



# Annual Report on Risk Management 2024/2025

and

## Action Plan for 2025/26

### *Governance and Audit Committee (GAC) Report*

*Directorate of Strategic Planning & Customer Engagement*  
ELT Approval: 08/05/25  
GAC Approval: 20/05/25

## Contents

<b>1. Purpose of the Report</b>	<b>1</b>
<b>2. BSO Risk Management Process</b>	<b>1</b>
<b>2.1 Key Updates</b>	<b>1</b>
<b>2.2 BSO Risk Outputs Delivered</b>	<b>5</b>
<b>2.3 Corporate Objectives</b>	<b>6</b>
<b>2.4 Reporting</b>	<b>7</b>
<b>2.5 Information Governance</b>	<b>8</b>
<b>3.0 Risk Management Framework 2024/25</b>	<b>8</b>
<b>4.0 Information Governance Risk</b>	<b>9</b>
<b>5.0 Update on 2024/25 Action Plan</b>	<b>10</b>
<b>6.0 Risk Management Action Plan 2025/26</b>	<b>10</b>
<b>7.0 BSO Accreditations</b>	<b>11</b>
<b>8.0 Conclusion</b>	<b>11</b>
<b>9.0 Recommendation</b>	<b>11</b>
<b>Appendix 1: Risk Management Standard Action Plan 2025/26</b>	<b>12</b>

## 1. Purpose of the Report

The purpose of this report is to provide assurance to the Governance and Audit Committee (GAC) and the Board that the Business Services Organisation (BSO) has a risk management system in place which meets Northern Ireland Health and Social Care and other requirements in respect of the management of risks. In addition, this report provides:

- An outline of BSO risk management activity during 2024/25; and
- An action plan for risk management for 2025/26.

## 2. BSO Risk Management Process

BSO is required to have an approved policy for managing risk that identifies accountability arrangements, resources available and contains guidance on what may or may not be regarded as acceptable risk within the organisation.

The BSO Risk Management Process (Policy) was approved by the Board in August 2009 and is supported by a BSO Risk Management Strategy, which establishes a consistent and integrated approach to risk management in BSO. This Strategy is in line with a number of audit findings and recommendations, as well as amendments to the Standing Orders and Standing Financial Instructions.

BSO is delivering an effective system of risk management within a robust framework. The updated Risk Management Strategy for 2025/29 has been reviewed and revised to ensure best practices and good governance arrangements are in place throughout the organisation. In doing so, the risk management process supports identifying, managing and mitigating against risks in all aspects of BSO. The Strategy has been developed to reflect the principles set out in the Northern Ireland Audit Office (NIAO) Good Practice in Risk Management Guidance 2011 and the HSC Regional Model for Risk Management.

NIAO recommend that strong leadership and clear ownership is essential in embedding an organisational risk management culture. This Strategy clearly defines the leadership and culture required and which has been strengthened in BSO over recent years.

### 2.1 Key Updates

Risk management is a business process which involves **identifying, evaluating and planning for potential business risks**. By using established risk management tools and processes BSO can mitigate significant unnecessary costs

whilst maintaining high quality service delivery. Risk management is therefore an integral part of effective BSO business development, strategy and sustainability.

The BSO Risk Management software was piloted across the organisation during 2024. The introduction of the risk management software, has supported..... risk definition, escalation and mitigation processes being implemented and refined – providing ELT, GAC and the Board with a comprehensive view of risk and assurance.

The BSO Risk Management Strategy 2025/29 was considered and approved by the Board on 27 February 2025. The Board acknowledged the significant progress and ongoing strengthening of strategic risk management across BSO.

The BSO Standing Orders has been revised for presentation to ELT, GAC and the Board in May 2025. This is to reflect compliance with the New February 2025 Procurement Regulations which forms part of the 2023 Procurement Act .

The Board is responsible for ensuring that BSO has robust and effective arrangements for governance and risk management. This includes overseeing and ensuring that systems are in place for identifying, assessing and managing all risks, both financial and organisational. Additionally, the Board is tasked with reviewing the Corporate Risk Register on a quarterly basis to monitor the status of identified risks, assess the effectiveness of mitigation measures and ensure alignment with the organisation's strategic objectives.

The Chief Executive holds overall responsibility for risk management and ensures that BSO implements a systematic programme for risk identification, assessment, management and quality improvement. These processes and procedures are approved and monitored by the Governance and Audit Committee (GAC) on behalf of BSO. Reporting on risks to the sponsor, Department of Health.

The Chief Executive demonstrates strong leadership and ongoing commitment to proactive risk management. Establishing and maintaining a comprehensive approach to risk management, supported by an effective risk management framework. Ensuring that roles and responsibilities related to risk management are clearly communicated, well understood and embedded across all levels of the organisation. Ensuring that there is a clear and efficient process for escalating risks/issues to the Executive Leadership Team (ELT) and BSO Board for attention.

The Executive Leadership Team (ELT) provides direct oversight of risk management within BSO, by reviewing Service and Corporate Risk Registers. They are committed to embedding a positive risk management culture within BSO by:

- Gaining assurance that risk and change in risk is being monitored.
- Receiving the various assurances which are available about risk management.

- Commenting on the appropriateness of the risk management and assurances which are in place.
- Reviewing Corporate and Service Risk Registers and challenge how risks are managed including the approval, escalation and closure of risk when it is deemed appropriate.

**ELT is responsible for:**

- Promoting and leading the implementation of the BSO Risk Management Process.
- Ensuring that objectives have been established at Corporate and Directorate level. Identifying any subsequent risks with the potential to impact on the achievement of those objectives by developing, managing and supporting the maintenance of both the Corporate and Service Risk Registers.
- Directing the annual programme and process for risk management activities and monitoring .
- Assessing the need for staff awareness and training with regard to Risk Management and Assurance.
- Reporting to the Governance and Audit Committee (GAC) and Board so that the Board can assess the effectiveness of the controls and assurance given for the management of risks throughout BSO.

**Directors & Assistant Directors are responsible for:**

- Implementing the Corporate Risk process across assigned Service Areas whilst ensuring responsibility, consistent application and adherence to the Risk Management Process and subsequent guidelines.
- Actively participating in BSO business planning and performance arrangements, managing and supporting the maintenance of accurate and up-to-date risk registers and providing regular updates as required.
- Ensuring the timely escalation of risks where appropriate for discussion at ELT.
- Communicating risk management and updates effectively to all relevant staff.
- Assessing the need for staff awareness and training with regard to Risk Management and Assurance.

- Appropriate population of their risk register in line with the Risk Management Strategy.
- Monitoring the implementation of all risk scores, controls and actions.
- Formally reviewing all relevant service risks within their Directorate on at least a quarterly basis (agendas/minutes must be made available to the Governance and Risk Officer as appropriate).
- Ensuring records are kept to demonstrate that risk management is embedded throughout the service area, will meet internal audit requirements and are available to support the annual Risk Management Standard assessment.
- Providing the Governance and Risk Officer with evidence that these responsibilities are being met.

BSO's Risk Registers are an integral part of the Assurance Process and are used as a mechanism for the Board, GAC and ELT to assess the effectiveness of controls and assurances and to monitor actions identified to mitigate risks. The Risk Registers are managed at two levels:

- **Corporate Risk Register:**

The Corporate Risk Register records and maintains details in relation to strategic and significant risks. It is a central repository for tracing risks, likelihood impact and mitigation measures. It details the controls, assurances and actions approved by the GAC to ensure the focused and effective management of these risks. It is comprised of risks that have been identified which may affect the achievement of the BSO Strategic Objectives and other significant risks that have arisen. The Corporate Risk Report is managed by ELT through a monthly review process. A Corporate Risk and Assurance Report (CRAR) is presented quarterly to the GAC and the Board.

- **Service Risk Register:**

Service Risk Registers are managed locally through the BSO Risk Management Platform. Assistant Directors and Senior Managers are responsible for reporting on risks at least quarterly to their respective Directors. They are also accountable for the proactive management of risks, including timely reviews of controls and ensuring that any actions to mitigate risks are completed within the agreed timeframes.

Risk Registers are formal records of identified and assessed risks, maintained at both corporate and service levels. They serve to ensure that the effectiveness of risk controls is regularly monitored and that risks are prioritised for action. In BSO, these registers are managed electronically using the BSO Risk Management Software system, where each risk is assigned a unique reference number. All designated Risk Owners and Editors have direct access to the system.

The BSO Risk Management System supports risk owners in identifying risks, outlines the controls in place and supports the risk owner in documenting the risk and associated scoring. It encompasses all risks across each service area within a Directorate. Whilst ultimate responsibility and accountability for risk management sits with Directors it is important to note that everyone has a role to play in identifying and managing risk.

Action plans are developed for risks that are actively being treated and progress is monitored by the Directors to ensure mitigation measures are implemented.

In accordance with the regional HSC Risk Management Model (updated August 2018), all risks are scored using the HSC Regional Risk Matrix which is based on the principles of the ISO 31000:2018 standard.

In addition to the Risk Management Strategy 2025-29, a Procedure for the Management of Risk Registers is in place which outlines the methods for identifying and assessing risk, scoring and recording risks on the register, development of risk action plans and the process for escalation and aggregation of risks.

The BSO Risk Management Process is outlined in Risk Management Strategy.

## **2.2 BSO Risk Outputs Delivered**

Based on the ISO 31000: 2018 the BSO has adopted the following definition of risk: - Risk is the “ the effect of uncertainty on an objectives”.

The BSO recognises that it is not possible to eliminate all risks but aims to manage and mitigate risks where possible in line, with its risk appetite which is currently defined as ‘Cautious’ within the BSO Risk Management Strategy.

It has been agreed that:

- There will be inherent risks in order to achieve its aims and deliver beneficial outcomes to stakeholders
- Risks will be taken in a considered and controlled manner
- Exposure to risks will be kept to a level of impact deemed acceptable by the Board

- The acceptable level may vary from time to time and will therefore be subject to at least annual review and revision
- Some particular risks above the agreed acceptable level may be accepted because:
  - the likelihood of them occurring is deemed to be sufficiently low
  - they have the potential to enable realisation of considerable reward/benefit
  - they are considered too costly to control given other priorities
  - the cost of controlling them would be greater than the cost of the impact should they materialise
  - there is only a short period of exposure to them

ELT held a 'Deep Dive' Workshop to review the Corporate Risk and Assurance Report (CRAR) on 9 August 2024. The Strategy, Engagement and Improvement Team (SEI) facilitated an overview session of the new Risk Management system to the Board on 20 September 2024. The session outlined reporting capabilities, features and formatting of the software. Focus was placed on the enhanced functionalities contained within the system which support the streamlining risk management and the tracking corporate risk.

Following review by ELT in October 2024, the Risk Appetite has been updated to reflect a focus on beneficial outcomes to stakeholders and acceptable exposure levels. It represents more emphasis on the involvement of senior management across BSO and the integration of risk management into the organisation. The Board approved the revised BSO Risk Appetite and Matrix on 28 November 2024.

### **2.3 Corporate Objectives**

The Board of BSO have defined corporate objectives and identify corporate risks that may threaten the achievement of these objectives. Controls are in place to manage identified risks, underpinned by organisation assurance and explicit arrangements for obtaining assurance on the effectiveness of existing controls across all areas. On an ongoing basis the Board will assess the assurances given, identify where there are gaps in controls and/or assurances and take action on where gaps have been identified to eliminate and mitigate associated risks. It is important that BSO maintain dynamic risk management arrangements, regularly reviewing the Corporate Risk and Assurance Report (CRAR) and giving due consideration to acceptable risk as defined by the Risk Management Strategy.

## 2.4 Reporting

BSO delivers a systematic approach for risk identification, assessment and management through the following measures:

- Production of an annual Governance Statement which provides a high-level summary of the system of internal control and requires disclosure of any significant control or risk issue;
- Identification of the principal risks to the achievement of the Corporate Objectives outlined in the BSO Corporate Strategy 2024/27 and the Annual Business Plan 2025/26;
- Development of a Corporate Risk and Assurance Report (CRAR) which identifies the principal risks to corporate objectives, highlights gaps in control and/or gaps in assurance processes and provides details of necessary actions. This provides the BSO Board and Governance & Audit Committee with a level of assurance on strategic risk management; Trends of risks are reported to GAC and the Board on a quarterly basis.
- The Corporate Risk and Assurance Report (CRAR) provides a structure for the Accounting Officer, the Governance and Audit Committee and the BSO Board for acquiring and examining the evidence to support the Governance Statement;
- Production of Risk Registers at service level which include treatment actions where appropriate;
- Evaluating risk, in accordance, with the BSO Risk Management Strategy and Procedures which includes a process for escalating risk from service to corporate level;
- The escalation process allows risks where relevant to be escalated from Service Risk Registers to the Corporate Risk Register. For risks that are deemed to be Extreme on the Risk Score Matrix these are automatically escalated by the Risk Owner to the Governance and Risk Officer who will present the update in a report to ELT.
- In turn ELT consider all escalated risks and decide appropriateness of addition to Corporate Risk Register. The Governance and Risk Officer updates the Corporate Risk Register in these cases. The Corporate Risk Register will be issued to Board on a quarterly basis.
- For 'non-extreme' Risks, Risk Owners can escalate these to ELT through the Governance and Risk Officer. Once the Officer has been alerted and the Risk reviewed the Director of the Risk Owner confirms if the Risk should be formally escalated to ELT.
- Directors reviewing service risk registers, with particular consideration to any risks for escalation;

- The Governance and Risk Officer will seek further detail on any financial implications associated with the risk being escalated.
- Directors defining local risk management responsibilities within their Directorate and holding Assistant Directors/Senior Managers responsible for the management and update of their Service Risk Register, development of risk actions plans and monitoring of progress;
- Risk Reporting Monitoring Arrangements are in place to report progress on risk actions to the appropriate level - Board, GAC, ELT and Directors; and
- Risk Awareness training continuing through e-learning and monitored by the Governance and Risk Officer.

## **2.5 Information Governance**

- Risks to the management of information/data security are identified and managed by the Information Asset Owners (IAOs) within the BSO, co-ordinated via the Information Governance Management Group (IGMG). Representation on this group includes appropriate staff from all BSO Services. Following the outcomes of a commissioned review into Information Governance within BSO, IGMG was reconstituted, with representation at more senior level within the organisation. Terms of Reference were revised in 2024/25.

## **3.0 Risk Management Framework 2024/25**

The risk control framework has continued to be supported in 2024/25 by the following actions and events:

- Monthly review of the Corporate Risk and Assurance Report (CRAR) by ELT;
- Quarterly review of the Corporate Risk and Assurance Report (CRAR) by GAC;
- Quarterly review of the Corporate Risk and Assurance Report (CRAR) by the BSO Board;
- Quarterly monitoring of progress on Service Risk actions by ELT and GAC
- Quarterly review of the Issues and Incident Log report by ELT;
- ELT Governance and Assurance Framework Workshop was held on 12 April 2024, to review the organisation's governance and accountability arrangements;
- Amberwing Ltd Risk Training on Governance and Risk Management and Business Model Workshop for Assistant Directors/Directors was held on 15 May 2024;

- Strategy, Engagement and Improvement Team attended Amberwing Ltd Issues and Incident Training session on 15 May 2024;
- ELT Deep Dive review of the Corporate Risk Register was held on 9 August 2024;
- A Board Governance Self-Assessment was completed in September 2024, in line with Department of Health (DoH) requirements. The Chief Executive's Forum published the 'Northern Ireland Audit Office (NIAO) Board Effectiveness – Good Practice Guide' in June 2022. This Guide reflects the move to a much greater level of partnership working and collaboration across government and its arms-length bodies, all of which are embodied in the new partnership agreements. This publication will make essential reading for public service Board Chairs and members; Chief Executives and Senior Executives and for staff in sponsoring departments;
- To date 92.60% of staff have undertaken risk management training, according to the figures held by People and Place. Heads of Service are reminded on a quarterly basis that all staff must undertake this training; and
- Risk Awareness Training continues through e-learning, one to one and management team Risk Management training sessions;
- Governance and Risk Officer attended Operations Directorate Meetings on a quarterly basis; and
- Recommendations from the Risk Audit have been addressed.

#### **4.0 Information Governance Risk**

The arrangements in place to manage information risks include:

- The Director of People and Place is the Senior Information Risk Officer of the Organisation who regularly reviews information to ensure that appropriate controls are in place;
- The Chief Legal Adviser is the Personal Data Guardian and reviews all applications for data sharing;
- Information Asset Owners are in place within each Directorate to manage the risk to personal and corporate information;
- Directorate Information Assets Registers and the Corporate Information Asset Register are reviewed regularly and updated;
- Information risk is recorded and monitored via the Information Asset Register;
- Mandatory training is available via a e-learning platform to all BSO staff providing them with an up to date understanding of information governance issues and risks;

- A Data Protection Officer is in post for BSO;
- BSO Information Governance and associated policies are kept under regular review; and
- As IGMG meet on a quarterly basis (as per above) and provide a report to Governance and Audit Committee. Whilst records management is part of the assurance statement to be provided by Information Asset owners, consideration will be given to the development of this toolkit and roll out across the Information Governance and Management Group in 2025/26.

## 5.0 Update on 2024/25 Action Plan

There were four actions agreed in the previous 2024/25 Action Plan. Below provides updates and progress on these agreed actions:

- **Review of Risk Management System** – The Integrated Governance and Assurance Framework 2025-26 will be presented to ELT, GAC and the Board in May 2025.
- **New Corporate Risk and Assurance Report (CRAR)**– A new CRAR has been developed to define assurances received using the 3 lines of Defence.
- **Risk Management Strategy** – An updated Risk Management Strategy has been revised for 2025-29, to ensure good governance arrangements are in place to identify, manage and mitigate against risks in all aspects of BSO. The Strategy is developed to reflect the principles set out in the Northern Ireland Audit Office (NIAO) Good Practice in Risk Management Guidance 2011 and the HSC Regional Model for Risk Management.
- **Records Management Self-Assessment** - A new Records Management has not been developed. Consideration will be given to the development of this toolkit and roll out through the Information Governance and Management Group in 2025/26.

## 6.0 Risk Management Action Plan 2025/26

An Action Plan for risk management for 2025/26 has been developed to further improve risk management in the BSO for the next financial year, as described in **Appendix 1**.

## **7.0 BSO Accreditations**

BSO continues to promote the value of External Assurances gained through attainment/reaccreditation of recognised awards such as NI Government Opportunities (GO) Awards, UK Government Opportunities (GO) Awards, Certificate of Personal Effectiveness (COPE), Investors in People (IIP), International Organisation Standardisation (ISO), Lexcel and the Chartered Institute of Credit Management and Procurement Centre of Excellence. These awards support the BSO in providing assurance to others that risks are effectively identified and managed and that the Organisation is on track to achieve its strategic vision, aims and objectives.

BSO ITS and NIPACS+ Programme Highly Commended at the Belfast Telegraph IT Awards – Best Place to work in IT over 100 employees and IT Project of the Year – November 2024; BSO Income Shared Services, Accounts Receivable, (SSAR), Credit and Collections Industry Accreditation (CICMQ) re-accreditation with a Distinction grade to retain their coveted Centre of Excellence status. – December 2024; The CIPD NI 2025 Awards - Best digital and technology initiative in HR/L&D – Leadership Centre – Awards 6<sup>th</sup> March - January 2025; BSO Leadership Centre Celebrates Post Graduate Diplomas - Post Graduate Diploma in Health and Social Care Management. – February 2025.

## **8.0 Conclusion**

Risk Management is fully integrated within BSO's business planning and monitoring processes. Whilst the management of Risk is everyone's responsibility, Directors and Senior Managers continue to embed good risk management practices across the BSO as demonstrated through the progress of actions contained within this report. Additionally, Directors and Senior Managers who develop and manage Annual Business Plans are, in agreement, on the importance of risk management, and the pivotal role they have in identifying risks to the achievement of objectives at both a Corporate and Service level.

## **9.0 Recommendation**

GAC is asked to note the contents of this Report.

## Appendix 1: Risk Management Standard Action Plan 2025/26

No	Description	Action	By Whom	By When
1.	Risk Management Software	Continue to embed the new Risk Management system across BSO Service Areas and provide support/training	Governance and Risk Officer	2025/26
2.	Inclusion of corporate risks linked to Performance Against Business Planning Reporting	Rollout of reporting to reflect the links between business planning and corporate risks	Director of Strategic Planning and Customer Engagement	2025/26
3.	Integrated Governance & Assurance Framework 2025/26	Implement the new Integrated Governance and Assurance Framework	Assistant Director of Strategic Planning and Customer Engagement	2025/26
4.	Review and update risk management documents to incorporate new Integrated Governance and Assurance Framework, Risk Appetite and new risk management software	Comprehensive review of risk management documents/Standard Operating Procedures	Governance and Risk Officer	2025/26

5.	<p><b>Records Management Self-Assessment</b></p> <p>Consideration will be given to the development of this toolkit and roll out across the Information Governance and Management Group in 2025/26.</p>	<p>Representation on this group includes appropriate staff from all BSO Services. Following the outcomes of a commissioned review into Information Governance within BSO, Information Governance Management Group (IGMG) has been re-constituted with membership drawn from a more senior level within the organisation (Assistant Director level). Terms of reference have been revised and the group meets on a quarterly basis.</p>	<p>Head of Corporate Services/Data Protection Officer</p>	<p>2025/26</p>
----	--	--	---	----------------