NIPEC Corporate Risk Register 2023-24

1. Purpose of this report

The purpose of this report is to provide Audit & Risk Committee with an update on the Corporate Risk Register 2023-24. At the Business Team meeting on 4th April 2023, the Corporate Risk Register 2022-23 was reviewed and discussion took place regarding which risks should be carried forward into 2023-24 and which should be closed. The following was agreed:

- Risks 1 & 2 should be retained;
- Risks 3 & 4 should be archived;
- Risks 5 & 7 should be merged;
- Risk 6 was a regional risk and should be retained;
- Risk 8 should be archived;
- Risk 9 should be kept;
- Risk 10 should be archived.

No new risks were identified.

2. Audit & Risk Committee are asked to note the changes and approve Version 1 of the 2023-24 Corporate Risk Register.

May 2023

Business Objective: Governance and Performance

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**	Open	**Target date for action completion**	March 2024
Current classification	**Medium (9)**	**Risk Category**	Performance		
Controls	• Progress on corporate and professional objectives reviewed at monthly Business Team meetings and at quarterly Council and A&RC meetings; • 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 meetings.				
Sources of Assurance	• Annual Report and Accounts; • Mid-year Assurance report; • Annual Quality report; • Performance Reports to NIPEC Council.				
Impact of Risk • **Gap in Control** • **Assurance**	**Business Objective: Governance & Performance** Failure to achieve objectives could result in the organisation being unable to demonstrate that it has robust performance and governance frameworks in place and how it made best use of its resources causing reputational damage to the organisation. It may also limit opportunities to participate in other areas of work.				

Actions taken to date	**April & May 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 leads. Professional workshop to take place with Council to provide assurance on annual workplan delivery.
Future Actions	**April 2023 – March 2024:** • Monitoring of progress on corporate and professional objectives at Business and Professional Team meetings, and quarterly Council and A&RC meetings. • Chief Executive to monitor progress of individual objectives at senior team 1:1 meetings. • Reporting of progress to Sponsor Branch, Ground Clearing & Accountability meetings.

Business Objective: Governance and Performance

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 for action completion**	March 2024
Current classification	**Medium (6)**	**Risk Category**	Performance & Reputational		
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; • Suppression of one vacancy and close scrutiny / limiting use of NIPEC's bank list.				
Sources of Assurance	• Reporting of financial position to Business Team, A&RC and Council; • 'Clean' Annual Accounts for 2023-24.				
Impact of Risk • **Gap in Control** • **Assurance**	**Business Objective: Finance & Governance** Failure to achieve financial breakeven would impact NIPEC's financial governance arrangements and reputation and would lead to a 'limited' set of accounts.				

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.
Future Actions	**May 2023 – March 2024:** • Monthly budget meetings 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-committed.

Business Objective: Governance and Performance

RISK 3: Failure to effectively implement NIPEC's Business Continuity Plan 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 for action completion**	March 2024
Current classification	**Medium (6)**	**Risk Category**	Performance & Reputational		
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; • NIPEC/Regional ALBs continue to be represented on regional Cyber Programme by Head of ITS.				
Sources of Assurance	• BSO ITS SLA including Cyber-security; • BSO Governance Statement; • Testing of NIPEC Business Continuity Plan.				
Impact of Risk • **Gap in Control** • **Assurance**	**Business Objective: Governance & Performance** Unauthorised access to NIPEC information resulting in a breach of regulatory compliance, statutory obligations, and the potential for fines in addition to reputational damage. Inability to deliver an appropriate level of service to our service users in the event of any disruption resulting in potential performance 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 by the Chief Executive and Head of Corporate Services for use in the event of a cyber-attack on HSC.
Future Actions	**May 2023:** • NIPEC to review the BSO SLA and service offering for 2023-24 and ensure ITS emergency response plan updated. **September/October 2023**: • Desk top test of the Business Continuity Plan to be completed; • 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. **Ongoing:** NIPEC Business Continuity Plan remains a 'live' document and will continue to be updated when required.

Business Objective: Governance and Performance

RISK 4: Risk to the HSC network and organisations in the event of a cyberattack on a supplier or partner 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 the HSC to continue to deliver services to Patients / service users / Customers, compromise or loss of personal and organisational information, and loss of public confidence. **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 for action completion**	March 2024
Current classification	**High (16)**	**Risk Category**	Performance & Reputational		
Controls	• 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; • Regional Cyber Boards.				

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.
Impact of Risk • **Gap in Control** • **Assurance**	**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.
Action taken to date	• Service Continuity Plans reviewed, updated and tested against the impact of a cyber incident; • HSC Cyber Security Team rolled out on-line training in 2022-23 for all HSC staff.
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; • Consider development and use of legally binding arrangements; • Identify actions to support Partner/ Supplier Cyber Incident Recovery Planning: • Seek a technical report on recovery actions undertaken by the partner/ supplier and consider against known best practice; • Seek written, evidenced assurances from supplier / partner on the secure transfer and storage of HSC data.

Business Objective: Governance and Performance

<table>
<tr><td colspan="6">RISK 5: NIPEC may not be fully compliant with the legislative requirements of Public Sector Bodies Websites and Mobile Applications (No. 2) Accessibility Regulations 2018.</td></tr>
<tr><td>Impact Score</td><td>3 (Moderate)</td><td>Risk Owner(s)</td><td>Chief Executive/SMT</td><td>Date added to register</td><td>2nd May 2023</td></tr>
<tr><td>Likelihood Score</td><td>3 (Possible)</td><td>Risk Appetite</td><td>Cautious</td><td rowspan="2">Target date for action completion</td><td rowspan="2">March 2024</td></tr>
<tr><td>Current classification</td><td>Medium (9)</td><td>Risk Category</td><td>Performance & Reputational</td></tr>
<tr><td>Controls</td><td colspan="5">• BSO ITS SLA;
• Hosting of NIPEC Corporate Website on WordPress Framework;
• BSO ITS audit of WordPress Framework;
• Accessibility Statement on websites.</td></tr>
<tr><td>Sources of Assurance</td><td colspan="5">• BSO ITS SLA;
• Internal Audit report and implementation of recommendations – progress reported to A&RC.</td></tr>
<tr><td>Impact of Risk
• Gap in Control
• Assurance</td><td colspan="5">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 and could also lead to possible investigation and legal action by ECNI.

Gap 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.</td></tr>
</table>

Action 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.
Future Actions	**April / May 2023:** • A 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. **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.