NIPEC Corporate Risk Register 2025-26

1. Purpose of this report

The purpose of this report is to ask Audit & Risk Committee to review and approve Version 7 of the Corporate Risk Register 2025-26.

Risks which have been updated:

- Risk 1
- Risk 2
- Risk 3

Risk 3 pertaining to Business Continuity and Risk 5 relating to Accessibility Legislation 2018 have been removed from the Corporate Risk Register following Council approval on 3rd December 2025.

2. Action Required

Audit and Risk Committee are asked to approve Version 7 of the 2025-26 Corporate Risk Register.

RISK 1	NIPEC is unable to fully achieve its business objectives as stated in the NIPEC Business Plan 2025-26				
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 2026**
Current Classification	**High (16)**	**Category**	**Performance**	**Target Score/ Classification**	**Low**
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				
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 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 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 resources / availability of slippage to increase capacity if required; • Partial retirement of 3 members of staff commencing October; • Requests for NIPEC to assume the lead for additional projects will affect capacity and may result in us not being able to meet all of the objectives listed in the Business Plan.

Sources of Assurance

Source of Assurance	Type of Control	Line of Assurance*	Control Effectiveness**
Annual Report and Accounts	Detective	Third	
Mid-year Assurance Report	Detective	Third	
Performance Report against Business Plan/Professional Workplan to NIPEC Committees and Council	Detective	Second	
C Ex update to Council	Detective	Second	
Assurance Maps action plan and progress updates to Audit & Risk Committee	Detective	Second	
Annual Quality Report	Detective	Second	

** three lines model*
***RAG rating based on HM Treasury guidance*

Gaps in Assurance	None identified
Mitigating Actions taken to date	**March/April 2025:** • Meeting with CNO and officials on 20th March 2025 to discuss NIPEC's draft Business Plan 2025/26; • Draft budget prepared and mitigations in place in relation to challenges of forthcoming budget forecast; • Draft Business Plan 2025/26 presented to Professional & Business Committee and Council in March 2025 for approval; • Council approved draft sent to DoH Sponsor Branch for ratification. **May 2025:** • Senior Team structure workshop held on 7th May to discuss future staffing requirements and the achievement of Business Plan Objectives; • Business Plan 2025-26 approved by CNO and published on NIPEC's website. **June 2025:** • Completion of Senior Team's appraisals and personal development plans; • Audited 'Clean' Annual Report & Accounts 2024-25 approved by Audit and Risk Committee and Council in June 2025; **July 2025:** • Second senior team planning day took place on 1st July to look at future structures, facilitated by an external advisor; • Meeting took place with BSO HR to seek advice on plans for recruitment and restructuring following planning day. **September 2025:** • Chief Executive and Head of Corporate Services met with HSCLC facilitator to review the out workings of the review of structures and provide feedback. • Head of Corporate Services drafted a Band 7 JD/Spec for a new Professional Officer post and following feedback from nursing and midwifery colleagues, submitted to BSO HR for AFC matching.

	October 2025 • Business Planning day held with senior staff on 28th October to identify priorities for 2026/27. **November 2025** • Second Business Planning day held on 19th November to progress priorities for the Business Plan for 2026/27; • Chief Executive and Head of Corporate Services attended the Ground Clearing meeting with Chief Nursing Officer (CNO) and Sponsor Branch officials. As there were no significant issues to report the mid-year Accountability Review meeting with the Permanent Secretary and CNO was stood down. **December 2025** • Business and Professional Committee met on 28th November 2025 and reviewed the professional workplan, progress on objectives and NIPEC's Performance Management Framework. • The professional workplan and corporate objectives were reviewed at Council in December 2025. • Requisitions raised for two band 7 Professional Officers.
Future Actions	**January 2026 to March 2026:** • Recruitment of new Professional Officers' posts; • Appointment of Bank Staff to support capacity where appropriate subject to available funding; • Ongoing monitoring of progress objectives by BTM, PTM, Professional & Business Committee and Council; • Chief Executive to monitor progress of individual objectives at senior team 1:1 meeting; • Reporting of progress to Sponsor Branch, Ground Clearing & Accountability meetings; • Completion of Senior Team's appraisals and personal development plans.

RISK 2	Risk to NIPEC's ability to achieve financial breakeven due to a reduction in NIPEC's financial allocation for 2025-26				
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 2026**
Current Classification	**High (12)**	**Category**	**Performance & Reputational**	**Target Score/ Classification**	**Low (4)**
Impact of Risk	**Business Objective: Governance & Performance** 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.				
Controls	• Confirmation of flat cash allocation for 2025-26; • Controls to remain in place regarding discretionary non-pay spend; • Head of Corporate Services to continue to represent NIPEC at the quarterly DoH Finance Forum; • Restrictions in place regarding use of NIPEC's Associate list; • 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	• Potential request for further savings in 2025-26 from DoH;				

Sources of Assurance

Source of Assurance	Type of Control	Line of Assurance*	Control Effectiveness**
Reporting of financial position to Business Team, A&RC and Council	Detective	Second	
Presentation of Annual	Preventative	Third	

	Report and Accounts to Audit & Risk Committee and Council in June 2025;	Detective		
	Financial Management audit 2025-26	Detective	Third	
	Quarterly assurance from BSO Finance that all objectives in SLA carried out	Detective	Second	
	** three lines model* ***RAG rating based on HM Treasury guidance*			
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 2023-24
Mitigating actions taken to date	**March / April 2025:** • Preparation of a 2025-26 draft budget which was presented to Council in March 2025; • Regular updates to Senior Management Team and Business Team meetings; • Draft Annual Accounts 2024-25 submitted to DoH finance and NIAO for auditing. **May 2025:** • Budget position discussed at Ground Clearing meeting in May 2025; • Draft unaudited Annual Report and Accounts 2024/25 presented to Audit and Risk Committee in May 2025. **June 2025:** • Sign off of Annual Report and Accounts 2024-25 by Chair and Chief Executive. • Update on budget position provided to Audit and Risk Committee and Council. **July 2025** • Month 3 FMR submitted to DoH Finance with a projected breakeven position at year end. **August 2025** • Month 4 FMR submitted to DoH Finance with a projected breakeven position at year end. **September 2025:** • Discussion by Senior Team to introduce a scrutiny panel to agree expenditure in light of the DoF circular 19-2025 and the message from the DoH Finance Forum; • Month 5 FMR submitted to DoH Finance with a projected breakeven position at year end.

	October 2025: • Month 6 FMR submitted to DoH Finance with a projected breakeven position at year end; • Staff reminded at weekly meetings of the current budget position. **November 2025** • Month 7 FMR submitted to DoH Finance with a projected breakeven position at year end; • Staff reminded on budget position at Business Team meeting on 11th November and email reminder issued re embargo on non-essential spend. **December 2025** • Month 8 FMR submitted to DoH Finance with a projected breakeven position. • Staff reminded of the budget position at Business Team and at regular team briefings. • Financial report to Council in December 2025.
Future Actions	**January 2026 to March 2026:** • 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; • Ensure all NIPEC staff are regularly updated and fully aware of the budget position.

RISK 3	**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 2026**
Current Classification	**High (16)**	**Category**	Performance & Reputational	**Target Score/ Classification**	**Medium (9)**
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.				
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. • Introduction of Entra ID Password Protection across the HSC Network. • BSO Cybersecurity Strategy, Programme & Workplan (via ITS Regional Cyber Security Programme Board)				

- NIPEC Business Continuity Plan tested and updated in 2024/2025 with a focus on cyber security
- Regional IT Security/cyber security training is now mandatory for all staff
- HSC Supplier framework – to include Security and IG clauses, risk assessment and security management plans, approved by Cyber Security Programme Board in June 2022 now being implemented. (note: currently under review (Sept 25) but existing framework still in place)

Gaps in Control

- Regular cyber security reports from BSO;
- NIPEC reliant on BSO ITS for management of cyber security.

Sources of Assurance

Source of Assurance	Type of Control	Line of Assurance*	Control Effectiveness**
BSO SLA for provision of ICT	Preventative Detective	Second	
Contract Management and Reviews	Preventative Detective	Second	
Data Access Agreements/Memorandum of Understanding	Preventative	Second	
Supplier / Partner Frameworks	Preventative Detective	Second	
DoH Information Advisory Group	Preventative Detective	Second Third	
HSC Cyber programme Board - NIPEC represented by head of ITS	Preventative Detective	Second Third	
BSO Annual Governance Statement	Preventative Detective	Second	
Regional cyber security training	Preventative	First Second	
ALB Forum briefings by Head of Cyber Security	Preventative	Second	

** three lines model*
***RAG rating based on HM Treasury guidance*

RISK 3	**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.
Gaps in Assurance	• Regular written reporting from BSO ITS on cyber security developments.
Mitigating 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 2025.

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.