

NIPEC Corporate Risk Register 2025-26

1. Purpose of this report

The purpose of this report is to ask Audit & Risk Committee to review version 1 of the Corporate Risk Register 2025-26. This was approved by NIPEC's Business Team on 6th May 2025.

All risks from 2024-25 have transferred into this version.

2. Action Required

The Audit & Risk Committee are asked to approve Version 1 of the 2025-26 Corporate Risk Register.

BUSINESS OBJECTIVE

GOVERNANCE AND PERFORMANCE

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	2 nd 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
Controls	<ul style="list-style-type: none"> Progress on corporate and professional objectives are reviewed by Council and the senior team as follows: <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Limited resources / availability of slippage to increase capacity if required; 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. 				

BUSINESS OBJECTIVE

GOVERNANCE AND PERFORMANCE

Sources of Assurance	<ul style="list-style-type: none"> • Annual Report and Accounts; • Mid-year Assurance report; • Internal Audits; • Assurance Maps and Action Plan update to Audit and Risk Committee; • Annual Quality report; • Performance Reports against Business Plan / Professional Workplan to NIPEC Council and Committees; • CEX update report to Council.
Gaps in Assurance	<ul style="list-style-type: none"> • Prioritisation of Projects for the 2025-26 year
Impact of Risk	<p>Business Objective: Governance & Performance</p> <p>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.</p>
Actions taken to date	<p><u>March/April 2025:</u></p> <ul style="list-style-type: none"> • Meeting with CNO and officials on 20th March 2025 to discuss NIPEC's draft Business Plan 2024/25; • 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.
Future Actions	<p><u>May 2025 to March 2026:</u></p> <ul style="list-style-type: none"> • Ongoing monitoring of progress objectives by BTM, PTM, Professional & Business Committee and Council; • Monthly monitoring of budget and using slippage where available to increase capacity; • Chief Executive to monitor progress of individual objectives at senior team 1:1 meeting; • Reporting of progress to Sponsor Branch, Ground Clearing & Accountability meetings; • Senior planning day to be arranged to prioritise / weight projects; • Completion of Senior Team's appraisals and personal development plans.

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 2025-26					
Impact Score	4 (Major)	Risk Owner(s)	Chief Executive/SMT	Date Added to Register	2 nd 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)
Controls	<ul style="list-style-type: none"> Confirmation of flat cash allocation for 2025-26; NIPEC have prepared a draft 2025-26 budget based on confirmed allocation; Controls to remain in place regarding discretionary non-pay spend; 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	<ul style="list-style-type: none"> Potential request for further savings in 2025-26 from DoH 				
Sources of Assurance	<ul style="list-style-type: none"> Reporting of financial position to Business Team, A&RC and Council; Presentation of Annual Report and Accounts to Audit & Risk Committee and Council in June 2025; Financial Management audit 2025-26; Quarterly assurance from BSO Finance that all objectives in SLA carried out. 				
Gaps in Assurance	None identified.				

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 of Risk	<p>Business Objective: Finance & Governance</p> <p>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.</p>
Actions taken to date	<p><u>March / April 2025:</u></p> <ul style="list-style-type: none"> • 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.
Future Actions	<p><u>May 2025 to March 2026:</u></p> <ul style="list-style-type: none"> • 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.

BUSINESS OBJECTIVE

GOVERNANCE AND PERFORMANCE

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	2 nd May 2023
Likelihood Score	2 (Unlikely)	Risk Appetite	Cautious	Target Date Action Completion	March 2026
Current Classification	Medium (6)	Category	Performance & Reputational	Target Score/Classification	Low (4)
Controls	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 in the event of a cyber security attack on HSC. 				

BUSINESS OBJECTIVE

GOVERNANCE AND PERFORMANCE

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	<ul style="list-style-type: none"> • Internal Audit 2024-25 of NIPEC's Business Continuity Planning arrangements – satisfactory assurance received; • BSO ITS SLA including Cyber-security; • Head of BSO ITS Annual Report shared with Council members; • BSO Annual Governance Statement presented to Audit and Risk Committee; • Testing of NIPEC Business Continuity Plan.
Gaps in Assurance	<ul style="list-style-type: none"> • Reports from BSO on their Business Continuity testing and outcome/mitigations for Audit & Risk Committee; • Arrangements for BSO to contact NIPEC in the event of a cyber-attack not in place; • Lack of clarity on arrangements for Payroll, HR, IT and Payments' services (all BSO) in the event of a cyber-attack on HSC.
Impact of Risk	<p>Business Objective: Finance & Governance</p> <p>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.</p>
Actions taken to date	<p><u>March 2025/ April 2025</u></p> <ul style="list-style-type: none"> • Escalated correspondence and dialogue between NIPEC and BSO to raise the matter around gaps in assurance from BSO. Time for implementation estimated end June 2025; • HoCS attended annual SLA review with BSO ITS and raised issues around gaps in assurances; • Paper presented to Council in March detailing an update on the assurances from BSO on Business Continuity and the plan for the desktop test exercise.

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	<p><u>May 2025 to March 2026:</u></p> <ul style="list-style-type: none"> • Desk-top test of the current Business Continuity Plan to be completed in James House on 6th May 2025 and any amendments made to the Plan; • 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 follow up with BSO to seek more detailed assurances on Business Continuity testing; • Request for personal contact details from Council members and staff to be issued to ensure these are 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; • Recommendations from Internal Audit of NIPEC's Business Continuity arrangements to be completed and reported to the Audit & Risk Committee.

BUSINESS OBJECTIVE

GOVERNANCE AND PERFORMANCE

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	1 st 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)
Controls	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 2025.

BUSINESS OBJECTIVE

GOVERNANCE AND PERFORMANCE

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	2 nd May 2023
Likelihood Score	3 (Possible)	Risk Appetite	Cautious	Target Date Action Completion	March 2026
Current Classification	Medium (9)	Category	Performance & Reputational	Target Score/Classification	Low (4)
Controls	<ul style="list-style-type: none"> BSO ITS SLA; Hosting of NIPEC Corporate and Careers' Websites on WordPress Framework; Upgrades of WordPress Framework carried out between January and March 2025; BSO ITS audit of WordPress Framework; Accessibility Statement on websites; NIPEC Website Governance Group. 				
Gaps in Control	<ul style="list-style-type: none"> None identified 				
Sources of Assurance	<ul style="list-style-type: none"> BSO ITS SLA; Internal Audits. 				
Gaps in Assurance	<ul style="list-style-type: none"> None identified 				

BUSINESS OBJECTIVE

GOVERNANCE AND PERFORMANCE

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	<p>Business Objective Governance & Performance</p> <p>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.</p>
Actions taken to date	<p><u>March/April 2025:</u></p> <ul style="list-style-type: none"> • Work is finalised on the update of NIPEC's website (including upgrades to the WordPress Framework) and the new NIPEC website went live in March 2025; • Work is on-going with HSC and other disability users testing the website and an update on outcomes will be reported to Council in June 2025.
Future Actions	<p><u>May 2025 to March 2026:</u></p> <ul style="list-style-type: none"> • Upgrade and updates to the Careers' website has been commissioned from BSO ITS; • Internal Website & Media Governance Group to continue to monitor governance of the 2 websites.

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. |