HSC Business Services Organisation

To: Senior Management Team

From: Director of Customer Care and Performance

Subject: Annual Report on Risk Management 2017-18 and Action Plan 2018-19

Status: FOR NOTING

Date of Meeting: 28th March 2018

Background

HSC Organisations are required to ensure that an independently assured risk management system is in place which meets HSC and other requirements in respect of the management of risks, hazards, incidents, complaints and claims.

The Risk Management Controls Assurance Standard requires an annual report to be produced to demonstrate the risk management system's continuing suitability and effectiveness in satisfying the organisation's risk management policy and strategy.

This report has two purposes:

- To report on the Business Services Organisation's risk management activity during 2017-18
- To set out an action plan for risk management for 2018-19

Annual Report on Risk Management 2017-18 and Action Plan 2018-19

1. Introduction

HSC Organisations are required to ensure that an independently assured risk management system is in place which meets HSC and other requirements in respect of managing risks, hazards, incidents, complaints and claims.

During December 2017 Internal Audit carried out an audit of Risk Management and provided Management with satisfactory assurance in relation to Risk Management within BSO.

2. BSO Risk Management Process

2.1 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. The core principle within this Policy was to ensure that risk management was embedded within the organisational management processes and to implement a risk management process for identifying and evaluating risks associated with the various activities of the organisation, assessing and addressing their impact and providing for appropriate disclosure of the progress made in managing the identified risks.

To support the process, BSO developed a Risk Management Strategy (including a Policy Statement) and other risk policies which established a consistent and integrated approach to risk management in BSO.

2.2 The BSO Board is responsible for ensuring that there is an effective system of internal control and that the system is effective in managing risks in order to contribute to the achievement of the BSO objectives. The Board is also responsible for ensuring that the organisation has effective systems for identifying and managing all risks, financial and organisational.

2.3 The Chief Executive ensures that the BSO has a programme of risk management which is approved and monitored by the Governance and Audit Committee. While the Director of Finance has corporate responsibility for risk management, in practice it is delivered through the Customer Care and Performance Directorate by a Governance and Risk Officer.

2.4 Leadership is given to the risk management process by SMT, who are operationally responsible for the management of risks within their respective services in accordance with BSO Risk Management Policies and Procedures. Risk Management is a core component of the job description of senior managers within the organisation.

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

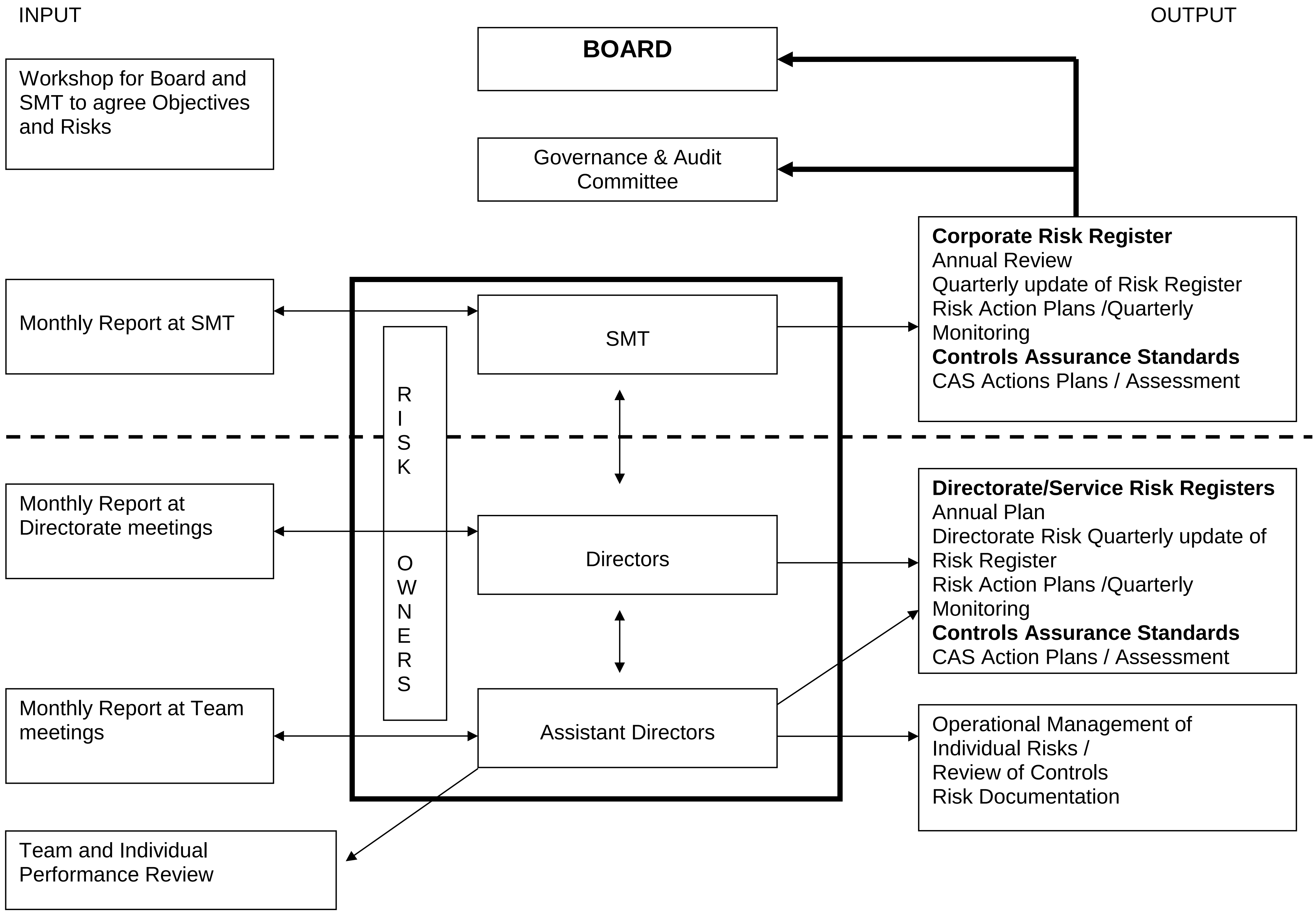
- The Corporate Risk Register contains risks to the achievement of Corporate Objectives and is operationally managed by SMT who review the risks and their respective actions monthly. A Corporate Risk and Assurance Report is presented quarterly to the Governance and Audit Committee and biannually to the BSO Board;

- Service Area Risk Registers include risks to specific service areas and are the direct responsibility of the relevant Director/Head of Service. Action Plans are developed for risks where appropriate and progress on actions is monitored quarterly by SMT and the Governance & Audit Committee.

2.6 In addition to the Risk Management Strategy, the following policies are in place – Risk Management Guide for Managers and Staff and the Procedure for the Management of Risk Registers. The former provides information and guidance on the management of risk, while the latter outlines the methods for identifying and assessing risk, scoring and recording risk on the register, development of risk action plans and the process for escalation and aggregation of risks.

The Risk Strategy and the Procedure for the Management of Risk Registers was reviewed in 2017. The amendments to the policies were approved by SMT and the Governance & Audit Committee; following consideration and discussion of the risk appetite, members agreed that the definition was appropriate and it remained unchanged. The Risk Strategy and the Procedure for the Management of Risk Registers are due for review again in 2018.

2.7 The BSO Risk Management Process is outlined in the flowchart overleaf.



INPUT

OUTPUT

BOARD

Governance & Audit Committee

Workshop for Board and SMT to agree Objectives and Risks

Monthly Report at SMT

SMT

Corporate Risk Register
Annual Review
Quarterly update of Risk Register
Risk Action Plans /Quarterly Monitoring
Controls Assurance Standards
CAS Actions Plans / Assessment

RISK OWNERS

Monthly Report at Directorate meetings

Directors

Directorate/Service Risk Registers
Annual Plan
Directorate Risk Quarterly update of Risk Register
Risk Action Plans /Quarterly Monitoring
Controls Assurance Standards
CAS Action Plans / Assessment

Monthly Report at Team meetings

Assistant Directors

Operational Management of Individual Risks /
Review of Controls
Risk Documentation

Team and Individual Performance Review

3. BSO Risk Outputs Delivered

3.1 The BSO definition of risk describes it as “an event or uncertainty that may enhance (i.e. opportunity) or impede our ability to achieve objectives effectively.” The BSO recognises that it is not possible to eliminate all risks but aims to minimise the risk where possible. The establishment of a risk management system for BSO was achieved 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 2015-18 and the Annual Business Plan 2017-18;
- The integration of risk management methodologies into the business planning process;
- Development of a Corporate Risk and Assurance Report 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;
- Production of Risk Registers at service level which include action plans where appropriate;
- Evaluating risk in accordance with the BSO Risk Management Policies and Procedures which includes a process for escalating risk from service to corporate level;
- 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, Governance & Audit Committee, Senior Management Team and Directors;
- There is a nominated accountable officer and lead officer for all applicable Controls Assurance Standards, charged with delivering action plans to secure substantive compliance;
- Lessons learned from past experience;
- Risk Management Awareness was part of the Corporate Induction process. The Corporate Induction Process was replaced in October 2017 with the Corporate Welcome Process and Risk Awareness Training is provided to new starts through mandatory online training.

3.2 Risks to the management of information /data security are identified and managed by the Information Governance Management Group, representatives of which are drawn from senior managers from all BSO Services. To ensure compliance with the Information Management Controls Assurance Standard, an annual action plan is developed and progress against action is monitored by the Business and Development Committee.

3.3 Controls measures are in place to ensure that the BSO's obligations under equality, diversity and human rights legislation are complied with.

2017-18

3.4 The risk control framework has been further strengthened in 2017-18 by the following actions and events:

- The implementation of a new format of the Corporate Risk Register taking into account changes agreed by the Board and GAC in respect of the revision of the process for reporting risks. The main changes to the Corporate Risk Register included an update of the risk matrix and the assignment of a risk appetite to each corporate risk.

- An audit of Risk Management in December 2017 produced a **satisfactory assurance** in relation to Risk Management within BSO;
- Monthly review of the Corporate Risk and Assurance Report by SMT;
- Quarterly review of the Corporate Risk and Assurance Report by the Governance and Audit Committee;
- Biannual review of the Corporate Risk and Assurance Report by the BSO Board;
- Quarterly monitoring of progress on Service Risk actions by SMT and Governance & Audit Committee;
- The review of the BSO's compliance with the applicable Controls Assurance standards for 2017-18 is pending. A final confirmed outcome is expected by the end of March 2018.
- **Controls Assurance Action plans** for 2017-18 were implemented and progress is reviewed quarterly;
- A Board Governance Self-Assessment was completed in August 2017 line with DoH requirements;
- **Risk awareness sessions** are delivered as part of the Corporate Induction process which ceased in September 2017. Risk awareness sessions continue to form part of the Corporate Welcome Process which commenced in October 2017.

3.5 Risks to the management of information / data security are identified and managed by the Information Governance Management Group, whose representatives are drawn from across the BSO. This group reports to the Board and SMT via the Director of Human Resources and Corporate Services.

The arrangements in place to manage information risks include:

- The HRCS Director is the Senior Information Risk Officer of the Organisation who regularly reviews information to ensure that it is protected;

- The Chief Legal Officer has been appointed as the **Personal Data Guardian** and personally reviews all applications for data sharing.
- Information Asset Owners are in place within each Directorate to reduce the risk to personal information;
- Directorate Information Assets Registers are reviewed regularly and updated;
- Regular mandatory training is delivered to all BSO staff providing them with an up to date understanding of information governance issues and risks;
- BSO ICT Security Policy and associated policies are kept under regular review.
- A programme of **IG and Records Management Audits** has been undertaken by the IGMG across the BSO to test compliance with the IG assurance framework.

3.6 The Corporate Risk and Assurance Report 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.

4. Controls Assurance Standards

4.1 Since 2002, DoH has required Health and Social Care organisations to achieve a target level of compliance with, and report on, a total of 22 Controls Assurance Standards annually, **15** of which apply to BSO.

HSC organisations are required to undertake a self-assessment for each applicable Standard. The Standards are about identifying and applying best practice and offering assurance that we are doing our reasonable best to control the risks to the achievement of our objectives.

4.2 Each year the core standards of Governance, Risk Management and Financial Management are independently assessed by Internal Audit. In 2017-18, compliance with the following applicable standard is also subject to internal audit verification:

- Fire Safety.

4.3 For 2017-18, HSC organisations are required to achieve substantive compliance (75-99%) in all standards applicable to the organisation. **It should be noted, however, that the Department of Health advised in August 2017 that Controls Assurance Standards will cease with effect from 1 April 2018. The DoH has indicated in correspondence, dated 27 March 2018, that further information will be issued regarding future arrangements.** It should be noted however that from a DoH perspective, the following governance and accountability tools provide the Department with assurance on risk management namely –

- Board Governance Self-Assessment Tool
- Assurance Framework
- Mid Year Assurance and Governance Statement
- Twice yearly formal accountability process
- Sponsor branch scrutiny of risk registers
- Independent assurance – BSO/RQIA.

4.4 For 2017-18, BSO has assessed its compliance against the **15** applicable Controls Assurance Standards and the outcome of the assessment is outlined in the table below:

Standard	DoH Expected Level of Compliance	Overall Level of Compliance Achieved	Reviewed by
Buildings, Land, Plant	Substantive	Substantive	Self-Assessed
Emergency Planning	Substantive	Substantive	Self-Assessed

Environmental Management	Substantive	Substantive	Self-Assessed
Fleet and Transport	Substantive	Substantive	Self-Assessed
Financial Management	Substantive	***to be confirmed**	Internal Audit
Fire Safety	Substantive	***to be confirmed**	Internal Audit
Governance	Substantive	***to be confirmed**	Internal Audit
Health & Safety	Substantive	Substantive	Self-Assessed
Human Resources	Substantive	Substantive	Self-Assessed
ICT	Substantive	Substantive	Self-Assessed
Purchasing and Supply	Substantive	Substantive	Self-Assessed
Information Management	Substantive	*Substantive	Self-Assessed
Risk Management	Substantive	***to be confirmed**	Internal Audit
Security Management	Substantive	Substantive	Self-Assessed
Waste Management	Substantive	Substantive	Self-Assessed

4.5 The three core standards of Risk Management, Governance, and Financial Management, in addition to scoring for Fire Safety (all marked ***** above) have been verified by Internal Audit / or are due for verification by Internal Audit.

4.6 Action Plans will be developed for all gaps in compliance identified in the 2017-18 assessments and progress will be monitored and reported to

SMT, Governance & Audit Committee and Board throughout the forthcoming year.

5. Risk Management Action Plan 2018-19

5.1 The requirement for Controls Assurance Standards reporting to the DoH will cease with effect from 1 April 2018, including the Risk Management Standard. In addition, the DoH licence for the AS/NZ risk management standard will cease in June 2018. Members of BSO staff (from Customer Care and Performance and Internal Audit) have been working with DoH and HSC colleagues to determine a future approach to risk management within HSC. There are benefits to maintaining a common standard across HSC, including from an Internal Audit perspective. Proposals for a future collaborative approach to risk management frameworks across the HSC organisations will be brought forward for consideration to BSO Board. An Action Plan for risk management for 2018-19 has been developed to implement the recommendations arising, as described in ***Appendix 1.***

6. Conclusion

Risk Management is fully integrated within BSO’s business planning, execution and monitoring processes. Directors and senior managers who develop and manage annual business plans are attuned to the importance of risk management and they play a pivotal role in identifying risks to the achievement of objectives at both a directorate and corporate level.

BSO continues to promote the value of External Assurances gained through benchmarking services, attainment/reaccreditation of recognised awards such as COPE, IIP, ISO, Lexcel. They form part of the Corporate Assurance Process (Internal and External) and assist the Organisation 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.

Appendix 1: Risk Management Standard Action Plan 2018-19

No	Description	Action	By Whom	By When
1.	Common Risk Management Standard Work with HSC colleagues to agree a common approach to risk management following the cessation of Controls Assurance Standards reporting process and the licensing of the AS/NZS 4360:2004 standard.	Agree a common approach across HSC with regard to a future framework for implementing risk management.	AD CCP/ G&R Officer	April 2018
		Review risk management documents with a view to amending to reflect cessation of AS/NZS and description of agreed future approach.	G&R Officer	June 2018
2.	Complaints and Claims processes Review complaints system in line with audit recommendations	Complaints programme to be made available to all staff and recorded through HRPTS.	Head of Corporate Services	September 2018
3.	Business Continuity training	Specific business continuity training to be undertaken jointly with the HCB/PHA under the auspices of the JEP.	Head of Corporate Services	December 2018