HSC Business Services Organisation

INVESTORS IN PEOPLE®
We invest in people Silver

Risk Management Strategy 2020-2024

Purpose	The control and management of risk to achieve organisational objectives
Operational date	April 2010
Most recent review	February 2023
Version Number	V 6
Supersedes previous	V 5
Director responsible	Director of Strategic Planning and Customer Engagement
Lead author	Joanne Martin
Lead author, position	Governance and Risk Officer
Department	Strategic Planning and Customer Engagement
Contact details	Joanne.martin@hscni.net Tel: 028 95363798
Equality Screened	20th May 2020

Version Control

Date	Version	Author	Comments
May 10	1	Fiona Moore	
Dec 10	1.01	Fiona Moore	
March 2013	1.02	Jill Jackson	
December 2015	1.03	Patricia Maginnis	
May 2017	2	Patricia Maginnis	
December 2018	3	Jane Keenan	
May 2020	4	Patricia Maginnis	
September 2021	5	Joanne Martin	
February 2023	6	Joanne Martin	Annual Review of Risk Management Strategy

Approval Process

		Date
Senior Management Team	Approved	9th March 2023
Governance & Audit Committee	Approved	20th April 2023

HSC Business Services Organisation

INVESTORS IN PEOPLE®
We invest in people Silver

CONTENTS

SCOPE

This strategy applies to all BSO employees, contractors and other third parties working within the BSO. Risk Management is the responsibility of all staff, in particular, managers at all levels are expected to take an active lead to ensure that risk management is a fundamental part of their operational remit. Managing risk is part of good governance and is fundamental to how an organisation is managed at all levels. Managing risk is part of all activities associated with an organisation and includes interaction with stakeholders; consideration of the external and internal context of the organisation, including behaviour and cultural factors.

AIM

The aim of this policy is to have a comprehensive and cohesive risk management system in place underpinned by clear responsibility and accountability arrangements based on the principles contained in the HSC Regional Model for Risk Management.

OBJECTIVES

The objectives of this policy are:

- To define the BSO approach to risk management including roles and responsibilities
- To make the effective management of risk an integral part of overall management practice.
- To raise awareness of the need for risk management by all within BSO
- To have a policy in place to support the Governance Statement, and corporate governance arrangements.
- To support the integration of risk management within the BSO aims and objectives and across the organisation

POLICY STATEMENT

The Business Services Organisation 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)".

WHAT IS RISK MANAGEMENT?

Risk Management is recognised as an integral part of good management practice. Good risk management awareness and practice at all levels is a critical success factor for the BSO. Risk is inherent in all that we do. There is no area of the organisation where zero risk exists. For the purpose of this strategy, risk is defined as:
"Risk is the "effect of uncertainty on objectives (ISO3100:2018)"
It is also often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

Risks take all forms including –

- Strategic
- Operational
- Health, Safety or Security
- Resources (people, finance)
- Assets (estate, hardware, equipment)
- ICT (including Cyber Security)
- Systems and processes
- Information Governance (data loss, breach, protection, mis-use)
- Governance (accountability, transparency, compliance, and business continuity)
- Credibility
- Third Party Providers
- Environmental and Climate Change

This is not a finite list but is included to reflect that all forms of risks are captured by this overarching Strategy. No risk, regardless of its origin, definition or nature stands outside this Strategy.

Good risk management also allows stakeholders to have increased confidence in the organisation's corporate governance and ability to deliver.[1]

MANAGING RISK THE ISO 31000 WAY

Managing risk is part of good governance and is fundamental to how an organisation is managed at all levels. Managing risk is part of all activities associated with an organisation and includes interaction with stakeholders; consideration of the external and internal context of the organisation, including behaviour and cultural factors.

ISO 31000: 2018 has three components for managing risk. These relate to

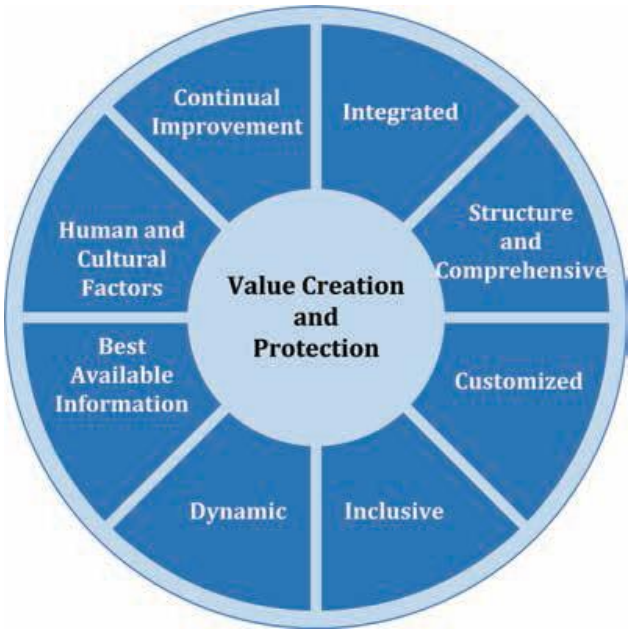
(i) the identification of core **principles of risk management** with the intention that these will be addressed by
(ii) the development of a **risk management framework.** In turn, the framework assists in managing risk through the
(iii) **risk management processes** as outlined in the ISO 31000 standard.

These are illustrated in diagrammatic format at Appendix 1.

PRINCIPLES OF RISK MANAGEMENT

To be fully effective any risk management process must satisfy a minimum set of principles or characteristics. These are shown in diagrammatic format in Figure 2 below. The principles are the foundation for managing risk and should be considered when establishing the organisation's risk management framework and processes and will help the organisation manage the effects of uncertainty on its objectives.

Figure 2 - Principles of Risk Management[2]



The principles are further explained below:

Integrated	Risk management should be integrated within all organisational activities.

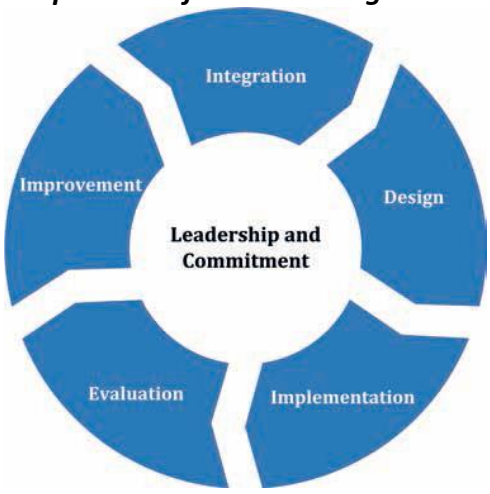
[2] Source – BSI ISO 31000:2018 – Risk Management Guidelines

Structured and comprehensive	A structured and comprehensive approach to risk management contributes to assurances in the Governance Statement.
Customised	The risk management framework and process should be customised and proportionate to the organisation's external and internal context related to its objectives.
Inclusive	Appropriate and timely involvement of stakeholders needs to be considered. This will better inform the organisation's risk management system.
Dynamic	Risks can emerge, change or disappear as an organisation's external and internal context changes. The risk management system needs to respond to these changes in a timely manner.
Best available information	Information should be timely, clear and available to relevant stakeholders.
Human and cultural factors	Human and cultural factors significantly influence all aspects of risk management.
Continual improvement	Risk management is continually improved through learning and experience and will feed into the organisation's quality improvement framework/systems.

RISK MANAGEMENT FRAMEWORK

Figure 3 below illustrates the elements of the second component - Risk Management Framework.

Figure 3 – Components of a Risk Management Framework[3]



Leadership and Commitment	Management needs to ensure that risk management is integrated into all organisational activities and

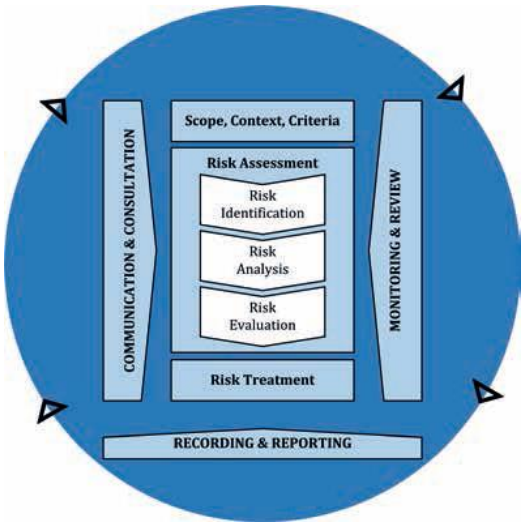
[3] Source – BSI ISO 31000:2018 – Risk Management Guidelines

	demonstrate leadership and commitment by implementing all components of the framework. This in turn will help align risk management with its objectives, strategy and culture.
Integration	Integrating risk management relies on an understanding of organisational structures and context. Risk is managed in every part of the organisation's structure. Everyone in an organisation has responsibility for managing risk.
Design	The organisation should examine and understand its external and internal context when designing its risk management framework.
Implementation	Successful implementation of the framework requires the awareness of all staff within the organisation.
Evaluation	The organisation should periodically measure its risk management framework against its purpose, implementation plans, risk management key performance indicators and expected behaviour. This will ensure it remains fit for purpose.
Improvement	The organisation should continually review, monitor and update its risk management framework to ensure it is fit for purpose.

THE RISK MANGAGEMENT PROCESS

The third component – Risk Management Process is outlined in diagrammatic format in Figure 4 below with short descriptors of each item.

Figure 4 – Risk Management Process[4]



[4] Source – BSI ISO 31000:2018 – Risk Management Guidelines

Communication and consultation	Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.
Scope, context and criteria	Scope, context and criteria involve defining the scope of the process and understanding the external and internal context.
Risk assessment	
Risk identification	Risk identification should be a formal, structured process that considers sources of risk, areas of impact and potential events and their causes and consequences.
Risk Analysis	Risks should be analysed by considering the consequences/severity of the risk and the likelihood/frequency that those consequences may occur. The risk criteria contained within the regionally agreed Risk Rating Matrix and Impact Assessment Table will provide a guide for analysis.
Risk Evaluation	Risk evaluation involves making a decision about the level of risk and the priority for attention through the application of the criteria developed when the context was established. This stage of the risk assessment process determines whether the risks are acceptable or unacceptable. Acceptable risks are those as outlined in the organisation's Risk Management Strategy i.e. its risk appetite.
Risk Treatment	The purpose of risk treatment is to select and implement options for addressing risk. Risk treatment involves an iterative process of: - formulating and selecting risk treatment options; - planning and implementing risk treatment; - assessing the effectiveness of that treatment; - deciding whether the remaining risk is acceptable; if not acceptable, take further treatment/action.
Monitoring and Review	Monitoring and review should take place in all stages of the process. Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback. The results of monitoring and review should be incorporated throughout the organisation's performance management, measurement and reporting activities.
Recording and Reporting	The risk management process and its outcomes should be documented and reported through appropriate mechanisms

DUTIES AND RESPONSIBILITIES FOR MANAGING RISK

To effectively manage the totality of risk management within the BSO, individuals, groups, and the Board are charged with responsibility for risk management relevant to their role and responsibilities.

BSO BOARD

As per the Code of Conduct and Accountability (July 2012), the Board is responsible for ensuring that the BSO has robust and effective arrangements in place for governance and risk management. The Board is similarly responsible for ensuring that the BSO has effective systems for identifying and managing all risks, financial and organisational. The BSO Risk Management process is outlined in Appendix 2. 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 has overall responsibility for risk management and is responsible for ensuring that the *Business Services Organisation* has a systematic programme of risk identification, assessment, management and quality improvement processes and procedures which shall be approved and monitored by the Governance and Audit Committee on behalf of the *Business Services Organisation*.

DIRECTOR OF STRATEGIC PLANNING AND CUSTOMER ENGAGEMENT

The Director of Strategic Planning and Customer Engagement is responsible for the administration of risk management including 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 the management of corporate risks. Directors are responsible for coordinating the operational elements of risk management within their Directorate/Service Area. They are responsible for:

- Identifying risks to service delivery through engagement with staff and service users;
- Ensuring that appropriate and effective risk management processes are in place within their designated area and scope of responsibility and that all staff are made aware of the risks within their work environment and of their

personal responsibilities, including designating risk manager roles where appropriate

- Appropriate population of their risk register in line with the Risk Management Strategy, and validating all risk scores attributed;
- Monitoring the implementation of risk action plans;
- Reviewing all risks on their risk register on at least a quarterly basis;
- Escalating risks, where appropriate for discussion at SMT;
- 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 & Risk Officer with evidence that these responsibilities have been met.

GOVERNANCE AND AUDIT COMMITTEE

The Governance and Audit Committee is responsible for reviewing the structures, processes and responsibilities for identifying and managing key risks facing the organisation, and receive periodic reports and assurance on risk which contribute to the assurances required for the Board.

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.

SENIOR MANAGEMENT TEAM

SMT is charged with supporting the Chief Executive in their responsibilities for risk, control and governance by:

- Gaining assurance that risk and change in risk is being monitored;
- Receiving the various assurances which are available about risk management and consequently delivering an overall opinion about risk management;
- Commenting on the appropriateness of the risk management and assurance processes which are in place.
- Reviews the Corporate Risk Register and challenges how risks are managed including the approval and escalation of risks and the closure of risks when that is deemed appropriate.

SMT 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 and that the risks to the achievement of those objectives are identified by developing both Corporate and Directorate or Service Area Risk Registers;
- Directing the annual programme for risk management activities and monitoring progress;
- Assessing the need for staff awareness and training with regard to Risk Management and Assurance;
- Reporting to the Governance & Audit Committee and Board so that the Board can assess the effectiveness of the controls and assurance given for the management of Risks throughout the Business Services Organisation.

ASSISTANT DIRECTOR OF STRATEGIC PLANNING AND CUSTOMER ENGAGEMENT

The Assistant Director of Strategic Planning and Engagement is responsible, through the Director of Strategic Planning and Customer Engagement for the design and oversight of the BSO's Risk Management Framework and manage the operational production of the Corporate Risk and Assurance Report and Service Risk Registers.

GOVERNANCE & RISK OFFICER

The Governance & Risk Officer is responsible for the maintenance of the BSO Corporate Risk Register and will monitor performance against risk action plans and report progress to the Senior Management Team. In conjunction with SMT, the Governance & Risk Officer will produce an Annual Risk Report.

In addition the Governance & Risk Officer 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 to highlight areas they believe need to be addressed. 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 that may be affected by service activity.

INTERNAL AUDIT

Internal Audit's primary objective is to provide independent assurance on the effectiveness of the risk management internal control framework (and, therefore, risk management) to both the BSO management and the Board through the Governance and Audit Committee. It does this by carrying out audits across the organisation focused on the key risks in the business area/organisation.

Internal Audit also has a key role to play in strengthening the overall process by monitoring, reporting and providing assurance on the effectiveness of the risk and control mechanisms in operation.
The system of internal control over risk management is subject to regular audit.

PREMISES COMMITTEE

The Director of Human Resources and Corporate Services is responsible for the operation of the premises, fire, health & safety & environment committee (known as the "Premises Committee') for 2 Franklin Street. Responsibilities of the Premises Committee include the review of Franklin Street risk assessment reports, accident/incident/near miss/fire reports/unannounced security and health and safety inspections within Franklin Street and ensure that any lessons learned and remedial follow up actions are implemented and shared with other local office Premises Committees as deemed appropriate. For all other BSO sites advice and guidance is provided on fire, health & safety and environment by the BSO Corporate Service Team.
Membership of the Management Group includes Corporate Services and representatives from Directorates/Service Areas, Trade Unions and customer organisations. Relevant Health & Safety issues are reported to the Senior Management Team of BSO.

BSO RISK APPETITE FRAMEWORK

ISO defines risk appetite as an *"organisation's approach to assess and eventually pursue, retain, take or turn away from risk.*[5]*"*

[5] ISO Guide 73:2009 Risk Management – Vocabulary

The BSO risk appetite is defined as follows:

> The BSO defines its overall risk appetite as cautious. This recognises the environment in which BSO operates and is cognisant of its role as an Arm's Length Body and the obligations that come with spending public money. The organisation is cognisant of its mission to deliver high quality business services; whilst balancing the need to invest, develop and innovate in order to achieve the best outcomes and value for money for our customers. The BSO acknowledges that whilst we have a cautious risk appetite in areas such as compliance e.g. legal, fraud, health and safety, we may adopt a more open approach depending on business need and the potential risk associated with the activity. For example, this may apply to our growth activities and in certain service areas e.g. ITS.

The BSO risk appetite is also defined in relation to the risk scoring matrix by way of the risk appetite line:

	Catastrophic	**5**	5	10	15	20	25
	Major	**4**	4	8	12	16	20
Impact	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 appetite line

More specifically, and in relation to the risk scoring matrix, we may be willing to accept risks which are assessed as medium or low after mitigation, in pursuit of objectives. The organisation will not, however, accept any risks that will be a 'high risk' after mitigation.

All risks on the Corporate Risk Register are assessed according to the risk appetite matrix (Appendix 3). SMT are responsible for reviewing the appetite of each risk.

Where Risk Appetite is breached this should be reported to the GAC and Board. Any movements in risk scores will be reported via SMT.

It is important to note that the risk matrix remains unchanged following the implementation of the Regional Risk Management Strategy. BSO endorsed the above risk matrix as it is appropriate to the unique organisational structure of BSO within Health and Social Care.

SHARED RISKS

The BSO recognises that it has a range of shared risks, in line with the nature of the organisation.

CUSTOMERS

Where risks exist to the BSO, these are also often risks to our customers; just as customers rely on the BSO to deliver an efficient, high quality service, the BSO often relies on customer organisations providing the right information on a timely basis, in order, for us to deliver that service.

SERVICE AND SUPPLY CONTRACTS

The BSO plans, coordinates and monitors the activities for service and supply contract companies to effectively minimise the risk, so far as is reasonable practicable, to staff, visitors and other persons including contractors' staff.

All service and supply contracts will be managed by the BSO Estates Manager who will monitor the work to ensure that it has been carried out, in accordance, with the contract and in full compliance with impacting Health & Safety Legislation. All Service & Supply Contracts include an Equality of Opportunity Contract Condition and the Estates Manager will outline to the contractor the expected Code of Conduct while on BSO premises and any health & safety issues pertinent to the work being undertaken. Where required, the Estates Manager will obtain Method Statements and Permits to Work from the contractor before work commences, in accordance, with the Health & Safety at Work Act. The BSO Estates team will then ensure that Directors are fully aware of any work being undertaken, the risks being introduced and how the work may affect the working environment and their staff, visitors and any other person in their place of work.

If an incident occurs, the BSO Health & Safety Manager will ensure that an Adverse Incident Report is completed and/or obtained from the contractor and processed, in accordance, with the Adverse Incident Reporting Policy.

PREMISES

The BSO directly manage a number of key properties. These are Franklin Street, Boucher Crescent, HSC Leadership Centre, Great Victoria Street (leased, Clarendon Dock (leased) and James House (leased). A significant proportion of BSO staff share accommodation in a landlord/tenant arrangement with other HSC organisations formalised through a Memorandum of Understanding.

With regard to 12- 22 Linenhall Street – arrangements for the ongoing management of this property remains with SPPG. Operationally the BSO manages the shared risks of our staff based in the building by means of:

- A shared estates service, including Planned Preventative Maintenance for plant and equipment;
- Common systems (fire safety, security) supplemented by joint operational procedures; and
- Representation on the SPPG Health & Safety Committee.

With regard to BSO Locations at other HSC, HSC Trusts, NICS and Commercial premises, the BSO manages the shared risks by:

- Promoting staff adherence to both BSO and local Trust policies;
- Engagement with the other Organisations to maintain facilities and IT infrastructure locally.

The Fire Safety Regulations (NI) 2010 states that all non-domestic premises are required to hold a valid fire safety risk assessment. For all rented accommodation, landlords will be required to provide documentation of their fire safety risk assessment to BSO Corporate Services who have corporate responsibility for Fire Safety.

BSO RISK REGISTER

The BSO's Risk Register is an integral part of the Assurance Process and is used as a mechanism for the Board, Governance & Audit Committee and SMT to assess the effectiveness of controls and assurances which have been identified to manage risks to the achievement of BSO objectives.

The Risk Register is operationally managed at two levels:

Corporate Risk Register, which quantifies strategic risks and outlines controls/ assurances and action plans approved by the Governance and Audit Committee to ensure the focused and effective management of these risks. It is comprised of risks that have been identified to the achievement of the BSO Strategic Objectives and other significant risks that have arisen. The Corporate Risk Register is operationally managed by SMT who review the risks on a monthly basis. A Corporate Risk &

Assurance report is presented quarterly to the Governance and Audit Committee and to the Board on a biannual basis.

Directorate/Service Risk Register, which quantifies all risks, sets out controls in place and determines the residual risk that remains. It is comprised of all the risks for each service within a Directorate and it is the direct responsibility of the various Directors to manage the risks in their respective areas. Action Plans are developed for all risks where these risks are being treated and progress monitored by Directors. Directorate/Service risk registers are operationally managed at local level and Assistant Directors /Senior Managers (also known as Risk Managers) will report at least quarterly to their Director and take ownership for the proactive management of risks, ensuring controls are reviewed and managed in a timely manner and actions identified to mitigate risk are completed within the agreed time period. Where considered appropriate, service areas may hold separate 'child' risk registers.

In accordance with the regional HSC Risk Management Model (Sept 2018), all risks are scored using the HSC Regional Risk Matrix which is based on the principles of the ISO 31000:2018 standard. There is an escalation process in place to allow risks, where relevant, to be escalated to/from Corporate / Service Risk Registers.

Project/Programme Risks
Risks specifically identified through projects/programmes will be managed through project/programme risk registers. Any risks that remain beyond the life of a project will be transferred to the most appropriate department/directorate/subject specific group risk register.
If, during the course of a BSO-led project or programme, a risk which is relevant to the BSO is identified, this should be shared with the most relevant service area/directorate and subsequently considered for addition to a risk register at the most appropriate level.

PROCESS FOR THE ASSESSMENT AND MANAGEMENT OF RISK

FIRST STAGE – IDENTIFYING RISKS

Risk identification should be a formal, structured process that considers sources of risk, areas of impact and potential events and their causes and consequences. Risks to the achievement of objectives should be identified at corporate and service level. By identifying key risks, steps can then be taken to either prevent the event occurring, or to minimise the impact.

The risks identified will be captured in standard format risk registers at corporate, service and, if necessary, project level.

To make sure that the identification of risks is as comprehensive as possible, cross divisional and partnership risks must also be considered.

The identification of risks is the responsibility of everyone and should be considered when making business decisions or embarking on a new approach. Furthermore it is important that the external environment and influences are also considered as these could impact the potential risks associated with service delivery. There should also be continuous assessment of risk; this can be done via regular review of the risk registers to ensure the appropriate associated risks have been identified, but also by including risk as a regular agenda item at team and management meetings to identify new risks which may have arisen. Risks should also been considered in the development and execution of the annual business plan and corporate plan. The risk register spreadsheet should be used and if necessary advice should be sought from the Governance and Risk Officer. Risks may also be identified through the following:

- Strategies, policies and procedures
- Resilience management
- Standards and accreditations
- Audit reports
- Horizon scanning and learning from others
- Complaints
- Adverse incidents
- Claims management
- Post event analysis

The Governance and Risk Officer works closely with the Board, GAC and Senior Management Team to capture strategic corporate risks. By presenting the corporate risk register monthly to the Senior Management Team meeting, quarterly to GAC, and biannually to Board, there is an opportunity for new and emerging risks to be discussed. The Governance and Risk Officer will then work with service areas to develop and capture associated risks as directed.

The BSO categorises risks under five key areas: namely Operational, Financial, Health & Safety, Compliance and Reputational. This is not an exhaustive list of all possible risk categories but broadly encompass risks faced by BSO. It is also recognised that risks can fall under more than one category.

Second Stage - Evaluating Risks

After identifying the risks, it is then necessary to evaluate those risks so that BSO has a means of comparing and prioritising risks. Risk evaluation involves making a decision about the level of risk and the priority for attention through the application of the criteria developed when the context was established. This stage of the risk assessment process determines whether the risks are acceptable or unacceptable.

Acceptable risks are those as outlined in the organisation's Risk Management Strategy i.e. its risk appetite.

The Risk Owner is responsible for evaluating each risk in terms of both:

Likelihood - The chance of the risk materialising after considering the control measures in place.
Impact - The effect of the risk should it materialise.

The impact of some risks, such as financial risks, may be quantifiable, whilst others, such as reputation risks, may be more subjective and difficult to quantify. To overcome this problem and to ensure that a consistent approach to evaluating risks is applied across the divisions an Impact Descriptors Matrix can be used. (Set out in appendix 4) This then feeds into the overall Risk Scoring Matrix for evaluating the risk.

When considering a risk it is important that scale-significance-severity is also considered. Actions and attention must be in proportion to the risk. Often cumulative risk can be overlooked and whilst an individual risk can appear relatively minor, if the same risk is repeated across a number of service areas then the cumulative affect can be significant.

For each risk, a risk score should initially be determined before any controls are applied. This is **the inherent or gross risk score**.

The **net risk score** can then be determined by assessing the likelihood and impact after the controls which are currently in place to address the risk have been applied.
The inherent/gross and net risk scores can then be used to prioritise all risks across the organisation.

A further "Target" score should be assessed to give a score for the level of risk which is likely to remain after all planned action has been taken. This will allow consideration of whether or not further control action is required.

The risk scoring matrix provided below should be used when scoring all new risks. The level of impact and likelihood of the event occurring should be combined to give an overall risk score:

impact					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	**2**	**3**	**4**	**5**

likelihood

Escalating Risks

The aim of risk management is not to eliminate risk but rather to manage risk within the agreed risk appetite. If action taken to manage risk does not bring the risk exposure to below the agreed risk appetite, the risk should be escalated to the next tier of management:

Risk Register	Risk escalated to	Register
Corporate	Board/GAC	Remains on the Corporate Risk Register
Service	Director	Escalate to SMT
Project/Programme	Appropriate Officer / Project Manager	Escalate to Director

Where a risk owner wishes to escalate a risk due to changes in the risk score or environment the below escalation process should be followed:

Escalating to…	Process	Approval by
Corporate	Risk Manager should engage with the Governance and Risk Officer and their Director. An option for escalating risks is included in the service risk register spreadsheet. The Governance and Risk Officer will contact the appropriate Service Area to confirm that they have Director level approval to escalate their risk. Once this has been confirmed a Proposed New Risk Template is completed and presented to SMT for their consideration and approval. Once approved the risk is included in the Corporate Risk and Assurance Report for GAC/Board. If a risk is escalated onto the corporate risk register, it should no longer be included on a service risk register.	GAC/Board
Service	The risk identifier should contact the risk manager outlining the risk. The Risk Manager should then review and include on the service risk register if appropriate or advise decision.	Risk Manager

Escalating to…	Process	Approval by
Project	The risk identifier should contact the Project Manager outlining the risk. The Project Manager should then review and include on project risk register if appropriate or advise decision.	Project Manager

Third Stage – Risk Appetite

The BSO has established a risk appetite – this is the amount of risk that BSO is willing to be exposed to. The appetite associated with each risk should be considered in line with the Regional Risk Appetite Matrix (appendix 3) and included in the Corporate Risk Register. The agreed risk appetite should support risk owners when making decisions about how to manage the risk or the level of mitigation required.

Fourth Stage - Managing Risks

There are a number of valid responses to risk management as set out below. In choosing the most appropriate response, consideration should be given to the level of appetite the organisation has set.

For each risk, the Risk Owner should select one or a combination of the following responses:

Managing Risk Responses

Response	Details
Transfer	The risk is transferred to a third party e.g. insurance or delivery partner through Service Level Agreements
Tolerate/ accept	A business decision could be taken to accept the risk i.e. no action is taken to mitigate or reduce the risk. This could be, for example, due to cost factors to mitigate the risk or the risk likelihood being very low. It is important that the risk is monitored to ensure it remains tolerable and no factors result in the risk becoming more significant.
Treat	Take action to reduce the likelihood of the risk occurring or the impact of the risk should it occur (Internal Controls)
Terminate	It may be necessary to eliminate the risk perhaps by doing things differently. This could be done by altering a process to remove the

Response	Details
	risk associated with it. Where this can be done without materially affecting the business it should be employed.
Take the opportunity	Take the opportunity the risk presents – are there any positive opportunities to be gained as part of the risk management process

Where the decision is taken to treat a risk then it should be captured on an appropriate risk register with an action plan.

Fifth Stage - Risk Monitoring and Review

Assurance regarding the effectiveness of the risk management policy is gained through the annual risk management systems audit by Internal Audit
In addition, the corporate risk register and service risk registers are subject to regular monitoring. The corporate risk register is reported to SMT on a monthly basis, GAC on a quarterly basis and Board on a biannual basis. A service risk report is also submitted to SMT and GAC on a regular basis.

RISK MANAGEMENT ACTION PLAN

The BSO will develop an annual Risk Management Action Plan as part of the Annual Risk Report, which will practically demonstrate how the BSO will implement its strategy on risk for the coming year.

RISK TRAINING AND SUPPORT

Knowledge of risk management is essential to the successful embedding and maintenance of effective risk management. In general, training is required as follows:

- high level awareness of risk management for the Board and senior staff;
- management of risk register for staff involved in risk management;
- generic risk awareness training to ensure that staff, where required, are trained in risk identification, assessment and management; this can be delivered either by e-learning or risk awareness sessions;

The BSO will ensure that the delivery of training will take into account the diverse needs of staff. The current training structure is set out below:

SUPPORTING AND RELATED POLICIES & PROCEDURES

This strategy is supported by a number of procedures covering specific areas of risk, and is related to a number of other BSO policies that have elements of risk management within them. Titles and scheme of delegation for approval are outlined in the following tables.

Table 1 Supporting Documents

Document Name	Approval	Owner
Procedures for the Management of Risk Registers	SMT & G&AC	Director of Strategic Planning and Customer Engagement

Table 2 Related Documents

Document Name	Approval	Owner
Complaints Policy	Board	Dir of HRCS
Adverse incident Policy	Board	Dir of HRCS
Information Assurance Policy	Board	Dir of HRCS
Zero Tolerance Policy	Board	Dir of HRCS
Health & Safety Policy	Board	Dir of HRCS
Fraud Policy and Response Plan	Board	Dir of Finance
Claims Management Policy	Board	Interim Chief Legal Advisor
Information Governance Policy	Board	Dir of HRCS
Information Governance Assurance Framework	Board	Dir of HRCS
Information Risk Management Policy	Board	Dir of HRCS

EQUALITY SCREENING

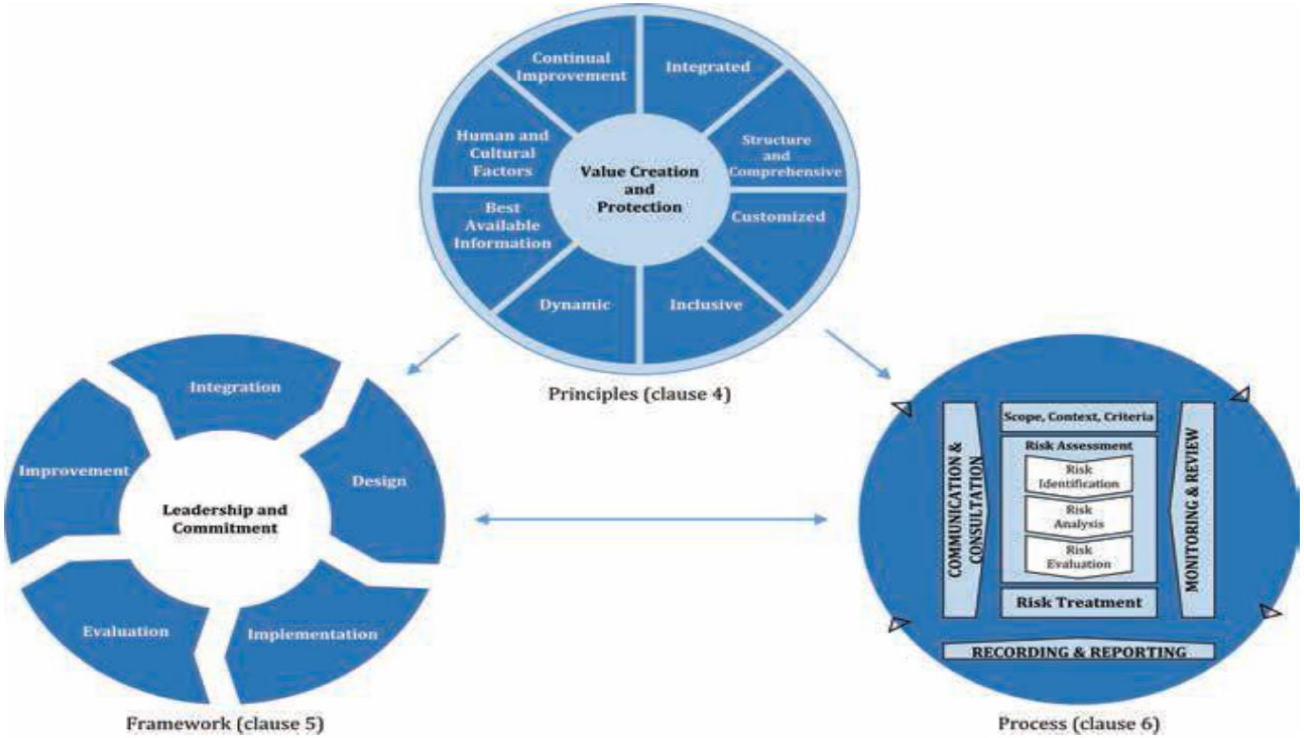
This strategy will be screened for equality implications as required by Section 75 of the Northern Ireland Act 1998 and for compliance with human rights and disability legislation. Documentation to evidence the screening will be produced and made publicly available.

Any request for the document in another format or language will be considered.

Please contact Strategic Planning and Customer Engagement Directorate:

2 Franklin Street; Belfast; BT2 8DQ;
Email: joanne.martin@hscni.net
Phone: 028 9536 3798

APPENDIX 1 - PRINCIPALS, FRAMEWORKS AND PROCESSES FOR RISK MANAGEMENT[6]

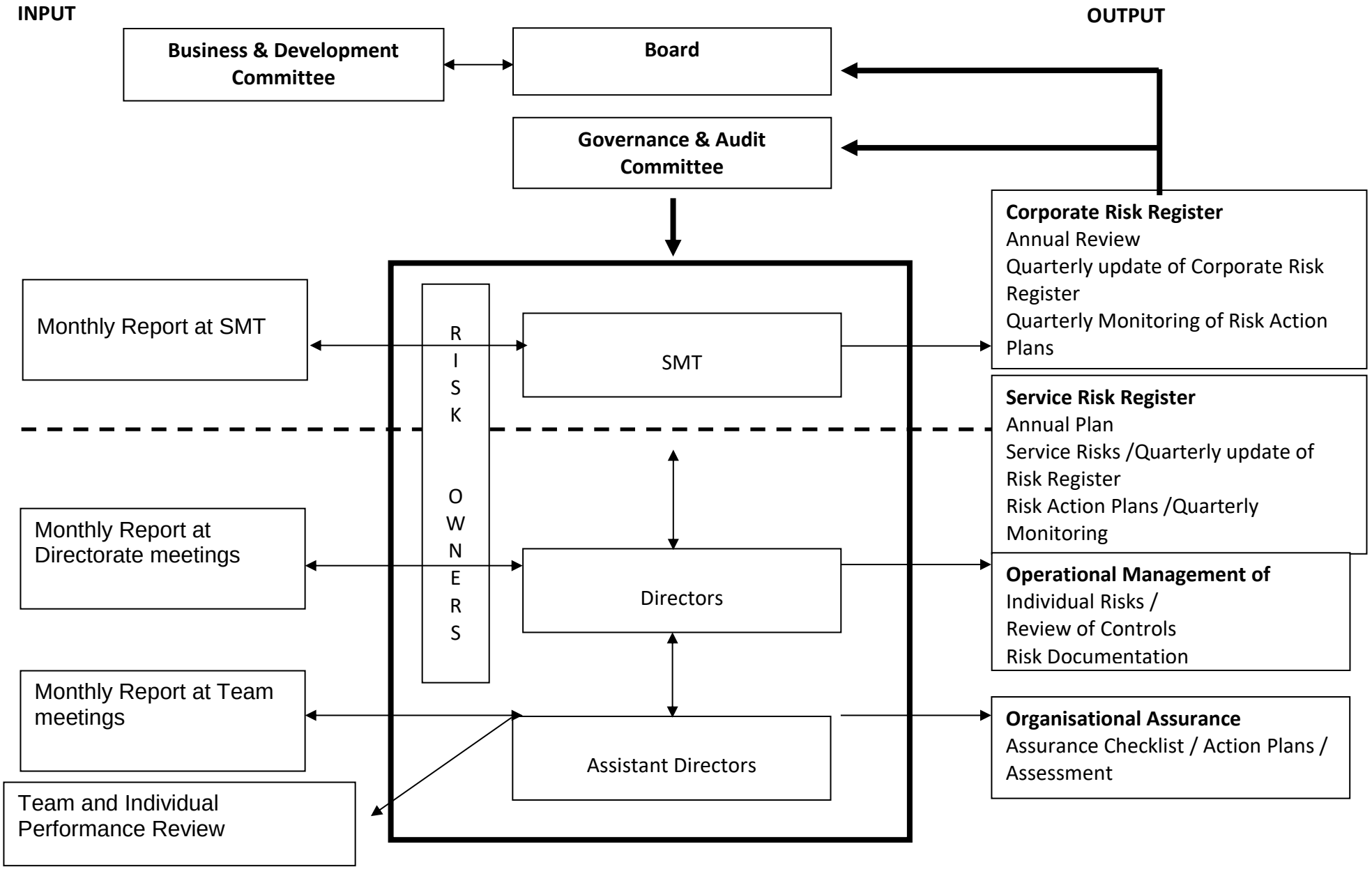


[6] Source – BSI ISO 31000:2018 – Risk Management Guidelines

Business Services Organisation

INVESTORS IN PEOPLE®
We invest in people Silver

Appendix 2 – Risk Management Process



APPENDIX 3 - RISK APPETITE MATRIX

This matrix [7]should be used as guidance for assessing risk appetite in conjunction with the Risk Appetite Statement

	Averse	**Minimalist**	**Cautious**	**Open**	**Hungry**
	Avoidance of risk and uncertainty is a key Organisational objective	**Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have a potential for limited reward.**	**Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.**	**Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money etc.).**	**Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk).**
Reputation	Minimal tolerance for any decisions that could lead to scrutiny of the Organisation, HSC, Government or the Department.	Tolerance for risk taking limited to those events where there is no chance of any significant repercussion for the Organisation, HSC, Government or the Department.	Tolerance for risk taking limited to those events where there is little chance of any significant repercussion the Organisation, HSC Government or the Department should there be a failure.	Appetite to take decisions with potential to expose the Organisation, HSC, Government or the Department to additional scrutiny but only where appropriate steps have been taken to minimise any exposure.	Appetite to take decisions that are likely to bring scrutiny of the Organisation, HSC, Government or the Department but where potential benefits outweigh the risks.

[7] *7 Adapted from Managing your risk appetite: A practitioner's guide, HM Treasury, Nov 2006.*

Operational	Defensive approach to objectives – aim to maintain or protect, rather than to create or innovate. Priority for tight management controls and oversight with limited devolved decision making authority. General avoidance of systems / technology developments.	Innovations always avoided unless essential. Decision making authority held by senior management. Only essential systems / technology developments to protect	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Systems / technology developments limited to improvements to protection of current operations.	Innovation supported, with demonstration of commensurate improvements in management control. Systems / technology developments considered to enable operational delivery. Responsibility for non-critical decisions may be devolved	Innovation pursued – desire to 'break the mould' and challenge current working practices. New technologies viewed as a key enabler of operational delivery. High levels of devolved authority – management by trust rather than tight control.
Financial	Avoidance of financial loss is a key objective. Only willing to accept the low cost option. Resources withdrawn from nonessential activities.	Only prepared to accept the possibility of very limited financial loss if essential. VfM is the primary concern.	Prepared to accept the possibility of some limited financial loss. VfM still the primary concern but willing to also consider the benefits. Resources generally restricted to core operational targets.	Prepared to invest for reward and minimise the possibility of financial loss by managing the risks to a tolerable level. Value and benefits considered (not just cheapest price). Resources allocated in order to capitalise on potential opportunities.	Prepared to invest for the best possible reward and accept the possibility of financial loss (although controls may be in place). Resources allocated without firm guarantee of return – 'investment capital' type approach.
Compliance	Avoid anything which could be challenged, even unsuccessfully Play safe.	Want to be very sure we would win any challenge.	Limited tolerance for sticking our neck out. Want to be reasonably sure we would win any challenge.	Challenge will be problematic but we are likely to win it and the gain will outweigh the adverse consequences.	Chances or losing are high and consequences serious. But a win would be seen as a great coup.

APPENDIX 4 - IMPACT DESCRIPTOR MATRIX

	1	2	3	4	5
Descriptors	**Insignificant /**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Operational - Service Provision (Internal and 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 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 Financial – Service level	Insignificant impact on ability to meet financial breakeven Target Insignificant cost	Minor impact on ability to meet Breakeven Target Less than 5% over budget	Moderate impact on ability to meet Breakeven Target 5-10% over budget	Major impact on ability to meet Breakeven Target 10-20% over budget	Breakeven Target cannot be met More than 25% over Budget
Reputation	Rumours Little impact on confidence levels	Elements of stakeholders expectation not being met – minor issues can be	Service below reasonable stakeholders expectation – moderate issues can be	Service well below reasonable stakeholders expectation leading to formal	Service drastically below reasonable stakeholders expectation which leads to

		addressed at Service level Minor impact on confidence levels	addressed at Directorate level Confidence in the BSO could be undermined	complaint raised to CX Confidence in the BSO undermined	departmental intervention Questions in Assembly PAC Enquiry
Compliance - 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 / Human Rights / Health & Safety / Freedom of Information / Data Protection and Organisational Assurances