite

Risk appetite can be defined as the *"amount and type of risk that an organisation is prepared to seek, accept or tolerate."* ISO defines risk appetite as an *"organisation's approach to assess and eventually pursue, retain, take or turn away from risk".* The Senior Management Team is responsible for setting the organisational attitude regarding risk and the Council is responsible for determining whether the risk attitude is aligned with the best interests of the organisation. NIPEC defines the risk appetite of the organisation as the extent of exposure to risk that is judged tolerable for it. Risk Appetite can be classified in five common classifications:[1]

- **AVERSE**: Avoidance of risk and uncertainty is a key objective*;*
- **MINIMALIST**: Preference for ultra-safe business delivery options that have a low degree of inherent risk and may only have potential for limited reward*;*
- **CAUTIOUS**: Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward;
- **OPEN**: Willing to consider all options and choose the one that is most likely to result in successful delivery while also providing on acceptable level of reward;
- **HUNGRY**: Eager to be innovative and to choose options based on potential higher rewards (despite greater inherent risk).

[1] Adapted from *Managing your Risk Appetite – a Practitioner's Guide*, HM Treasury 2006

Appendix C

Types of risk

NIPEC has identified four types of risk that could affect the strategic business objectives of the organisation:

Financial: the risk that the budget agreed may be exceeded; and/or that there is poor value for money. Also, consideration of risks in regard to regularity and propriety of public funds;

Performance: the risk that the outcomes for an agreed programme may not be achieved;

Reputational: the risk that unwanted actions of a provider may bring themselves, the programme or NIPEC into disrepute;

Opportunity: the risk that NIPEC or the provider, because they have not assessed risks accurately and are risk averse, decide not to take a business opportunity and so damage their effectiveness.