Business Services Organisation

Providing Support to Health and Social Care

Title	**Risk Management Guide for Managers & Staff**

Summary	The guidance provides management and staff with the information to consider and address risk management within their areas of responsibility.
Purpose	To provide guidance on the management of risk.
Operational date	April 2010
Review date	December 2015
Version Number	V 4
Supersedes previous	V 3
Director responsible	Director of Finance / Director of Customer Care & Performance
Lead author	Patricia Maginnis
Lead author, position	Governance and Risk Officer
Additional authors	
Department	Customer Relations & Service Improvement
Contact details	patricia.maginnis@hscni.net Tel: 028 9536 3806
Equality Screened	November 2015

Reference number	
Supersedes	Version 3

Version Control

Date	**Version**	**Author**	**Comments**
May 10	1	Fiona Moore	Available on Intranet
Aug 10	2	Fiona Moore	Revision of risk score matrix & components of risk register.
June 2013	3	Jill Jackson	Revision of BSO Risk definition & addition of Dof CCP's role. Inclusion of methods for identifying risks Update of Appendix A – update version of Register and Action Plan
December 2015	4	Patricia Maginnis	Revision of role of BSO Board Update of Appendix A – update version of Register and Action Plan

Policy Record

Author(s)	G&R Officer
Director responsible	DoF/DoCCP

Approval Process

		Date
Senior Management Team		
Governance & Audit Committee		

1. Introduction

The guidance outlined in this document provides management and staff with the information to consider and address risk management within their areas of responsibility. It describes the operational reporting procedures and documentation to be used to support internal control and corporate governance arrangements.

1.1 What is Risk Management?

Every business and every person faces risks each day. In a business sense, risk management is the process by which an organisation takes steps to control the risks to which it may be exposed. Risk is something which affects everyone within an organisation and managing risk effectively is something in which we all (management and staff) have a part to play.

There are different types of Risks:

Financial: eg. Fraud, poor accounting processes.

Technical: eg. IT system failure.

Health & Safety: eg. Trips, manual-handling injuries.

Reputation: eg. Poor service quality, bad publicity.

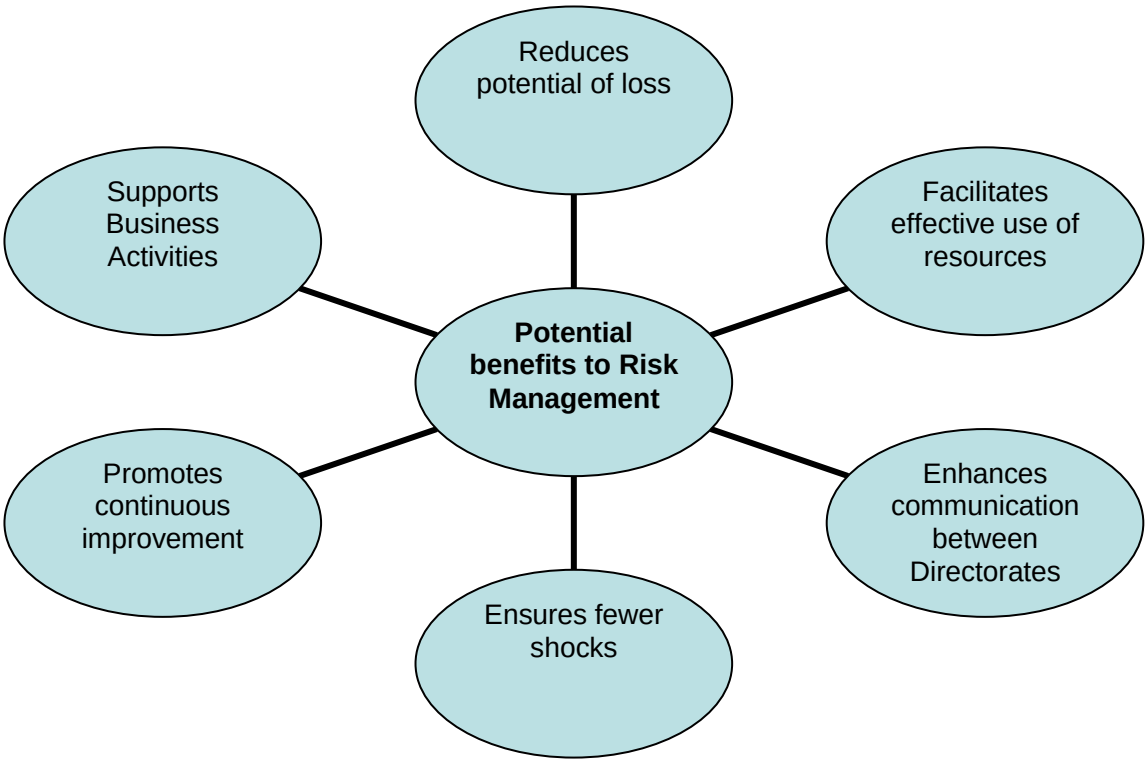
Risk is an event or uncertainty that may enhance (i.e. opportunity) or impede our ability to achieve objectives effectively.

Risks can also arise from not taking opportunities to deliver better and more effective services.

Risk Management means having in place a corporate and systematic process for evaluating and addressing the impact of risks in a cost effective way, and having staff with the appropriate skills to identify and assess the potential for risks to arise. Staff and managers who deliver services are best placed to identify and assess Risk.

1.2 Why Risk Management?

The aim of risk management is not to eliminate risks but to manage them. Done well, the process provides assurances from staff to team to Directorate and, ultimately, to the Board and helps ensure that the BSO is able to provide first class support services to HSC organisations.



1.3 What does the BSO do with regard to Risk Management?

The BSO policy statement on risk is: “The BSO will ensure that the management of risk is an integral element of its work in relation to customers, staff and the public (where relevant)”.

The BSO delivers this by defining the roles and responsibilities of risk management to officers and by establishing working groups and committees to provide assurances on the process of risk management.

1.4 Responsibility for Risk Management within the BSO

<u>BSO Board</u>

The Board is responsible for ensuring that there is an effective system of internal control and ensuring that the system is effective in managing risks so as to assist in the achievement of BSO Objectives. The Board is responsible for ensuring that the BSO has effective systems for identifying and managing all risks, financial and organisational. The Board has established a risk management structure to help deliver its responsibility for implementing risk management systems throughout the BSO. The programme of risk identification, assessment, management and quality improvement processes and procedures is approved and monitored by the Governance and Audit Committee on behalf of the Business Services Organisation.

Chief Executive

The Chief Executive as Accountable Officer has overall responsibility to the BSO Board for Risk Management. Operationally, the Chief Executive has delegated responsibility for implementation as outlined below:

Director of Finance

The Director of Finance is the designated officer on behalf of the Chief Executive and has corporate responsibility for Risk Management.

The Director of Customer Care & Performance

The Director of Customer Care & Performance is responsible for the risk reporting and risk training, and for ensuring that service areas are maintaining service risk registers.

Directors

Directors are responsible for following the BSO's risk management policy and for the management of corporate risks and operational risks within their own portfolios.

Governance & Risk Officer

The Governance & Risk Officer will be responsible for the maintenance of the BSO Corporate Register. They will monitor performance against risk treatment plans and report progress to the Senior Management Team and in conjunction with SMT will produce an Annual Risk Report. They will prepare the annual submission for the Controls Assurance Standards for Risk Management and

Governance. In addition they will act as catalyst at all levels of the organisation to ensure that the management of risk is addressed at all levels of the organisation. In fulfilling this role they will advise staff and management at all levels in the organisation as to best ways to manage risk, and support staff with training and development in this area.

Responsibility of all Employees, Agency and Contractors ("Staff")

Everyone has a role to play, all staff are encouraged to use the risk management process as a mechanism to highlight areas they believe need to be improved. However it is important to emphasise that each member of staff have a responsibility to safeguard their own health, safety and welfare and that of others who may be affected by service activity.

1.5 Process for Managing Risk

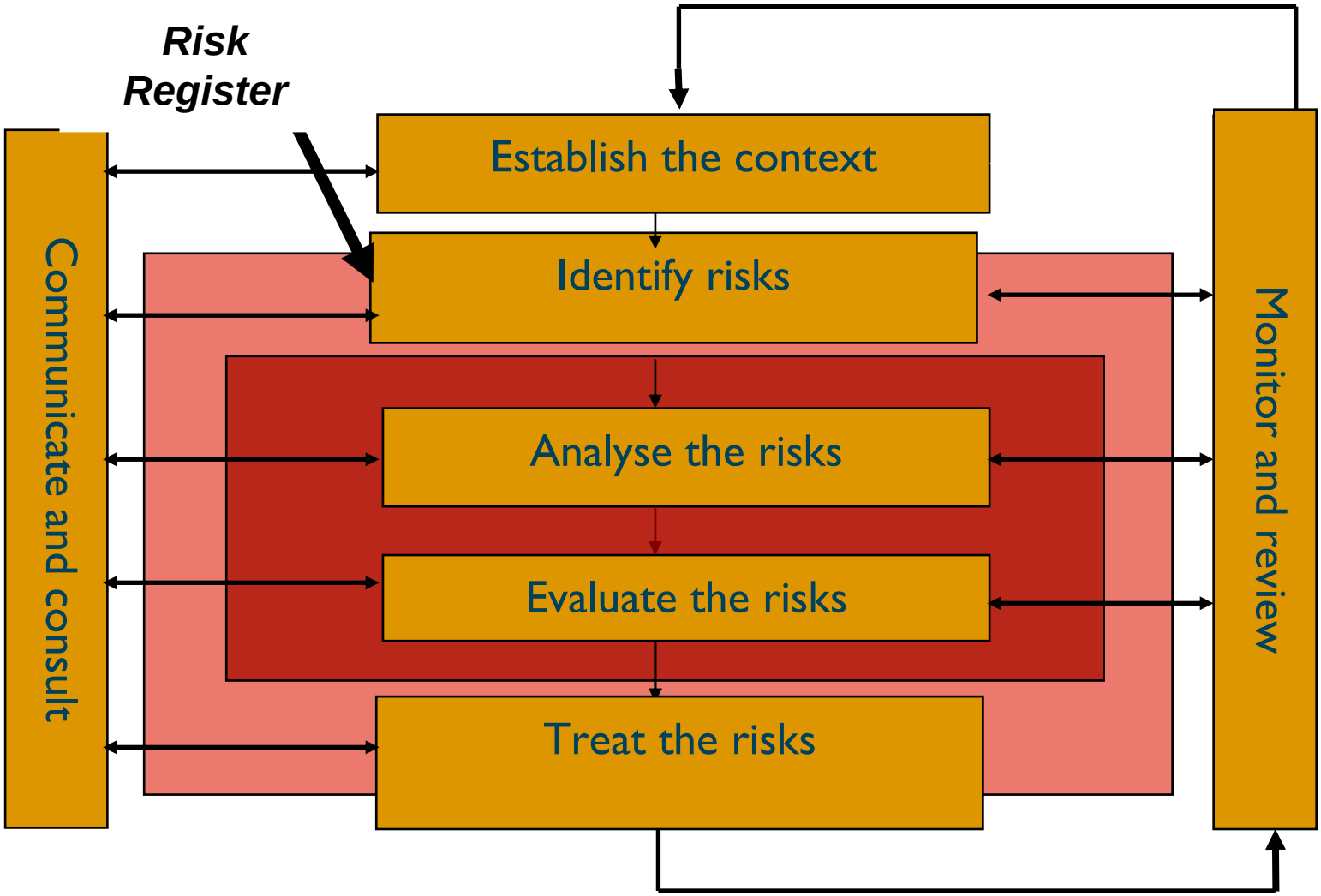
The process for managing risk is defined as[1] "the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluation, treating, monitoring and communicating risk."

The diagram below, which is in operation within the BSO, outlines this process. It is an ongoing process with frequent interaction between the steps.

.

[1] Australian and New Zealand Standard (AS/NZS4360 Risk Management)

Process for Managing Risk



2. Establish the Context

2.1 A key principle of risk management is that it should be fully integrated with the organisation's business planning process. Within the BSO, risk management is aligned to the achievement of corporate objectives and assurances on internal control.

2.2 The approach adopted by the BSO in the compilation of the Risk Register is based on the need to identify the risks likely to impede the achievement of BSO objectives; this can occur either in terms of the meeting of Service Level Agreement objectives and targets, or the completion of objectives at Corporate and Directorate/ Service Area as set out in the BSO Corporate Plan and annual Business Plan.

2.3 The Corporate Plan is available on the BSO website and local Business Plans are available to staff from their Directorate management.

3. Identify Risks

3.1 For each Directorate/Service Area this means recognising and identifying the key risks for which they are responsible and which are most likely to impact on their performance. Failure to identify risks could affect service delivery and result in non-achievement of objectives.

3.2 Risk Identification is a subjective exercise and can only provide reasonable but not absolute assurance. Risk Identification within Directorates is best carried out involving a range of officers discussing the inherent risks that exist (i.e. the level of risk that exists without any control mechanism in place), thereby focusing staff on risks which could prevent the achievement of objectives.

Some methods for identifying risks are:

- Discussion at staff meetings or workshops;
- Checking Audit Report recommendations;
- Awareness of changes in legislation and policy;
- Analysis of data e.g. 'Near Misses,' Complaints or FOIs, sickness or absence levels;
- Through Customer Forums.

3.3 To understand the risk and subsequently identify ways to manage it, the underlying root cause(s) should be identified, as should the implications(s) of the risk occurring. Each risk should be assigned an owner who has operational responsibility for managing that risk.

All identified risks are recorded in a Risk Register, an example of which is provided in *Appendix A.* Further details about Risk Registers are described in the Procedure for the Management of Risk Registers (December 2015).

4. Analyse the Risks

4.1 Each risk identified should be analysed to provide an overall assessment of the potential impact and the timescale over which the risk needs to be managed. The analysis should determine existing controls and their reliability in terms of:

i. minimising the likelihood of the risk maturing; and
ii. if the risk does mature, minimising its adverse consequences.

Consequence and likelihood may then be combined to produce estimated levels of risks, quantified wherever possible, or qualified in range of low to high.

4.2 All new and existing risks identified are assessed in terms of root causes and are individually scored against a 5 x 5 assessment matrix. Risk scoring involves an assessment in terms of the total IMPACT on the BSO against the LIKELIHOOD of the risk occurring.

4.3 The impact and likelihood of occurrence should again be considered in terms of inherent risks, i.e. the level of risk that exists without any control mechanisms in place. The scales (scoring) for determining impact and likelihood are shown in the tables below:

BSO Risk Score Matrix: Likelihood Descriptors

CODE	DESCRIPTOR	DESCRIPTION
1	Rare	The event may only occur in exceptional circumstances
2	Unlikely	The event could occur at some time
3	Possible	The event might occur at some time
4	Likely	The event will probably occur in most circumstances
5	Almost certain	The event is expected to occur in most circumstances

BSO Risk Score Matrix: Impact Descriptors

	1	2	3	4	5
Descriptors	**Insignificant/**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Service Provision (Internal & External)	• Failure to meet target, objectives, service provision – no sanctions applied	• Failure to meet target/standard – no significant resulting consequence • Loss of a service in a number of non critical area/s	• Failure of meet major targets. Significant Stakeholder attention in respect of non compliance with target/ Standard • Loss of a service in any critical area	• Failure to meet major target/s resulting in Departmental sanctions • Extended loss of an essential service/s in more than one critical area	• Significant failure/s to meet a major target/s over a prolonged period of time • Possible termination of senior executives contracts • Loss of multiple services/s in critical areas
Financial - Corporate level	• Insignificant impact on ability to meet financial breakeven Target	• Minor impact on ability to meet Breakeven Target	• Moderate impact on ability to meet Breakeven Target	• Major impact on ability to meet Breakeven Target	• Breakeven Target cannot be met
Financial – Service level	• Insignificant cost	• Less than 5% over budget	• 5-10% over budget	• 10-20% over budget	• More than 25% over Budget
Reputation	• Rumours • Little impact on confidence levels	• Elements of stakeholders expectation not being met – minor issues can be addressed at Service level • Minor impact on confidence levels	• Service below reasonable stakeholders expectation – moderate issues can be addressed at Directorate level • Confidence in the BSO could be undermined	• Service well below reasonable stakeholders expectation leading to formal complaint raised to CX • Confidence in the BSO undermined	• Service drastically below reasonable stakeholders expectation which leads to departmental intervention • Questions in Assembly • PAC Enquiry
Legal/Statutory Professional/ Standards	• Unlikely to cause complaint • Litigation risk is remote • Rare failure to meet statutory duties*/investigation by regulatory or other external body	• Complaint possible • Litigation unlikely • Unlikely failure to meet statutory duties*/ investigation by regulatory or other external body	• Litigation possible but not certain • High potential for complaint • High potential for failure to meet statutory duties*/ investigation by regulatory or other external body	• Litigation expected/ certain • Complaint certain • Expected failure to meet statutory duties*/ investigation by regulatory or other external body	• Litigation certain Failure to meet statutory duties*/ investigation by regulatory or other external body

* Statutory Duties includes Equality and Human Rights / Health & Safety / Freedom of Information / Data Protection and Controls Assurance Standards

4.4 In order to ensure that all risks are evaluated consistently, every risk is analysed using a combination of likelihood and impact. The cumulative effect of likelihood and impact is derived from a matrix using the risk scores. Risk are classified in accordance with AS/NZS Risk Management Standard 4360:2004 guidance

Total Scores are then calculated as follows:

Score = Likelihood x Total Impact

The Risk Score Matrix and Risk Classification are detailed below:

Total Impact

Catastrophic	**5**	5	10	15	20	25
Major	**4**	4	8	12	16	20
Moderate	**3**	3	6	9	12	15
Minor	**2**	2	4	6	8	10
Insignificant	**1**	1	2	3	4	5
		1	**2**	**3**	**4**	**5**
		Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**

Likelihood

Risk Classification

LOW	MEDIUM	HIGH	EXTREME

4.5 For example, a risk that is assessed as a 5 on each scale will score 5 x 5 = 25 is classified as **Extreme**, whilst the risk with the lowest score on each scale will be 1 x 1 = 1 is classified

as **Low.** Risks are in general scored with an emphasis on either impact or likelihood, but rarely on both.

4.6 The next stage is to identify what controls are in place to mitigate or manage the risk.

5. Evaluate the Risks

5.1 Having identified and prioritised the significant risks, and identified the controls in place (or planned for the future), the aim at this stage of the process is to establish the effectiveness of the controls in place.

In terms of the effectiveness of the controls this requires one of the following control strategies to be adopted:

- TOLERATE the risk - our ability to take effective action against some risks may be limited, or the cost of taking action may be disproportionate to the potential benefit gained. In this instance, the only management action required is to 'monitor' the risk to ensure that its likelihood or impact does not change. If new management options arise, it may become appropriate to treat this risk in the future. <u>This action is classified as a Risk Acceptance Measure.</u>

- TRANSFER the risk - e.g. it may be appropriate to address some risks through insurance. Certain risks may also be shared with our stakeholders or service providers. Contracting out can transfer some, but not all, of our risks

(and often introduces a new set of risks to be managed and monitored). This action is classified as a Risk Transference Measure.

- TERMINATE the risk - this is a variation of the 'Treat' approach, and involves quick and decisive action to eliminate a risk altogether e.g. by adopting an exit strategy. The introduction of new technology may also remove certain existing risks, though it will often result in a new set to be addressed. This action is classified as a Risk Prevention Measure.

- TREAT the risk - by far the greatest number of risks will involve this strategy. The purpose of treatment is not necessarily to terminate the risk but, more likely, to set in place a series of mitigating controls to contain the risk to an acceptable level e.g. by building checks and controls into the operational process, staff training, improved case management systems etc. This action is classified as a Risk Reduction Measure.

- TAKE THE OPPORTUNITY the risk presents – are there any positive opportunities to be gained as part of the risk management process. This action is classified as a Risk Opportunity Measure.

5.2 Each risk should then be evaluated. Evaluation enables identified risks to be ranked in order to set management

priorities and present information for business decisions about which risks need to be addressed.

6. Treat the Risks

6.1 The option of “Treat” in addressing risk can be further analysed into four types of control as defined below:

Preventive Controls

These controls are designed to limit the possibility of an undesirable outcome being realised (e.g. separation of duty, whereby no one person has authority to act without the consent of another).

Corrective Controls

These controls are designed to correct undesirable outcomes that have been realised (e.g. contingency planning).

Directive Controls

These controls are designed to ensure that a particular outcome is achieved (e.g. staff be trained with required skills before being allowed to work unsupervised).

Detective Controls

These controls are designed to identify occasions of undesirable outcomes having been realised (e.g. asset checks, monitoring activities, which detect changes that should be responded to).

6.2 When reviewing the controls in place the following points should be considered:

- is the control performed?
- who performs it?
- how often is it done?
- what evidence exists to support the control?

It is normally sufficient to design controls that give a *reasonable assurance* of reducing likely loss to the BSO. Every control action has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling. Generally speaking the purpose of control is to constrain risk rather than to eliminate it.

6.3 For all gaps in controls, additional actions to manage the risks should be identified, along with the date actions will be delivered and by whom. Additional risk actions should be recorded in the risk register action plan, refer to *Appendix A.*

7. Communication and Consult

7.1 Communication within the BSO about risk issues is important:

- to ensure that everybody understands, in a way appropriate to their role, what the BSO risk management process is, what the BSO and their Directorate/ Service

Area priorities are and how the responsibilities of their job fit into that process;

- to ensure that lessons learned are communicated so that everyone can benefit from them;

- to ensure that each level of management, including the BSO Board, actively seeks and receives appropriate and regular assurance about the management of risk within their span of control.

7.2 Risk Management is an essential part of good management and governance. To enhance the quality assurance process, Risk Management is a standing agenda item on the following groups across the BSO:

1. The BSO Board*
2. The Governance and Audit Committee*
3. Senior Management Team*
4. The Health, Safety & Environment Management Group
5. Internal Directorate/Service Area meetings

* These Groups have a particular focus on new risks that may be identified across the BSO.

7.3 At Directorate/Service Area level the BSO Risk Management Process should be cascaded to all staff through the line management structure and all staff should be aware of the risks in their area of work.

8. Monitor and Review

8.1 Management of risk has to be reviewed and reported on for two reasons:

- To monitor whether or not the risk profile is changing;
- To gain assurance that risk management is effective, and to identify when further action is necessary.

8.2 The Chief Executive must provide (as part of the Annual Accounts) an annual Governance Statement, which includes risk management. From 2009 onwards HSC Organisations are also required to provide a mid-year Assurance Statement.

8.3 The Board and Chief Executive seek assurances from a number of sources including suppliers and contractors, third parties, management and from regular internal and external audit reports; the latter determine whether the BSO is aware of the nature and extent of the risks it faces. Furthermore, BSO needs to ensure that the management of those risks is actively managed so as to promote a culture of continual improvement.

8.4 The Governance and Audit Committee reports directly to the Board on internal control, including risk controls and alerts them on any emerging risk issues.

8.5 Both Internal and External Audit have a role to play in supporting effective internal control, as their remit is to

provide independent assurance on the BSO internal control framework.

8.6 The BSO has implemented a risk management process at Corporate and Directorate/Service Area to review whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks has changed, to report significant changes which adjust risk priorities, and to deliver assurance on the effectiveness of the control process.

8.7 As part of the annual Business Planning process, HSC Organisations are now required to produce an Assurance Framework. The Assurance Framework maps out the organisations principal objectives, the risks to their achievement and related controls, whose effectiveness can be tested, assured and strengthened.

8.8 The attached schematic identified in *Appendix B* outlines the developing Assurance Approach.

9. Conclusion

9.1 Management of risk is the key to making the BSO successful in delivering its objectives. Good risk management allows the BSO to:

- have increased confidence in achieving its desired outcomes; and
- take informed decisions about exploiting opportunities.

It is not possible to eliminate all risks but organisations that actively identify and manage risks are more likely to be better prepared to respond quickly when things go wrong and to respond to change in general.

10 Other Risk Related Documents

10.1 This guide should be read in conjunction with the following documents:

- Risk Management Strategy inc Policy Statement;
- Procedure for the Maintenance of Risk Registers;
- Annual Risk Report;
- Adverse Incident Policy;
- Complaints Policy;
- Claims Policy;
- Health & Safety Policy;
- Environmental Management Policy.

10.2 The aforementioned information will be made available on the BSO Intranet. The purpose of these documents is to ensure that staff and other stakeholders are aware of the BSO's responsibilities and their individual responsibilities for risk evaluation and control.

10.3 A glossary of risk management terminology used in this guidance is provided in *Appendix C.*

References

The Orange Book, Management of Risks Principles & Concepts, HM Treasury, October 2004

Supporting Innovation, Managing Risk in Government Departments, NIAO, August 2000

Australian and New Zealand Standard**,** AS/NZS 4360 Risk Management

Risk Management Standard, Department of Health, April 2011

Government Internal Audit Manual

										Risk Action Plan			Expected Outcome after treatment			
Corporate Objectives	Risk No.	Risk Description	Risk Owner	Likelihood	Impact	Score	Controls in Place	Current Risk Rating	Acceptable Risk Y/N	New Risk Actions being developed	By Whom	By When	Likelihood	Impact	Score	Expected Risk Rating
1. To Deliver Value for Money Services to our Customers																
2. To Grow our Services and Customer Base																
3. To Pursue and Deliver Excellence through Continuous Improvement																
4. To Enhance the Contribution and Development of our People																

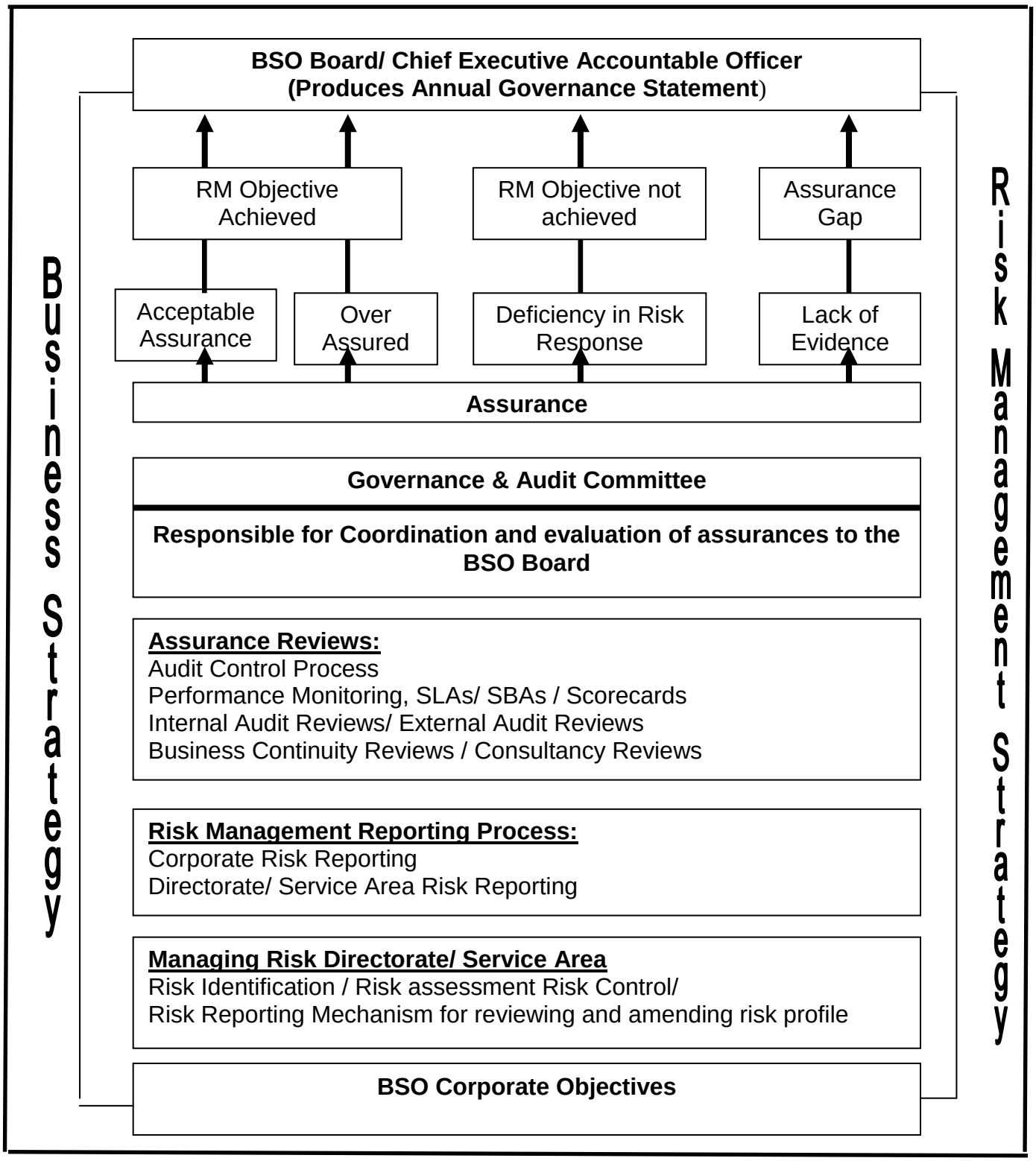
Appendix A

Risk Action Plan 2015-16

		Risk Action Plan				
Risk No	**Risk Description**	**New Risk Actions being developed in 2015-16**	**By When**	**Period**	**RAG Status**	**Comment**

Appendix B

BSO Assurance Approach



Adapted from the Management of Risk – Principles and Concepts October 2004 "The Orange Book", issued by HM Treasury.

Appendix C

Glossary of Terms [2]

Assurance	Gaining confirmation that risk assessment and control response is appropriate, adequate and achieving the effects for which it has been designed.
Control	Any action, procedure or operation undertaken to either contain a risk to an acceptable level of potential exposure or to increase the probability of a desirable outcome. Controls may be classed as follows: **Corrective control -** a control designed to correct undesirable outcomes. **Detective control -** a control designed to detect undesirable outcomes which have materialised **Directive control -** a control designed to ensure a particular outcome **Preventive control -** a control designed to prevent an undesirable happening
Corporate Governance	The overall management of an organisation where it is possible to explain/see how activities are undertaken with appropriate, associated, accountability. There is a need to establish control mechanisms and provide stewardship reports such that it is possible to see that the necessary activities are taking place.
Embedding risk management	Ensuring that the risk management strategy is reflected in the objectives and function of every level of the organisation.
Exposure	The range of outcomes arising from the combination of the impact of an event and the probability of the event actually happening.
Impact	The evaluated effect or result of a particular outcome actually happening.

[2] Note – The majority of the definitions here are drawn from: "*Management of Risk – Principles and Concepts October 2004 "The Orange Book"*, issued by HM Treasury. The definitions on *Internal Control* are based on the Government Internal Audit Manual (GIAM).

Internal Control	Consists of individual actions, procedures, or operations taken or instituted by management to ensure that activities and procedures are operating to achieve its objectives. Key features of control in an organisation are: The definition and establishment of business objectives, standards, processes, and procedures. Clear definition of responsibilities for management and operation of activities; Measurement of inputs, outputs and performance in relation to objectives, taking corrective action where appropriate; Critical review of objectives, risks, operations, outputs, and value for money; Reporting of financial and non-financial results and performance.
Likelihood	The evaluated probability of a particular outcome actually happening (including a consideration of the frequency with which the outcome may arise).
Opportunity	An uncertainty of outcome that may result in a positive or beneficial impact that the organisation wishes to take advantage of or exploit.
Risk	Can be defined as: “The threat or possibility that an action or event will adversely or beneficially affect an organisation’s ability to achieve its objectives”
Risk management	The task of ensuring that the organisation makes cost-effective use of a risk process. Risk management requires: processes in place to monitor risks; access to reliable up-to-date information about risk; the right balance of control in place to deal with those risks; decision making processes supported by a framework of risk analysis and evaluation.
Risk management framework	Sets the context within which risks are managed in terms of how they will be identified, analysed, controlled, monitored and reviewed. It must be consistent and comprehensive with processes embedded in management activities throughout the organisation.

Risk owner	A role, or individual, who is in a position to identify the risk and ensure it is managed or controlled.
Risk management process	A series of well-defined steps to support better decision making through good understanding of risks and their likely impacts.
Risk register	A document used to maintain information on all the identified risks pertaining to a particular business activity, project or programme.