

This log is used to record and track NIPEC Corporate Risks for 2021-2022

Risks are things that may or may not happen in the future that could have an effect on the organisation's success. This log includes all risks identified, including those that have passed and are no longer a threat, those that have been prevented or mitigated, and those that have become closed. As this is a permanent record of NIPEC's risks, no risk information is deleted from this log:

Version 3 - June 2021

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective: Governance & Performance R1	NIPEC fails to achieve the financial breakeven target of 0.25% or £20k (whichever is the greater) of its revenue allocation. This would result in the organisation being in breach of its Revenue Resource Limit (RRL) and may result in a Limited Assurance from External Audit (NIAO) at financial year end.	CE and HCS	1 st April 2021	20th June 2021	Business Objective: Governance & Performance NIPEC would not meet the financial target of containing net expenditure within the DoH target i.e. 0.25% or £20k. This would impact on NIPEC's ability to demonstrate robust governance processes and may result in a Limited Assurance on year end Accounts.	3 (Moderate)	2 (Unlikely)	6 (M)	<u>June 2021:</u> Completion of budget build for 2021-22. <u>April 2021:</u> Completion and submission of annual accounts to NIAO. <u>April 2021:</u> Finalisation of Month 12 accounts for 2020-21 and preparation of annual accounts and	<u>June 2021:</u> External Audit of annual accounts by PWC on behalf of NIAO. <u>June/July 2021:</u> Sign off of 2020-21 annual accounts by NIAO and laying of accounts in the NI Assembly. <u>June 2021 – March 2022:</u> Monthly budget meeting with BSO Finance to prepare and	Open Risk is currently being managed on an ongoing basis.

										report.	submit monthly FMR to DoH Finance.
										Confirmation of Resource Budget Opening Allocation from DoH.	Monthly budget reporting to Business Team meetings by HCS.
											Discussion at one to one meetings between CE and HCS.
											Quarterly reporting to and monitoring by NIPEC Council and Audit & Risk Committee meetings.

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective: Governance & Performance R2	NIPEC is unable to fully achieve its business objectives as stated in the NIPEC Business Plan 2021-22.	Senior Management Team	1st April 2021	20th June 2021	Business Objective: Governance & Performance This 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.	3 (Moderate)	2 (Unlikely)	6 (M)	<u>June 2021:</u> CNO continues to consider objectives to be prioritised and will respond when appropriate. A range of objectives continue to be delivered. <u>May 2021:</u> CEX discussed draft BP with Sponsor Branch and work objectives were identified to CNO for the year ahead. CNO and team to consider same and respond to NIPEC to identify which areas they would wish the organisation to prioritise during 2021-22.	<u>April 2021 – March 2022:</u> Monitoring of progress on objectives at monthly BTM and quarterly Council and A&R meetings. Progress update on Workplan to quarterly Council meetings. Progress updates on individual PDPs at senior team 1:1 meetings with CE. Regular meetings with SB including Ground Clearing & Accountability meetings.	Open Risk is currently being managed on an ongoing basis.

										<p>March 2021: Draft Business Plan 2021-22 presented to and approved by NIPEC Council and submitted to Sponsor Branch.</p>		
--	--	--	--	--	--	--	--	--	--	--	--	--

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective: Governance & Performance R3	The delay in advertising for new members to NIPEC Council could have an impact on the Governance of the organisation if appointments are not made in a timely manner.	Chair of Council	1 st April 2021	20th June 2021	Business Objective: Governance & Performance Impact on quorum at meetings may result in decisions not being made due to insufficient numbers. Therefore could raise issues in regard to organisational governance, performance and reputation.	4 (Major)	4 (Likely)	12 (H)	<u>May 2021:</u> Issue discussed at A&R Committee; Sponsor Branch rep.in attendance agreed to follow up again with PAU as a matter of urgency. <u>April 2021:</u> Upcoming NIPEC Council vacancies listed in April 2021 edition of Public Appointments Newsletter. <u>February 2021:</u> PAU confirmed	<u>June 2021:</u> Sponsor Branch to advise if members are to be offered further extensions to their terms subject to the approval of Public Appts Commissioner. DoH Public Appointments Committee to confirm timeline for public appointments competitions for 2021. NIPEC Chair will continue to liaise with DoH Sponsor Branch re progress of PAU competition. This may be	Open Risk is currently being managed on an ongoing basis.

										Ministerial approval for extension of terms for Chair and 2 non-executives to Sept 2021.	delayed due to the Covid-19 emergency response.	
--	--	--	--	--	--	--	--	--	--	--	---	--

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective Governance & Performance R4 	Risk of potential disruption to NIPEC service delivery due to turnover of corporate staff.	CE and Senior Management Team	1st April 2021	20th June 2021	Business Objective Governance & Performance - 5D This could impact on NIPEC's ability to deliver on objectives while interim arrangements are put in place and recruitment processes are completed.	4 (Major)	3 (Likely)	12 (H)	<u>June 2021:</u> Recommendations on the way forward approved by NIPEC Senior Team and shared with NIPEC JNCC. <u>April/May 2021:</u> Report produced including recommendations on corporate structure. If changes in corporate structure recommended, NIPEC to enter change management process in consultation with staff, trade unions and HR. <u>December 2020:</u> Scoping exercise	<u>June 2021:</u> Subject to response from JNCC to recommendations on way forward, proposals to be shared with Corporate Team. <u>July to December 2021:</u> Recruitment & appointment to vacancies Interim appointments to be put in place to cover gaps including use of NIPEC Bank and Agency staff.	Open Risk is currently being managed on an ongoing basis.

commenced to review the corporate structure and ensure it remains fit for purpose. Staff engagement completed in February 2021 and JNCC informed.

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective Governance & Performance R5 	Chief Executive secondment from DoH is in place up to 30 th June 2021 and needs to be reviewed.	NIPEC Chair / Sponsor Branch	1st April 2021	24th May 2021	Business Objective Governance & Performance - 5D A delay in extending the secondment could lead to NIPEC not having an Accounting Officer in place and may have governance and performance implications for the organisation.	4 (Major)	2 (Unlikely)	8 (H)	<u>May 2021:</u> Confirmation of extension received. <u>April/May 2021:</u> Sponsor Branch to put in place arrangements for extension. <u>April 2021:</u> Extension of secondment has been sought by NIPEC Chair.		Closed Successfully mitigated.

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective: Governance & Performance R6	Risk of a cyber security breach that results in the unavailability of systems that facilitate HSC services. See also Risk 12	BSO Director CCP / Head of BSO ITS & NIPEC SMT	1 st April 2021	20th June 2021	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.	4 (Major)	3 (Possible)	12 (H)	<u>June 2021:</u> NIPEC received annual assurance from BSO CEX in the form of BSO Draft Governance Statement. This included detail of a prioritised Cyber Security Programme to address a gap analysis against ISO 27001 and confirmation of significant levels of investments in technology and services to protect the HSC network.	<u>July 2021 onwards:</u> NIPEC to collaborate with BSO ITS to ensure implementation of Internal Audit recommendations including review of SLA and provision of bespoke assurances to NIPEC on services delivered including Cyber Security. <u>Ongoing:</u> NIPEC/ALBs continue to be represented on regional Cyber Programme by Head of ITS.	Open Risk is currently being managed on an ongoing basis.

											<p><u>May/June 2021:</u> HCS continued to engage with regional SIRO Group to monitor impact of the cyber attacks on HSCNI.</p> <p><u>May 2021:</u> Notification of further data breach in HSE and DoH, ROI, which may impact HSC. All emails to HSE suspended and further mitigations being managed by SIROs.</p> <p><u>March 2021:</u> NIPEC received notification of a cyber security breach at QUB which may have an impact on HSCNI systems. HCs attended a number of regional SIRO / IG meetings in March & April to discuss potential mitigations including temporary</p>	
--	--	--	--	--	--	--	--	--	--	--	---	--

										cessation of emails between HSCNI and QUB until further assurance provided by QUB on the extent of the breach.	
--	--	--	--	--	--	--	--	--	--	--	--

2. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective: Governance & Performance R7	Risk of failure to have a sufficiently tested organisational response to a cyber incident/attack, and recovery plan to support ongoing delivery of services.	BSO Director CCP / Head of BSO ITS & NIPEC SMT	1 st April 2021	20th June 2021	Business Objective: Governance & Performance 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.	4 (Major)	2 (Unlikely)	8 (H)	<u>June 2021:</u> NIPEC received annual assurance from BSO CEX in the form of BSO Draft Governance Statement. This included detail of a prioritised Cyber Security Programme to address a gap analysis against ISO 27001 and confirmation of significant levels of investments in technology and services to protect the HSC network. <u>May 2021:</u> BTM approved draft BCP. <u>April 2021:</u>	<u>June 2021:</u> Draft Business Continuity Plan to be presented to Council for approval. Ongoing: Continual review of BCP in line with regional response to Cyberattacks on HSC.	Open Risk is currently being managed on an ongoing basis.

									Review of NIPEC Business Continuity Plan and Emergency Planning arrangements.		
--	--	--	--	--	--	--	--	--	--	--	--

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective Governance & Performance R8	<p>Risk of the Online Portfolio and Careers Websites being housed on an unsupported BSO server.</p> <p>This could lead to a data breach (Online Portfolio) as Personal Identifiable Information of 4000 registrants is stored on this site.</p> <p>Removing access in the event of a risk would mean neither was available to registrants. The online portfolio stores registrant data which may be needed for revalidation, a regulatory requirement of the professional regulator</p>	CE and Senior Management Team	1 st April 2021	20th June 2021	<p>Business Objective Governance & Performance - 5D</p> <p>In the event of a data breach, this would have serious consequences for NIPEC in terms of financial costs of a fine by ICO and reputational and for individuals who might be impacted.</p> <p>Any disruption to availability of either of the sites would result in potential performance and reputational damage.</p>	4 (Major)	2 (Unlikely)	8 (H)	<p><u>June 2021:</u> HoCS met with ITS Performance & Customer Care Manager to discuss issues with SLA including hosting of secure websites, compliance with Accessibility Regulations, NIPEC audit of websites, general issues with the SLA and lack of responsiveness on occasion to NIPEC correspondence.</p> <p><u>April/May 2021:</u> Internal Audit carried out a review of</p>	<p><u>June 2021 onwards:</u> NIPEC to collaborate with BSO ITS to take forward IA findings including requirement to store personal data and how security can be strengthened after the migration to the new servers.</p> <p>BSO ITS Performance & Customer Care Manager to provide progress update on Accessibility audit and transfer of Online Portfolio</p>	Open Risk is currently being managed on an ongoing basis.

								<p>NIPEC IT arrangements including websites and SLAs.</p> <p><u>April 2021:</u> ITS identified a potential new server and agreed to liaise with Aurion (developer) requesting their assistance to transfer to this server. HCS requested a meeting with ITS senior management to clarify the position and agree a way forward on the management of the sites and NIPEC SLA.</p> <p><u>March 2021:</u> Contact made with ITS regarding the broken links which alerted to the issue. Assurance sought on the level of risk of the sites being hacked, securing the sites and agreement on a way forward to move both sites to a secure server. ITS server</p>	to new server.
--	--	--	--	--	--	--	--	---	----------------

										team implemented patching as a temporary measure and confirmed that the data and sites remain reasonably secure and at low risk.		
--	--	--	--	--	--	--	--	--	--	--	--	--

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective Governance & Performance R9	NIPEC fails to meet the legislative requirements of Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 . This could result in the organisation being in breach of these regulations and subject to investigation by Government Digital Service (GDS). Could also result in the organisation being in breach of the Disability Discrimination Act 1995 and subject to investigation by ECNI.	CE and Senior Management Team	1 st April 2021	20th June 2021	Business Objective Governance & Performance - 5D 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. This could also lead to possible investigation and legal action by ECNI. The resource required to carry out an audit and undertake remedial action as a result of findings is currently not known.	3 (Moderate)	5 (Almost Certain)	15 (H)	<u>June 2021:</u> HoCS met with ITS Performance & Customer Care Manager to discuss issues with SLA including hosting of websites, compliance with Accessibility Regulations, NIPEC audit of websites, general issues with the SLA and lack of responsiveness on occasion to NIPEC correspondence. <u>April/May2021</u> Internal Audit completed review of NIPEC IT arrangements	<u>June 2021 onwards:</u> NIPEC to collaborate with BSO ITS to take forward IA findings including requirement to store personal data and how security can be strengthened after the migration to the new servers. BSO ITS Performance & Customer Care Manager to provide progress update on ITS Accessibility audit and transfer of Online Portfolio	Open Risk is currently being managed on an ongoing basis.

										including websites and SLAs.	to new server.	
										<u>March 2021:</u> HCS sought update from ITS progress on the audit of the Word Press themed template.		
										CE & HCS reported to NIPEC Council on current position.		

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective Governance & Performance R10	NIPEC fails to review its current process and implement a documented approvals process for policies and procedures. This could result in some policies & procedures not being formally ratified by the relevant NIPEC Committee.	CE and Senior Management Team	1st April 2021	20th June 2021	Business Objective Governance & Performance - 5D This could impact on NIPEC's ability to maintain a robust governance and accountability framework.	3 (Moderate)	2 (Unlikely)	6 (M)	<u>December to June 2021:</u> NIPEC to process the 41 policies identified in the audit of policy approvals. All are being approved by BTM and Council or Audit & Risk Committee.	<u>June to August 2021:</u> Approval of remaining Policies to be completed. <u>September 2021:</u> Timeline to be agreed for rollout of procedures review.	Open Risk is currently being managed on an ongoing basis.

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective Governance & Performance R11	Risk of lack of /or insufficient support from BSO HR SLA.	CE and Senior Management Team	1st April 2021	20th June 2021	Business Objective Governance & Performance - 5D This could impact on NIPEC's ability to take forward recruitment overall and more especially, implement the findings of the corporate team scoping exercise and fill vacancies in a timely manner. It could also more broadly affect NIPEC's adherence to governance and contractual requirements.	3 (Moderate)	3 (Possible)	9 (M)	<u>June 2021:</u> CEX and HoCS met with BSO Directors of Finance & Customer Care for annual SLA meeting. Highlighted concerns around the HR SLA. <u>June 2021:</u> BSO Service Offering issued. Within the offering HR stated that a review of their SLA has highlighted services that are currently provided which are not covered under	<u>June/July 2021:</u> BSO Directors of Finance & Customer Care to discuss NIPEC concerns with Director of HR and report back to NIPEC. Should delays in requests for support occur these will be reported through to CE and escalated to Director of HR and/or BSO CE if required. Sponsor Branch will be kept informed.	Open Risk is currently being managed on an ongoing basis.

the SLA.
During 21/22
the activity in
these services
will be
monitored to
determine
impact on
future SLAs.
**No further
detail
received on
which
services are
referred to.**

April 2021:
HCS met with
Director of HR
for annual
SLA review
meeting;
concerns
discussed
including level
and cost of
service.
HCS asked
for a
breakdown of
services
provided for
the annual
SLA charge.

March 2021:
HCS met with
HR Business
Partner March
2021 to
discuss
issues
concerning
the SLA and
support going
forward.

1. BASIC RISK INFORMATION					2. RISK ASSESSMENT INFORMATION				3. RISK RESPONSE INFORMATION		
Risk Number	Risk Description / Risk Event Statement	Responsible	Date Reported day-month-year	Last Update day-month-year	Impact Description	Impact Score	Probability Score	Level of Risk	Completed Actions	Planned Future Actions	Risk Status Open / Closed
Provide a unique identifier for risk	A risk event statement states (i) what might happen in the future and (ii) its possible impact on the organisation.	Name or title of team member responsible for risk	Enter the date the risk was first reported	Enter the date the risk (not the entire log) was updated	List the specific impact the risk could have on the financial, Performance, Reputational or Opportunity.	Enter here the score according to impact definitions	Enter here the score according to likelihood definitions	Enter here the cum. score i.e. (L) Low; (M) Medium (H) High or (E) Extreme	List, by date, all actions taken to respond to the risk. This does not include assessing the risk	List, by date, what will be done in the future to respond to the risk	State if the risk is open (still might happen and still has to be managed); closed (has passed or has been successfully mitigated).
Business Objective Governance & Performance R12	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.	CE and Senior Management Team	1st April 2021	20th June 2021	Business Objective Governance & Performance - 5D 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.	4 (Major)	4 (Likely)	16 (H)	Controls: <ul style="list-style-type: none"> IGAG; Risk Management Framework; IG Processes & monitoring; Emergency Planning & Service Business Continuity Plans; Disaster Recovery Plan; Change Control processes; Data Protection legislation; Regional Cyber Boards. Sources of Assurance:	Actions to address Gaps in Control / Assurance: <p>Service Continuity Plans to be reviewed, updated and testing against the impact of a cyber incident;</p> <p>IGAG to develop an IG management plan in the event of a Cyber incident;</p> <p>Regional IG working group to be established to take forward the review of data flows from HSC/Partner organisations;</p>	Open Risk is currently being managed on an ongoing basis.

See also Risk 6

- Contract Management and Reviews;
- DAA/MOU;
- Supplier / Partner Framework;
- Information Governance Advisory Group
- Cyber programme Board

Supplier framework – to include Security and IG clauses, risk assessment and security management plans;

Consider development and use of legally binding arrangements;

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.