RISK MANAGEMENT

Statement of Standard

An independently assured risk management system is in place that conforms to the principles contained in AS/NZS 4360:2004, and which meets HSC and other requirements in respect of managing risks, hazards, incidents, complaints and claims.

Overview

This Standard is principally concerned with ensuring that all the Department's arm's length bodies (ALBs) – ie HSC bodies, the Northern Ireland Fire and Rescue Service (NIFRS), the Regulation and Quality Improvement Authority (RQIA), the Northern Ireland Social Care Council (NISCC) and the Northern Ireland Practice and Education Council for Nursing and Midwifery (NIPEC) – have the basic building blocks in place for managing risk through development and implementation of a comprehensive risk management system.

This Standard, together with the Governance and Financial Management Standards, provides the basis for statutory reporting for the Governance Statement as set out by the Department of Finance in Managing Public Money NI A3.1 : Governance Statement

https://www.finance-ni.gov.uk/publications/managing-public-money-ni-chapter-3-and-associated-annex

Subsequent to this, new requirements were introduced for 2008/09 by Circular HSS(F) 19/09 in mitigating information risks. From 2009/10, each ALB is required to provide a mid-year assurance statement from the accounting officer attesting to the robustness of the organisation's system of internal control. The adoption of an Assurance Framework, to assist boards in the control of risks to strategic objectives, has also been made mandatory from April 2009.

Risk management should be recognised within an organisation as an integral part of good practice and should be part of the organisation's culture. It should be integrated into its philosophy, practices and business plans, and not be viewed or practised as a separate programme. When this is achieved, risk management becomes the business of everyone in the organisation.

Business continuity management is complementary to risk management. Having an appropriate business continuity management plan will contribute a response to specific risks and also to the overall risk awareness of the organisation. However the primary driver for business continuity management planning is on maintaining the organisations' ability to deliver its critical functions for a defined period. Like risk management, business continuity management should be seen as a core element of normal good management practice.

Whilst this standard does address key issues, it does not purport to be exhaustive. The boards of HSC bodies, NIFRS, RQIA, NISCC, and NIPEC should satisfy themselves that all relevant internal control and risk management requirements incumbent upon them, including those associated with the duty of quality, are properly identified and suitably addressed. When addressing risks to the organisation, in particular those which the organisation deems high/extreme to the achievement of key objectives, the risk and actions identified across other organisational controls assurance standards need to be considered.

The design of a risk management system will be influenced by and tailored to the existing structure of the individual body, the services provided and the processes and specific practices followed. A specific risk management approach applicable to all organisations is, therefore, unlikely to be serviceable. However, common principles can be identified and used to form the basis for the Standard. These in large part originate from the Australia/New Zealand Standard on risk management, which defines a set of generic principles for establishing a risk management system in any organisation. The Standard has been licensed for the HSC and the full Standard has been made available to all relevant bodies, which are encouraged to make use of the information and guidance contained in AS/NZS 4360:2004. Only 10% or less of the standard's definitions and references should be extracted and used within internal policy and procedure documents.

KEY REFERENCES

Statutes

Statutory Instruments: The Health and Personal Social Services (Quality, Improvement and Regulation) (Northern Ireland) Order 2003 SI 2003/431 (NI 9)

Statutory Rules: Social Security (Claims and Payments) Regulations (Northern Ireland) 1977 No.351

Statutory Rules: Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (Northern Ireland) 1997 No.455

Guidance and Codes

HPSS Complaints Procedures Directions (Northern Ireland) Order 1996

The Miscellaneous Complaints Procedures Directions (Northern Ireland) 1996

HPSS (Special Agencies) Complaints Procedures Directions (Northern Ireland) 1996

Standards Australia Risk Management AS/NZS 4360:2004

HSC	Controls Assurance Standard	Risk Management

NHS Good Practice Guide for Convenors, October 1999

Complaints in Health and Social Care – Standards and Guidelines for Resolution and Learning

Financial Reporting Council:

Health Estates (various) Firecode (Northern Ireland)

Department of Health, Social Services and Public Safety (2004): Guidance Note – Implementing the Equality Good Practice Reviews

ALARM /UCL - Clinical incident investigation protocol

NHS Resilience and Business Continuity Management Guidance –

DHSSPS Hospital Lockdown Guidance for Health and Social Care Trusts –

Circulars

Circular HSS (PDD) 1/1994 - Management of Food Services and Food Hygiene in the HPSS

Circular HSS (THR) 1/1999 – Management of Food Services and Food Hygiene in the HPSS

Circular HSC (SQSD) 5/10 – Handling Clinical and Social Care Negligence and Personal Injury Claims

Circular HSS (F) 19/2000 – Clinical Negligence Central Fund: Accounting Arrangements

Managing Public Money NI A3.1 : Governance Statement
https://www.finance-ni.gov.uk/publications/managing-public-money-ni-chapter-3-and-associated-annex

Circular HSS (PPM) 4/2005 – AS/NZS 4360: 2004 – Risk Management

Circular HSS (PPM) 8/2002 – Risk Management in the Health and Personal Social Services
htm

Circular HSS (PPM) 10/2002 – Governance in the HPSS: Clinical and Social Care Governance - Guidance on Implementation

HSC	Controls Assurance Standard	Risk Management

Circular HSS (PPM) 13/2002 – Governance in the HPSS – Risk Management

The Northern Ireland Adverse Incident Centre (NIAIC) operates as a function of the DoH with the objective of taking all reasonable action within its remit to safeguard the health of HSC service-users and staff through the provision of a regional centre for the voluntary reporting and investigation of adverse incidents involving medical devices, non-medical equipment, plant and building elements and for providing relevant safety guidance in relation to these items.

Circular HSS(SM) 4/2003 – Code of Conduct for HPSS Managers
Department of Health, Social Services and Public Safety (2003): Code of Conduct for HPSS Managers

Circular HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance

Managing Public Money NI A3.1 : Governance Statement
https://www.finance-ni.gov.uk/publications/managing-public-money-ni-chapter-3-and-associated-annex

Circular HSS(SQSD) 18/2007 – Conducting Patient Safety Reviews/Lookback Exercise

Circular HSS(SQSD) 18/2007 – Guidance Document – A Practical Guide to Conducting Patient Safety Reviews or Lookback Exercises

Circular HSS(SQSD) 34/2007 – Guidance Document

Circular HSC(SQSD) 22/2009 – Learning from Adverse Incidents and Near Misses reported by HSC organisations and Family Practitioner Services

Circular HSC (SQSD) 08/2010 – Phase 2 – Learning from Adverse Incidents and Near Misses reported by HSC organisations and Family Practitioner Services

Circular HSS (PPM) 8/2004 – Governance in the HPSS: Controls assurance standards – update

Other Publications

Lord Woolf's Report (1996) 'Access to Justice'. The Stationery Office, London

HSC	Controls Assurance Standard	Risk Management

National Audit Office 2000, *Supporting Innovation: Managing risk in government departments.* The Stationery Office, London, HC 86f4 Session 1999-2000

Best Practice – Best Care (2001): A framework for setting standards, delivering services and improving monitoring and regulation in the HPSS.

HM Treasury (2001) *Management of Risk: A Strategic Overview*

Health & Safety Executive (2003): 'Interventions to control stress at work in hospital staff'. The Health & Safety Executive, London

HM Treasury (2004): *Managing risks with delivery partners*

Quality Standards for Health and Social Care: supporting good governance and best practice in the HPSS

Safety First: a framework for sustainable improvement in the HPSS

An Assurance Framework: a Practical Guide for Boards of DoH Arm's Length Bodies

INDEX OF RISK MANAGEMENT CRITERIA

Criterion 1 (*Board accountability*)

Board level responsibility for risk management, including business continuity, is clearly defined and there are clear lines of individual accountability for managing risk throughout the organisation, leading to the board.

Criterion 2 (*Organisation-wide risk management processes*)

The organisation's senior management has defined and documented its strategy for managing risks, including objectives for, and its commitment to, risk management. The risk management strategy is relevant to the organisation's strategic context and its goals, objectives and the nature of its business. Management ensures that the strategy is understood, implemented and maintained at all levels of the organisation.

Criterion 3 (*Organisation-wide accountability*)

A committee structure is in place, which supports the risk management accountability arrangements within the organisation and ensures that all significant risks are properly considered and communicated to the board.

Criterion 4 (*Adverse incidents*)

An agreed process for reporting, managing, analysing and learning from adverse incidents is in place, in accordance with HSC guidance.

Criterion 5 (*Complaints and claims*)

An agreed process for reporting, managing, analysing and learning from complaints and claims is in place, in accordance with HSC guidance.

Criterion 6 (*Risk management process*)

A risk management process, based on the requirements of AS/NZS 4360:2004 and covering all risks, is embedded throughout the organisation at all levels, including the board, with key indicators being used to demonstrate performance. The whole system of risk management is continuously monitored and reviewed by management and the board in order to learn and make improvements to the system.

Criterion 7 *(Business Continuity Management)*

Business continuity management plans aligned to the International Standard on Business Continuity Management Systems (ISO 22301) are in place and can be activated in order to protect and maintain essential services to a pre-defined level through a business disruption.

Criterion 8 (*Capability*)

All employees, including members of the board, clinical and social care professionals, managers, bank, locum and agency staff, together with (where relevant) contractors and volunteers are provided with appropriate risk management and business continuity management training.

Criterion 9 (*Independent assurance*)

The board receives independent assurance(s) that a risk management system is in place that meets the requirements of this standard.

CRITERION 1

Board level responsibility for risk management, including business continuity, is clearly defined and there are clear lines of individual accountability for managing risk throughout the organisation, leading to the board.

Source

- Standards Australia Risk Management AS/NZS 4360: 2004
- Circular HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance
- Circular HSS(SM) 4/2003 – Code of Conduct for HPSS Managers. DHSSPS(2003): Code of Conduct for HPSS Managers

Guidance

Implementation of risk management programmes at all levels, especially at the corporate level, is a challenge for all managers. Its success will depend largely on the support of the Chief Executive and senior management team. Critical to this process is the involvement of clinical and social care professionals – nursing, medical, social services, pharmacy and allied health professionals.

The ultimate goal of any risk management programme is to make the effective management of risk an integral part of everyday practice. This can only be achieved if there is a comprehensive and cohesive risk management system in place, underpinned by clear accountability arrangements throughout the management organisational structure.

The following sub-criteria will help in deciding whether the key requirements of the main criterion are being met:

- The Chief Executive has overall responsibility for risk management.
- An Executive Director, who may be the Chief Executive, has been designated accountable for the implementation of risk management and controls assurance
- A risk management strategy has been approved by and is owned by the board.
- Clear lines of accountability for risk management have been established throughout the organisation.
- One or more persons are charged with the responsibility for advising on and co-ordinating risk management activities. The designated Executive Director should be consulted on the strategic direction of all such activities.

Examples of Verification

- Risk management strategy has been approved by the board;
- Job descriptions for executive directors and senior managers;
- Job descriptions for specialist risk management advisors or governance managers;
- Risk management organisational chart;
- Assurance Framework in place and in operation;
- Terms of reference for the exclusively non-executive audit committee;
- Minutes of the audit committee;
- Terms of reference of the board sub-committee(s) responsible for overseeing risk management;
- Minutes of the board sub-committee(s) responsible for overseeing risk management;
- Minutes of the board;
- Copy correspondence or minutes of meetings of the executive directors with responsibility for risk management;
- Audits/checks of compliance with risk management objectives, financial, organisational and clinical and social care.

CRITERION 2

The organisation's senior management has defined and documented its strategy for managing risks, including objectives for, and its commitment to, risk management. The risk management strategy is relevant to the organisation's strategic context and its goals, objectives and the nature of its business. Management ensures that the strategy is understood, implemented and maintained at all levels of the organisation.

Source

- Standards Australia Risk Management AS/NZS 4360: 2004
- Managing Public Money NI A3.1 : Governance Statement
- Assurance Framework in place.

Guidance

Management of risk should be integrated into the philosophy of an organisation. A risk management strategy should be developed, which provides the organisation with strategic direction.

The following sub-criteria will help in deciding whether the key requirements of the main criterion are being met:

- There is a board-approved strategy for risk management which promotes integrated governance and which is reviewed annually.
- The risk management strategy includes a list of key objectives for managing risk and is relevant to the organisation's strategic aims and objectives and the nature of its services.
- The strategy takes a holistic approach to the management of risk across the organisation and sets out the organisation's attitude to risk.
- The strategy clearly describes the process for reviewing the organisation's performance with regard to the management of risk.
- The strategy contains guidance on acceptable risk and for the management of situations in which control failure leads to material realisation of risk.
- The strategy includes reference to other risk management policies/procedures.
- Individual directorates/departments maintain local strategies that reflect their individual risk profile.
- The strategy specifies how new activities should be assessed for risk and incorporated into risk management structures.
- The strategy makes reference to and considers appropriately shared risks and those owned elsewhere (eg by independent contractors)

Examples of Verification

- Risk management strategy;
- Minutes of the board;
- Assurance Framework in place and in operation;
- List of internal and external stakeholders;
- Evidence of the risk management strategy being linked to the strategic/corporate plan;
- Specialist risk management policies and procedures;
- Risk management organisational chart;
- Evidence of strategy distribution to staff and its availability to other stakeholders;
- Local risk management strategies

CRITERION 3

A committee structure is in place, which supports the risk management accountability arrangements within the organisation and ensures that all significant risks are properly considered and communicated to the board.

Source

- Standards Australia Risk Management AS/NZS 4360: 2004
- Circular HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance
- Circular HSS(SM) 4/2003 – Code of Conduct for HPSS Managers. DHSSPS(2003): Code of Conduct for HPSS Managers
- Managing Public Money NI A3.1 : Governance Statement
- Audit Committee Handbook, April 2013 – HM Treasury

Guidance

The full benefit of risk management will only be achieved if there is a comprehensive and cohesive system in place, underpinned by an organisation-wide risk management structure.

To ensure that all significant risks are properly considered and communicated to the board, boards of HSC bodies should ensure that they have a sub-committee for overseeing risk management within their organisations.

Departmental guidance concerning the composition, modus operandi etc of this sub-committee is currently under review. Pending revised guidance, the following sub-criteria will continue to help in deciding whether the key requirements of the main criterion are being met:

- There is a board sub-committee(s) responsible for overseeing all aspects of risk management.
- The role and responsibilities of the committee(s) responsible for overseeing risk management activities are clearly defined to ensure that an integrated governance approach is being taken and that any necessary separations of clinical and social care, financial and organisational risks are kept under review.
- The Executive Director designated with responsibility for specific aspects of risk management must be a member of the committee.
- There is at least one Non-Executive Director as a member of the committee.
- The Committee's responsibility includes organisation-wide co-ordination and prioritisation of risk management issues.
- The committee(s) responsible for risk management issues oversee the work of any specialist risk management groups, and these specialist groups report directly to it.

- The role of the Audit Committee in reviewing and providing verification on the systems in place for risk management is clearly defined.

Examples of Verification

- Risk management strategy;
- Terms of reference for committees;
- Risk management organisational chart;
- Minutes of meetings;
- Annual risk management reports;
- Schemes of delegation;
- Annual report;
- Committee objectives;
- Agendas and supporting documentation
- RQIA assessment (for HSC bodies)

CRITERION 4

An agreed process for reporting, managing, analysing and learning from adverse incidents is in place, in accordance with HSC and NIFRS guidance.

Source

- Standards Australia Risk Management AS/NZS 4360: 2004.

- Circular HSS (PPM) 10/2002 – Governance in the HPSS: Clinical and Social Care Governance - Guidance on Implementation.
- Health Estates, Northern Ireland Adverse Incident Centre (NIAIC), Reporting Adverse Incidents and Disseminating Medical Devices/Equipment Alerts DB(NI) 2008 (01).
- DHSSPS, 2001 – Guidance for reporting accidents with, and defects in, medicinal products
- Managing Public Money NI A3.1 : Governance Statement
- Safety First: a framework for sustainable improvement in the HPSS
- Circular HSS(SQSD) 18/2007 – Guidance Document on Conducting Patient Safety Reviews/Lookback Exercise
- Circular HSS(SQSD) 34/2007 – Guidance Document on HSC Regional Template and Guidance for Incident Review Reports
- Circular HSC(SQSD) 22/2009 – Learning from Adverse Incidents and Near Misses reported by HSC organisations and FPS
- Circular HSC (SQSD) 08/2010 – Phase 2 – Learning from Adverse Incidents and Near Misses reported by HSC organisations and Family Practitioner Services

Guidance

Incident reporting is a fundamental tool of risk management, the aim of which is to collect information about adverse incidents, including near misses and hazards, which help to facilitate wider organisational learning.

Incidents and their consequences, if not properly managed, may result in loss of public confidence in the organisation, loss of assets and unnecessary proliferation of loss.

The following sub-criteria will help in deciding whether the key requirements of the main criterion are being met:

- There is a board-approved policy/procedure for recording, reporting, analysing and managing incidents and that these are treated in accordance with DoH guidance.

- The policy/procedure is based upon a standard definition of incidents
- The policy/procedure promotes a positive and non-punitive approach towards incident reporting.
- The policy/procedure states that all incidents must be reported promptly and an incident form completed and submitted to the risk manager (or equivalent).
- The policy/procedure contains clear guidance to be followed on incident investigation and root cause analysis.
- The policy/procedure states that management actions and preventative measures taken must be recorded.
- For adverse incidents that could have an impact or 'adverse effect' upon staff, users or the public, the policy/procedure requires a mechanism to be in place to inform the board. Furthermore the senior manager at board level who has overall responsibility for the reporting and management of adverse incidents within the organisation should consider the incident against the provisions of Circular HSC (SQSD) 08/2010 and take action accordingly.
- All incidents are reported on a standard form(s), which may be paper-based or electronic, and which captures a 'minimum dataset' of information in accordance, where relevant, with HSC guidance.
- All reported incidents are graded according to severity of outcome and potential future risk to users and/or the organisation.
- Based on the grading, reported incidents are subject to an appropriate level of local investigation and causal analysis and, where relevant, an improvement strategy is prepared, implemented and monitored.
- All reported incidents and causal factors are classified and categorised in accordance with a standardised classification scheme.
- Aggregate reviews of local incident data/information are carried out on an ongoing basis and the significant results are communicated to local stakeholders.

Examples of Verification

- Incident reporting policy/procedure;
- Incident report form and guidelines for completion;
- Incident investigation reports;
- Trend analysis reports;
- Minutes of the committees responsible for overseeing risk management;
- Copies of relevant reports to the DoH and to other external bodies and stakeholders;
- Induction training programmes;
- Completed incident report forms;
- Relevant correspondence;
- Action plans and follow up reports;
- Major incident policy;
- RQIA assessment (for HSC bodies).

CRITERION 5

An agreed process for reporting, managing, analysing and learning from complaints and claims is in place, in accordance with guidance.

Source

- Standards Australia Risk Management AS/NZS 4360: 2004.
- Complaints in Health and Social Care – Standards and Guidelines for Resolution and Learning.
- Circular HSC(SQSD) 23/2009 – Guidance on Complaints Handling in Regulated Establishments and Agencies.
- Circular HSC(SQSD) 34/2007 – HSC Regional Template and Guidance for Incident Investigation/Review Reports
- Circular HSC (SQSD) 08/2010 – Phase 2 –Learning from Adverse Incidents and Near Misses reported by HSC organisations and Family Practitioner Services
- Circular HSC (SQSD) – Handling Clinical and Social Care Negligence and Personal Injury Claims
- Circular HSS (PPM) 10/2002 – Governance in the HPSS: Clinical and Social Care Governance - Guidance on Implementation.
- DHSSPS (2004): Guidance Note – Implementing the Equality Good Practice Reviews
- Safety First: a framework for sustainable improvement in the HPSS

Guidance

Competent handling of complaints can assist in improving the quality of care and minimising claims by listening to the voice of service users and using this as an opportunity for the organisation to learn from complainants. Complaints and claims when examined in conjunction with reported incidents, accidents and near misses allow trends to be identified at both a local and regional level. This leads to prevention of recurrence or of more serious incidents and complaints occurring.

The following sub-criteria will help in deciding whether the key requirements of the main criterion are being met:

- There is a documented complaints procedure, which meets HSC requirements and is approved by the board.
- There is a designated complaints manager responsible for co-ordinating the local complaints arrangements and managing the process
- There is a designated senior person within the organisation with responsibility for the local complaints procedure.

- The arrangements for making complaints are publicised to service users.
- Front line staff receive training and guidance on the complaints procedure to enable them to deal with complaints on the spot.
- The organisation has an effective system for the recording of complaints.
- The organisation monitors how it, or those providing care on its behalf, deals with, and responds to, complaints.
- The organisation learns from complaints and improves services as a result.
- Independent review panelsare in place in full accordance with the HPSS Complaints Procedure (1996).
- All reported complaints are graded according to severity as well as potential future risk to users and/or to the organisation.
- One or more persons are charged with the responsibility for the management and co-ordination of claims.
- There is a documented claims management procedure, which meets HSC requirements and is approved by the Board.
- All reported claims are graded according to severity as well as potential future risk to users and/or to the organisation.
- Information on complaints is reported to and considered by a relevant sub-committee of the Board.

Examples of Verification

- Complaints policy/procedure;
- Compliance with the standards for complaints handling;
- Claims handling policy/procedure;
- Evidence of dissemination of learning within the organisation and use of the Equality Good Practice Review on the handling of complaints
- Job descriptions;
- Annual/Board reports;
- Reports of the committee responsible for overseeing risk management;
- Complaints committee reports
- Training needs analysis;
- Training programmes;
- Training evaluation forms;
- Induction programme;
- Complaints leaflets and posters;
- Complaints files;
- Customer feedback;
- Independent review reports (including those from RQIA);
- Evidence of claims management training;
- Evidence of claim settlement negotiations.

CRITERION 6

A risk management process, based on the requirements of AS/NZS 4360:2004 and covering all risks, is embedded throughout the organisation at all levels, including the board, with key indicators being used to demonstrate performance. The whole system of risk management is continuously monitored and reviewed by management and the board in order to learn and make improvements to the system.

Organisations should be aware that the AS/NZS 4360:2004 has been superseded by a new International Standard on Risk management. The Department has a license that allows organisations to reproduce and extract 10% or less of the AS/NZS 4360:2004 definitions and references. This license will expire in 2018. It should be noted that over the forthcoming years the Department in discussion with organisations will determine the appropriate way forward in relation to risk management.

Source

- Circular HSS (PPM) 8/2002 – Risk Management in the Health and Personal Social Services.
- Circular HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance
- Managing Public Money NI A3.1 : Governance Statement
- Assurance Framework in place and in operation;
- Standards Australia Risk Management AS/NZS 4360: 2004.

Guidance

The organisation must be aware of its risk profile across its entire range of activities. Specific risk assessments will have been undertaken but in order to prioritise action an organisation-wide review is necessary to ensure that all exposures are duly considered.

"Key risks", sometimes termed "principal risks", are those which have significant potential to impair or affect the operational or financial ability of the organisation to deliver services and meet objectives, and may be strategic or operational in nature.

A comprehensive assessment of risks should be carried out, creating a continuum of risk assessments across the length and breadth of the organisation, encompassing all risks.

The following sub-criteria will help in deciding whether the key requirements of the main criterion are being met:

- Risks are systematically identified, recorded, assessed and analysed on a continuous basis.

- A comprehensive risk register is maintained on an ongoing basis for all units (eg directorates, departments, functions or sites) for significant projects and for the organisation as a whole. The corporate/organisation-wide risk register is 'owned' and regularly reviewed by the board.
- The risk register should identify risks in a consistent and structured way, show dependencies, and ensure linkage between principal and other key risks.
- There should be a reasonable mechanism for managing relationship risk, ie service partners/key suppliers taking into account the behaviour and risk priorities of those partners.
- Common terminology for risk activities, taking into account DoH guidelines, is applied throughout the organisation.
- For all risks identified as requiring treatment, actions are determined, appropriately recorded and implemented in order of priority using, where relevant, appropriate decision-making tools (e.g. risk ranking or cost-benefit analysis)
- The board is informed of and, where necessary, consulted on all principal/significant risks and associated risk treatment plans on a continuous basis. Any risk exposure should be recorded and exposure justified. Adequate contingency plans should be in place.
- All relevant stakeholders are kept informed and, where appropriate, consulted on the management of risks faced by the organisation.
- All relevant staff are kept informed of the management of significant risks faced by the organisation.
- Key indicators capable of showing improvements in management of risk and/or providing early warning of risk are used at all levels of the organisation, including the board, and the efficacy and usefulness of the indicators are reviewed regularly.
- An annual report is produced for the board to demonstrate the risk management system's continuing suitability and effectiveness in satisfying the organisation's risk management policy and strategy.

Examples of Verification

- Risk management strategy;
- Risk identification tools;
- Hazard reporting policy and forms;
- Risk assessment tools and forms;
- Completed risk assessments;
- Risk treatment options;
- Evidence of risk treatment;
- Business plans;
- Annual report;
- Risk registers;
- Minutes of committees;
- Job descriptions;
- Training programmes;

- Action plans;
- Evidence of communication with stakeholders;
- Evidence of communication with staff;
- Assurance Framework in place and in operation;
- Monitoring and review procedure;
- Performance indicators;
- Evidence of monitoring and review;
- Board minutes;
- Patient surveys;
- Incident, complaints and claims analysis.

Criterion 7

Business continuity management plans aligned to the International Standard on Business Continuity Management Systems (ISO 22301) , are in place and can be activated in order to protect and maintain essential services to a pre-defined level through a business disruption.

Source

• International Standard on Business Continuity Management Systems (ISO 22301)

• DHSSPS Policy Circular: Hospital Lockdown Guidance for Health and Social Care Trusts (March 2011)

Guidance

Good corporate governance practice requires all HSC organisations to have arrangements in place to enable them to continue to deliver their essential or priority services during periods of business disruption. This disruption may be internal to the organisation, for example the loss of a key building because of fire, flooding, the loss of IT services or because of a staffing crisis. Or it may be external, for example the loss of power supplies, prolonged disruptions due to strikes, or lack of fuel supplies.

The **International Standard on Business Continuity Management Systems (ISO 22301)** , defines BCM as 'a holistic management process that identifies potential threats to an organisation and the impacts to operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.'

BCM is, therefore, a process that helps manage risks to the smooth running of an organisation or delivery of a service, ensuring continuity of critical functions to a pre-defined level in the event of a disruption, and effective recovery afterwards. It forms a vital part of good corporate governance and risk management processes, as well as being part of good emergency planning and preparedness.

The business continuity management process is linked to risk management and should form part of organisations' corporate business planning cycles. It should include annual review and update to keep BCM plans current. Business continuity management measures must therefore be part of every organisation's core business, not just an adjunct to it, and should be seen as part of normal good management practice.

HSC	Controls Assurance Standard	Risk Management

Some elements of BCM will also overlap with emergency preparedness arrangements which aim to prevent emergencies occurring (where possible), and when they do occur, to reduce, control or mitigate the effects of the emergency in the management of its impact. But the focus of emergency planning is on dealing with the emergency and the consequences of that emergency, not with maintaining the core business of the organisation.

Business continuity management enables an organisation to anticipate, prepare for, prevent, respond to and recover from disruptions, to a pre-defined level, whatever their source and whatever aspect of the business they affect.

In developing and reviewing their business continuity management plans HSC organisations should ensure that they can demonstrate a systematic, planned and reviewed approach to BCM. The BCMS should detail how organisations will meet the general requirements articulated in ISO 22301 in relation to the following:

- **Context of the organisation** – understanding the organisation and its context, understanding the needs and expectation of interested parties and the scope of the BCM system. This will include determining internal and external issues that are relevant to the organisation's purpose and that affects its ability to achieve the expected outcomes of its BCMS, including understanding the needs and expectations of interested parties, supply chains, etc.

- **Leadership** – describing how top management and other relevant management roles demonstrate leadership with respect to business continuity management systems and management's ongoing commitment to the process, including providing the necessary resources for the BCMS and communicating the importance of effective business continuity management. Such leadership should be established as a core competence within the business continuity policy (which identifies all organisation roles, and ensuring that the responsibilities and that the authority for the relevant roles are assigned).

- **Planning** – establishing the strategic objectives and guiding principles for the BCMS, including identifying all actions in place to address risks and opportunities, in conjunction with business continuity management objectives and plans to achieve these objectives.

- **Support** – identifying the key elements that need to be in place to support BCMS, e.g. all resources, competent staff, training and awareness-raising, how resources have been determined and provided for the establishment, implementation, maintenance and continual improvement of the business continuity management system.

- **Operation** – operational planning and control to achieve business continuity, including Business Impact Analysis, risk assessment, identifying a business continuity management strategy, establishing

and implementing business continuity procedures and evidence of regular exercising and testing to validate plans.

• **Performance evaluation** – once the BCMS is implemented it will require permanent monitoring and regular review to improve its operation. This requires regular monitoring, measurement, analysis and evaluation; the conduct of internal audits; and the gathering of information to support management reviews at planned intervals.

• **Improvement** – striving for continual improvement, including taking any corrective action needed to address non-conformity which was identified through performance evaluation.

Examples of Verification

• Corporate Business Continuity Management Plans (aligned to ISO 22301)

• Notes of performance monitoring meetings

• Internal and external audit reports on the BCM plan

• Hospital lockdown plan/policy where appropriate

Links with other Standards

• Governance
• Financial Management
• Human Resources
• Emergency Planning

CRITERION 8

All employees, including members of the board, professionals, managers, bank, locum and agency staff, together with, where relevant, contractors and volunteers are provided with appropriate risk management and business continuity training.

Source

- Standards Australia Risk Management AS/NZS 4360: 2004
- Circular HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance
- Managing Public Money NI A3.1 : Governance Statement
- Report on Induction Process for Medical Staff in HSC

Guidance

This contributes to the organisation's risk management culture, which needs to be embedded at all levels throughout the organisation.

An appropriate training programme is an important means of achieving competence and helps to ensure compliance with safe working practices. All job descriptions for employees within the organisation should contain reference to their risk management responsibilities.

The following sub-criteria will help in deciding whether the key requirements of the main criterion are being met:

- The organisation has assessed and delivered the level of risk management training that is needed throughout.
- Training records are kept, monitored and reviewed and inadequate attendance rectified.
- Induction for all new starters includes risk management training.
- The organisation can demonstrate that risk management training is effective through monitoring and review.
- Employees with responsibility for co-ordinating and advising on aspects of risk management have adequate training and development to fulfil their role.

Examples of Verification

- Training needs assessment;
- Training prospectus;
- Local training needs assessment;
- Training records (risk management training in the *wider* sense such as training on fire safety, health & safety, first aid/CPR, management of

needle stick injuries, management of aggression, records
management, etc.);
- Reports on attendance levels;
- Induction programme;
- Local induction procedures;
- Training objectives;
- Evidence of review of training objectives;
- Training course evaluations.

CRITERION 9

The board receives independent assurance(s) that a risk management system is in place that meets the requirements of this standard.

Source

- Standards Australia Risk Management AS/NZS 4360: 2004;
- Assurance Framework in place and in operation;
- Circular HSS (PPM) 5/2003 – Governance in the HPSS: Risk Management and Controls Assurance
- Managing Public Money NI A3.1 : Governance Statement

Guidance

Reviews by independent bodies will assist organisations in demonstrating performance, and also in highlighting areas that need to be addressed. This will give the organisation assurance that controls are working satisfactorily and that local and national targets are being met. RQIA has access to controls assurance information and the Authority's reports on assessment of access to, and quality of services commissioned and provided by HSC and other organisations should be given due consideration and actioned as appropriate.

The following sub-criteria will help in deciding whether the key requirements of the main criterion are being met:

- The role of the Audit Committee in reviewing and providing assurance on the risk management systems in place is clearly defined.
- The role of the internal audit function in reviewing and providing verification on the systems in place for risk management is clearly defined.
- The internal audit function, aided as necessary by relevant technical specialists, carries out periodic reviews to provide assurances to the organisation that a suitable risk management system is in place and working properly taking into consideration reviews by other review bodies**.**
- The organisation has a system in place to ensure that reviews carried out by external agencies are effectively co-ordinated and any recommendations implemented within the context of available resources.
- Reports are presented to the Audit Committee and copied to the overarching committee(s) responsible for risk and any other relevant committee/group.

Examples of Verification

- Assurance Framework in place and in operation;

- Internal Audit reports;
- Internal audit statement to Chief Executive;
- Audit Committee minutes;
- Minutes of the committee(s) responsible for overseeing risk management;
- Minutes of the committee(s) responsible for overseeing Clinical and Social Care Governance;
- Reports from RQIA and other review bodies;
- Reports from external audit (NIAO);
- Reports from multi-professional audit.