NIPEC Corporate Risk Register 2023-24

1. Purpose of this report

The purpose of this report is to provide Audit and Risk Committee with an update on version 5 of the Corporate Risk Register 2023-24.

All risks (1-5) have been updated following an in-depth discussion at NIPEC Council Workshop and meeting on 20th September 2023.

No new risks were identified. At the Council workshop members had queried whether risks 3 and 4 could be merged. Following further review by the Head of Corporate Services and Business Manager, who sought the advice of the BSO Head of Cyber Security, it was deemed that these two risks stand separately. However, Audit and Risk Committee are requested to reconsider this approach and approve a way forward.

2. NIPEC Audit and Risk Committee are asked to note the changes and approve version 5 of the 2023-24 Corporate Risk Register.

RISK 1	NIPEC is unable to fully achieve its business objectives as stated in the NIPEC Business Plan 2023-24.				
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 2024**
Current Classification	**Medium**	**Category**	**Performance**	**Target Score/ Classification**	**Low**
Controls	• Progress on corporate and professional objectives reviewed at monthly Business Team meetings and at quarterly Council and A&RC meetings; • Newly appointed Professional & Business Committee; • RAG rated workplan which is 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	• Continued recruitment challenges which will impact on projected spend for the year; • Inability to appoint staff due to the uncertainty over amount of slippage; • External factors, for example further reduction in allocation.				
Sources of Assurance	• Annual Report and Accounts; • Mid-year Assurance report and Assurance Maps; • Annual Quality report; • Performance Reports to NIPEC Council and Committees.				

RISK 1	NIPEC is unable to fully achieve its business objectives as stated in the NIPEC Business Plan 2023-24.
Gaps in Assurance	None identified.
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/May/June 2023:** • Senior planning days held to break down the objectives into phases and agree timelines for completion of each stage; • Available resources discussed and allocated to project leads; • Professional workshop took place in May with Council to provide assurance on annual workplan delivery; • May 2023: Draft Annual Report 2022-23 presented to Audit & Risk Committee; • June 2023: Completion of Senior Team's appraisals and personal development plans; • June 2023: Audited 'Clean' Annual Report & Accounts 2022-23 approved by Council.
Future Actions	**September 2023 – March 2024:** • Monitoring of progress on corporate and professional objectives at Business and Professional Team meetings, and quarterly Council and A&RC meetings; • Establishment of new Council Professional & Business Committee who will be responsible for scrutinising the draft Annual Business Plan and progress on objectives before providing updates to 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;

RISK 1	NIPEC is unable to fully achieve its business objectives as stated in the NIPEC Business Plan 2023-24.
	• Chief Executive Report, KPIs and Professional Workplan presented at each NIPEC Council meeting; • Presentation of individual NIPEC projects to Council meeting remains a standing agenda item; • Working together to increase capacity within current budget; • Seek to strengthen external partnerships with stakeholders; • Promote NIPEC as an attractive place to work through the Health and Wellbeing Committee; • Monitoring BSO SLA and involvement in development of revised SLA templates during 2023-24; • Create promotional opportunities for staff to support staff retention.

RISK 2	Risk to NIPEC's ability to achieve financial breakeven due to a reduction in NIPEC's financial allocation for 2023-24				
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 2023**
Current Classification	**Medium (6)**	**Category**	Performance & Reputational	**Target Score/ Classification**	**Low (4)**
Controls	• NIPEC prepared a 2023-24 budget inclusive of plans for a 5% reduction and presented to NIPEC Council in March 2023; • Monthly budget monitoring meetings with BSO to track expenditure; • Submission of monthly Financial Monitoring Return (FMR) to DoH Finance; • Close scrutiny / limiting use of NIPEC's bank list subject to funds being available; • BSO Annual Finance SLA.				
Gaps in Control	• Financial savings in the 2023-24 financial year; • Slippage incurred by delays in filling vacancies presents challenges with use of any surplus funds; • Ability to recruit and persuade applicants that NIPEC is a good place to work.				
Sources of Assurance	• Presentation of Annual Report and Accounts to Audit & Risk Committee; • Reporting of financial position to Business Team, A&RC and Council; • '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 2023-24
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	**March 2023:** • Preparation of a 2023-24 draft budget with implications of various savings scenarios included; • Draft budget approved by NIPEC Council at its March 2023 meeting. **April 2023:** • NIPEC received an opening allocation letter outlining a 5% reduction (£75k) in the opening allocation. In addition, as a result of indicative funding being less than anticipated for HSC, a further £50k have been sought and the allocation reduced accordingly. **May 2023:** • Month 1 FMR submitted to DoH Finance with a projected breakeven position; • Financial position included on agenda of Ground Clearing meeting. **June 2023:** • Head of Corporate Services attended DoH quarterly Finance Forum to receive an update on the HSC budget position; • Sign off of Annual Report and Accounts by Chair and Chief Executive. **July 2023** • Meeting with NIPEC's senior team to discuss and agree spend for associates with available funds.

RISK 2	Risk to NIPEC's ability to achieve financial breakeven due to a reduction in NIPEC's financial allocation for 2023-24
	August 2023 • Meeting with NIPEC's senior team took place and spend agreed for 2023/24 associates.
Future Actions	**September 2023 – March 2024:** • 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; • Promote NIPEC as an attractive place to work through organisational pathways of development and health and wellbeing opportunities.

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 2024
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; • Cyber-security training provided by BSO ITS 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.				
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; • 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	**December 2022:** • Business Continuity Plan ratified by Business Team and Council. **December 2022/January 2023:** • Personal contact details sought from Council members and staff 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. **August 2023** • Personal contact details of Council members and staff updated on a six-monthly basis.

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	**September/October 2023:** • NIPEC to review the BSO SLA and service offering for 2023-24 and ensure ITS emergency response plan updated; • Desk top test of the Business Continuity Plan to be completed in James House; **September/October 2023 (cont'd)**: • 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. **October 2023:** • Business Continuity Plan to be updated and presented to Council in December 2023; • Seek Business Continuity training for staff and Council members. **Ongoing:** • NIPEC Business Continuity Plan remains a 'live' document and will continue to be updated when required. • 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 2024
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; • 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.
	• Clarity on cyber security provision from BSO via the annual SLA.
Sources of Assurance	• Contract Management and Reviews; • Data Access Agreements/Memoranda 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 at ALB forum by cyber security programme manager.
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 a 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.

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 2024
Current Classification	**Medium (9)**	**Category**	Performance & Reputational	**Target Score/ Classification**	**Low (4)**
Controls	• BSO ITS SLA; • Hosting of NIPEC Corporate Website on WordPress Framework; • BSO ITS audit of WordPress Framework; • Accessibility Statement on websites; • Website Governance Group.				
Gaps in Control	• The Careers' Website is currently managed by a 3rd party supplier who do not use the WordPress Framework. This may lead to a 2-tier standard of Accessibility compliance.				
Sources of Assurance	• BSO ITS SLA; • Internal Audit report and implementation of recommendations – progress reported to A&RC.				
Gaps in Assurance	• 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	**February 2023:** • NIPEC Business Team considered a report prepared by HSC Leadership Centre outlining recommendations for the way forward in hosting the Careers' Website; • It was agreed that the site should be transferred to a BSO WordPress framework at the earliest opportunity; • NIPEC included an action in the Draft Disability and Equality Action Plans to carry out an accessibility audit of the two websites. **March 2023:** • Appointment of new Communications Officer who will lead management of the websites going forward. **May 2023:** • Head of Corporate Services issued commissioning letter to BSO ITS to request transfer of Careers Website to a BSO Word Press framework. **June 2023:** • Head of Corporate Services met with Internal Audit to agree date for 2-day advisory assignment.

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.
Future Actions	**September/October 2023:** • Final date to be agreed with BSO ITS to transfer the Careers' Website to BSO WordPress Framework; • 3rd Party supplier to be informed of the decision and SLA not renewed; • Appointment of Communications Manager on 6th October to take forward work on NIPEC website and social media channels; • Internal Website Governance Group to take this work forward. **October to December 2023:** • Accessibility audit of NIPEC's websites to be initiated. **January to March 2024:** • Internal Audit to carry out a 2-day advisory assignment on the implementation of the IT & Websites audit 2021-22.

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.