Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Developing and Populating a Risk Register
Best Practice Guidance

Revision 11, April 2009

Document Reference Number	*OQR010*	**Document Drafted By**	*Cornelia Stuart* *Risk Lead* *Office of Quality and Risk*
Revision Number	*11*	**Document Approved By**	*Ms. E. Dunne,* *Head of Quality and Risk*
Revision Date	*20090422*		
Review Date	*201004*	**Responsibility**	*Office of Quality and Risk*

Table of Contents

1.0 Introduction

It is the policy of the HSE to operate an integrated process for the management of risk and the development of a risk register is a logical starting point in this regard. Using the process outlined in this guidance the service[1] will take stock of the context of its operating environment, identify key risks, assess the risks and review the service capacity to deal with the risks.

The outcome of this process is the development of a risk register which helps a service to establish a direction for managing its risks. The risk register consequently provides managers with a high level overview of the services' risk status at a particular point in time and becomes a dynamic tool for the monitoring of actions to be taken to mitigate risk. This guidance is in line with the AS/NZS 4360:2004 Standard and is consistent with best practice.

The risk register is a key example of evidence required in Criterion 9 of the Quality & Risk Management Standard.

1.1 Scope

This document has been developed primarily to provide operational Service Areas with guidance in relation to the development of their first risk registers and applies to all operational service areas within in the HSE and those services funded by the HSE.

The principles upon which it is based are equally applicable to other areas of the HSE.

1.2 Responsibilities

Risk management is a line management responsibility and consequently the line manager is responsible, in consultation with his/her staff, for the development of a risk register in their area of responsibility. The risk register when complete should be brought to the attention of all employees working in the service in a clear and understandable manner taking into account their level of training, knowledge and experience. A critical part of the risk register is an action plan to address the additional controls identified as required to reduce the risk to an acceptable level. Additional controls (actions) identified as being required that cannot be managed at the service level at which they have been identified should be referred to the next level of management in order that decisions can be taken to manage them. Such decisions may involve the allocation of required resources, the provision of required authority or to escalate the action to a higher level of management. At any stage in the process it may be decided to 'live with' or accept a certain level of risk as it is acknowledged by the HSE that not every risk can be eliminated, for practical or other reasons.

A risk that cannot be completely eliminated must, nevertheless, be recorded in the relevant risk register along with a list of controls to be in place to reduce the risk to an acceptable level. These accepted risks will be monitored by the relevant service on a regular basis.

Risk Registers will capture risk information from the "bottom up" within each Service Area. The risk register will be a primary tool for risk tracking, and will contain the overall system of risks, and the status of any risk mitigation actions. (See Figure 1)

[1] Service refers to a Care/Clinical Service, Hospital, Clinical Directorate, Department.

Fig 1.
Example of how risk registers contribute to the process

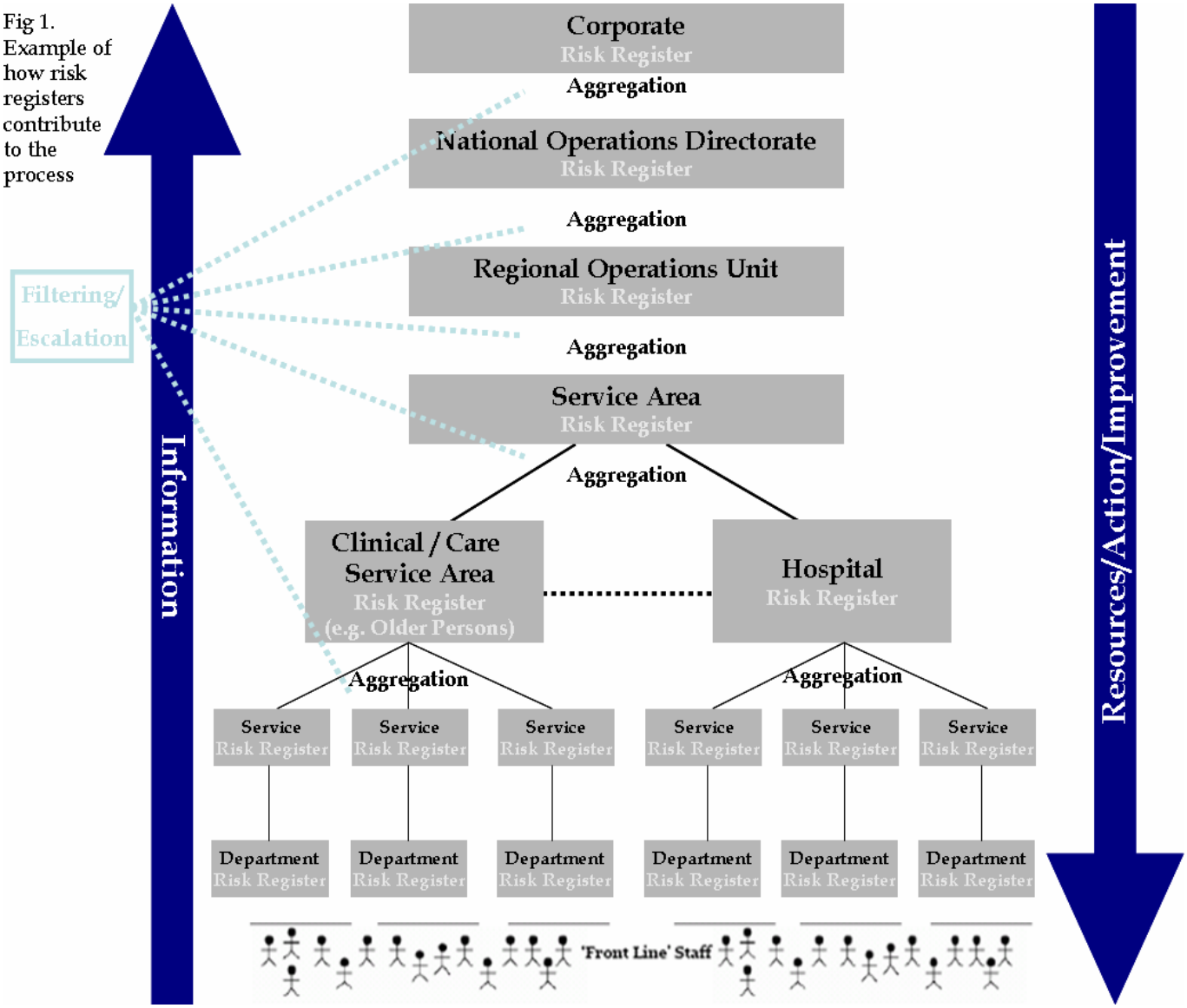


Figure 1 takes account of the proposed reconfiguration of services for integration e.g. Service Area refers to the integrated services (hospital and PCCC) for a geographical area.

1.3 Role of Local Risk Management Department

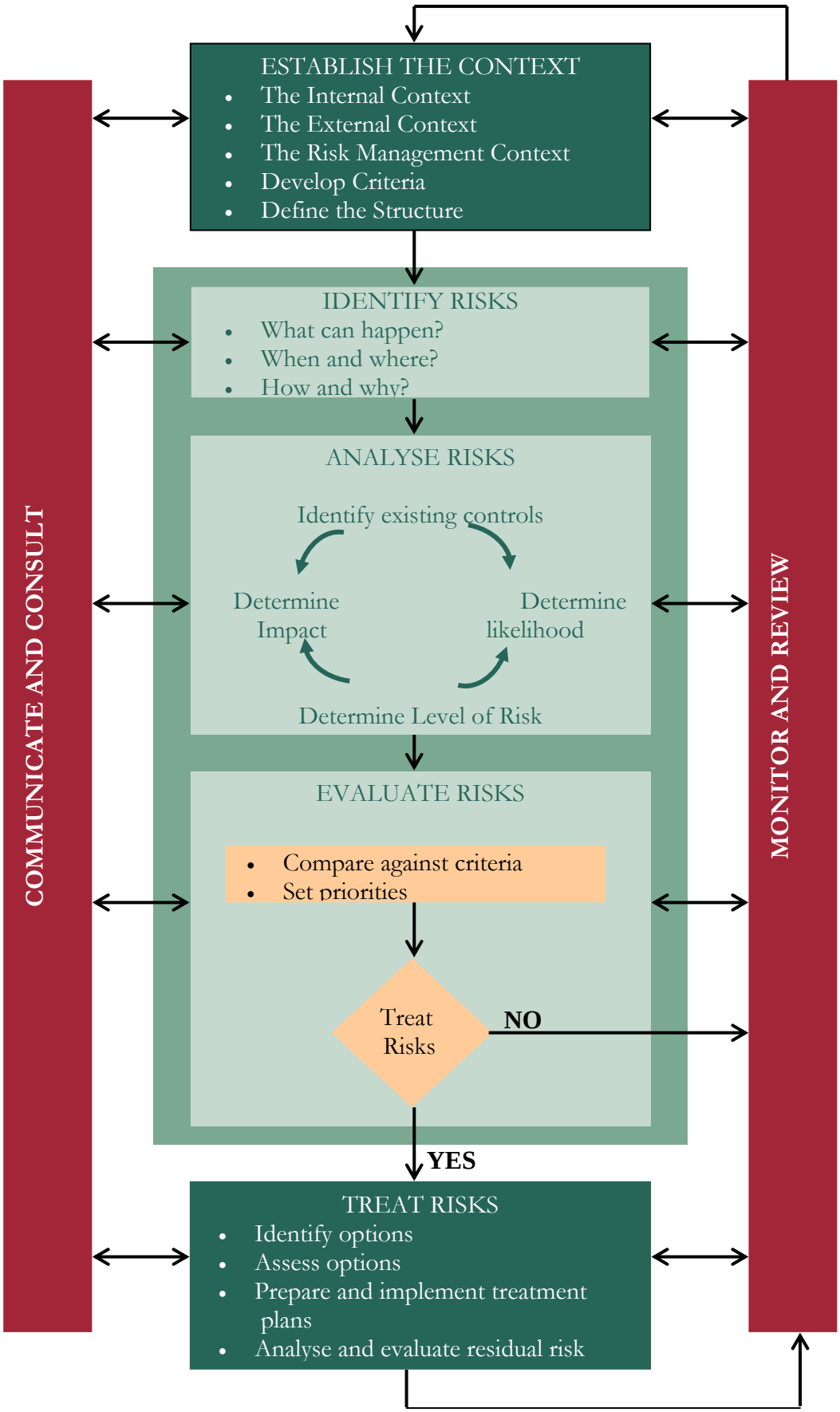
The principal purpose of the Local Risk Management Department, where available, is to facilitate, support and advise line management and employees in relation to the management of risk. It is not their responsibility to manage risks identified within a service. The management of risks is a line management function and responsibility.

1.4 Role of the National Quality and Risk Team.

The role of the National Quality and Risk Team with regard to this process is to offer support, advice and facilitation as is required. This is of particular importance in the instance where there are no locally based risk advisors available. The National Quality and Risk Team also has a role in the provision of independent assurance in respect of the risk register process.

2.0 Overview of the Process for the Development of a Risk Register

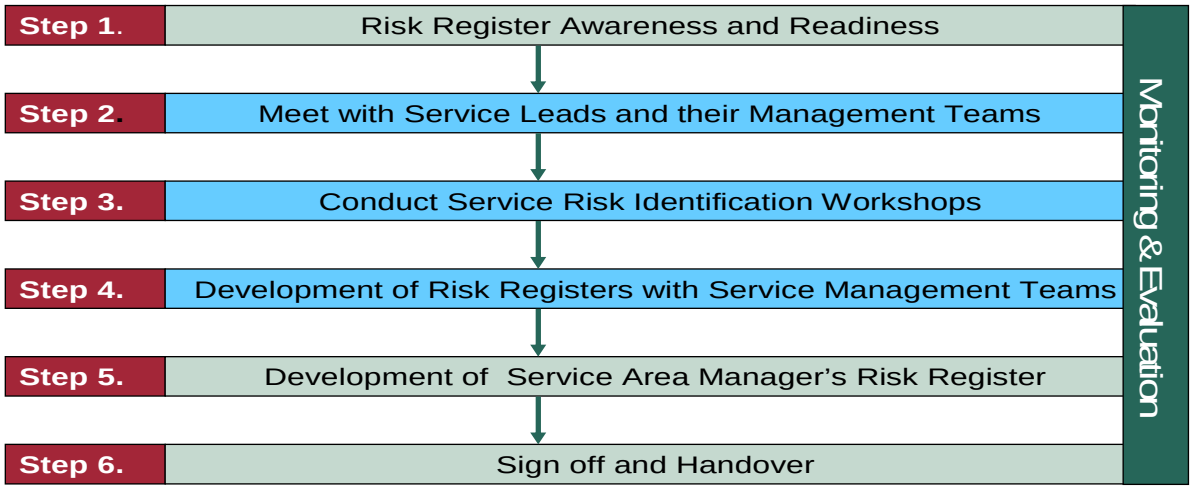
Figure 2: Risk Register Development Process



3.0 Developing a Service Area Risk Register e.g. hospital, LHO

The development of a Service Area Risk Register is a six step process as outlined in Figure 3 below.

Figure 3. Steps in the Development of a Service Area Risk Register



Prerequisites to undertaking the Process

- **Availability of Risk Expertise**

It is accepted that the extent of the risk expertise required to support the process is variable throughout the HSE. The profile of available risk expertise essentially falls into three broad categories.

1) Areas which have internal access to risk staff who would be familiar with and have the experience required to fully support the process from the outset pending orientation to the standardised process and tools to be used.
2) Areas which have risk staff who are not familiar with nor have the experience to fully support the process from the outset and will require training in preparation for supporting development of the register and recourse to expertise in the form of coaching throughout the process.
3) Areas which have no access to risk expertise and will need access to this externally.

Undertaking the process will therefore provide an opportunity to develop risk management capacity as an outcome in that those sites where a register is being developed as staff supporting the process will receive education, training and coaching. The quantum of support provided being proportional to the needs of staff. (see points 1 & 2 above).

The notion of working co-operatively between areas will not only maximise learning but also lead to an accelerated process e.g. in a hospital network or area PCCC all risk staff available in that area could put a focus on one hospital/LHO and work together to the completion of the process in that hospital/LHO. The process would be completed more efficiently and risk staff will gain end to end practical experience of the process. This knowledge would then be transferred back to their own location with the assistance reciprocated when completing the registers in their own area. Obviously such arrangements would need to be discussed and agreed by relevant managers within the system.

- **Use of Approved Support Materials and Tools**

The HSE has approved for use a number of documents and tools to support this process in a uniform and standardised manner. It is essential that all areas who undertake the process of developing risk registers

use these materials and tools in a consistent way. This document and other support materials are reviewed regularly and it is essential that the latest version of these is used when undertaking the process.

- **Commitment and Ownership**

This is critical to the success of the process. There needs to be visible commitment of the senior manager in the area in which the process is being undertaken. This commitment must be communicated and support gained from the service managers who, along with their staff will be participating in the process.

As the management of the completed register(s) will lie with the manager of the area to which they related, it is essential that they take ownership of the development process from the outset. It is the role of the risk staff to support the process and to advise in relation to maintenance of the completed register and not to manage the risks identified.

- **Availability of Site Support**

The process of developing risk registers requires support of an administrative nature e.g. organisation of workshops, co-ordination of the process, point of contact within area etc. A person of sufficient seniority needs to be designated to support the process.

Step 1. Risk Register Awareness and Organisational Readiness

- **Initial planning by Service Area Manager and Risk Management Support Person**

The Service Area Manager should meet with the Risk Management support person. The purpose of this meeting is to ensure that the Service Area manager has an overview of the risk management process and to discuss and agree the development of risk registers in their area of responsibility. At this meeting the clinical/care/support services/departments in which risk registers are to be developed should be defined and a lead person responsible for each of these identified.

- **Describe in detail the accountability structure for the management of quality and risk.**

It is key critical to spend time at the outset in describing the accountability structure for the management of quality and risk within the Service Area. This is required as the actions required to mitigate risks identified at any level may not be within the control of the manager at that level and may require notification and escalation to a more senior level of management for action. The lines of responsibility need to be clearly defined on the principles of line management. The HSE web-based ICT support for the management of risk is predicated on this principle and so a failure to adequately define the accountability structure will have long term implications for the success of the system within the Service Area.

- **Describe the Service Area's internal, external and risk management context for managing risk within the healthcare setting.**

The context in this regard is dependant on those factors which impact on the particular Service Area where a risk register is to be developed. For example, the internal context will be the context of the Service Area and Regional Operations Unit. The external context will include any legislation and agencies that govern or regulate its operation e.g. Health Act, Safety Health and Welfare Act etc, or HIQA, the Mental Health Commission and the relevant professional bodies that pertain to the service area e.g. Royal Colleges, An Bord Altranais etc. The risk management context will refer to the patient profile, the complexity of the clinical specialities in the Service Area, the adequacy of the environment of care.

- **Ensure appropriate communication and consultation throughout the development process.**

Within the healthcare service, good communication is paramount in developing a 'culture' where positive and negative dimensions of risk are valued. Engaging with others can help to embed risk management as a normal part of the way services operate. Communication efforts must be focused on consultation, rather than one way flow of information from decision makers to stakeholders.

Initial communication will commence with the organisation and delivery of the risk register briefing meeting with the management team, service leads and other relevant staff. The purpose of this briefing is

to outline the overall process to be undertaken, their role in the process and the benefits of the process to them.

- **Enlist the help of relevant local and organisational supports.**

It is important that any line manager undertaking this process has access to risk management advice/expertise. In many cases this may be available within the Service Area or if not contact should be made with the Area Quality and Risk Manager.

Apart from persons directly employed in risk management the local delivery system may also include employees that have a role in identifying and reducing risk e.g. Infection Control, Quality, Health & Safety, Haemovigilance employees etc. Support from these employees may be accessed as required by the area in which the risk register is being developed.

There are also resources in the HSE support services areas which can be accessed to assist with the actions arising out of the risk identification process e.g. training and development, team-working etc. Departments such as Organisational Development and Design, Corporate Learning & Development may be accessed for such support (See Appendix 1 for a list of support persons within the HSE).

Step 2. Meet with Service Leads and their Management Teams

The Risk Management support person should meet with each service nominated lead and other key members of their management team prior to their service workshop. The purpose of this meeting is to:

- Provide an overview of the purpose of the risk management process and the process of the workshop;
- Stress the importance of establishing the Service context (external, internal, risk management)

The context in this regard is dependant on those factors which impact on the particular Service where a risk register is to be developed. In an acute hospital speciality/directorate, for example, the internal context will be the context of the hospital and its Service Area and Regional Operations Unit. The external context will include those agencies that regulate its operation e.g. HIQA and the relevant professional bodies that pertain to the service area e.g. Royal Colleges, An Bord Altranais etc. The risk management context will refer to the patient profile, the complexity of the clinical speciality, the adequacy of the environment of care.

In the Mental health setting, the external context will include the relevant legislation e.g. Mental Health Act 2005, and the Mental Health Commission as service regulator. In a support service such as Human Resources (HR), the external context will be the HR legal framework, and the internal context will take account of national HSE HR policy and local needs.

- Re-enforce the need to review of sources of risk information that may currently lie within the service area;

Within each service there exists information in relation to the level and type of risk to which the service is exposed. Since one of the purposes of the risk register is to create a repository for all risk it is essential that information from existing sources is considered as part of the development process.

It is important to ensure that high quality information/data is used in identifying risks. The line manager of the service in which the risk register is being developed should ensure that a process is undertaken to identify risks from any information source available.

Such sources of information include but are not confined to:

- Health & Safety Risk Assessments
- Clinical Risk Assessments

- Activity Information (e.g. throughput, readmissions, waiting lists)
- Alerts received relevant to your service
- Analysis of Consumer Feedback – i.e. complaints, client satisfaction surveys, compliments
- Audit Reports
- Incident/accident Reports and Investigation/review (internal and external)
- Research/Literature Reviews
- Peer Review Meetings
- Morbidity and Mortality Meetings
- Evaluations
- Claims Data
- Media Reports
- Minutes of Team Meetings
- Occupational Health Surveillance
- PQs
- Review of External Inspection Reports e.g. Mental Health Commission reports, Accreditation reports, Health & Safety Authority reports, Registration and Inspection reports/notices, Professional Body Inspectorates, Irish Medicines Board alerts, Ombudsman reports/appeals
- National Reviews of Major Incidents
- Sickness Absence/Employee Turnover
- Visual Inspection
- Speciality Specific Checklists
- General Checklists

This information when collected will assist in the validation and proofing of risks identified at the workshop thereby providing a comprehensive risk listing upon which the register will be developed.

- Identification of the key stakeholders to attend the workshop(s). The attending employees should be representative of all employee types e.g. clinical, administrative and support and grades of employees e.g. senior to junior. It is also important to invite employees from other services who support the delivery of the service e.g. diagnostics. As one of the main purposes of the workshop is to get as wide a perspective as possible in relation to the risks that attend to the service, the more individuals you can manage to involve the better.
- Once the stakeholders have been identified a communications and consultation plan can be developed in relation to the development process.
- Discuss the number of workshops required for the service. The number of workshops required will depend on the size of the service. In many instances only one workshop may be necessary and in the case of smaller departments/services a number of these can attend at one workshop.
- Discuss the organisation of the workshop(s) i.e. dates, invitations, venue, set up of the room, equipment required etc.
- Evaluate the degree to which the objective of the pre-workshop meeting was achieved. All participants at this meeting should fill in an evaluation form.

Step 3. Conduct Service Risk Identification Workshops

The Risk Management support person facilitates the risk identification workshop(s) with a cross section of employees relating to the service in which the risk register is being developed.

At the workshop(s) the Risk Management support person should:

- Give an introduction to Risk Management to cover why risk management is important, what are the benefits of risk management and an overview of the risk management process. Take time to explain this objective of the workshop to those attending i.e. to use their knowledge of the service to identify those issues that might pose risk.
- Conduct the first break out session, during this the attendees work individually to brainstorm all the issues they perceive pose risk to (a) patients/service users, (b) employees and (c) the organisation. Issues identified are recorded on post-it notes and gathered by the Risk Management support person and displayed on the wall under the headings of (a) patients/service users, (b) employees and (c) the organisation. It is a good idea in displaying the post-its on the wall to group and theme issues of a similar nature. If a number of departments are attending at the workshop ensure that they identify their department on each post-it used or alternatively provide each department with different coloured post-its. This is critical as the post-its will be used to develop the risk list (and the subsequent assessment) for creating the departmental risk register.
- Take a sample number of issues identified as a result of this process (it will not be possible to review all the issues identified at the workshop) and through a process of discussion with those attending describe the risks associated with these issues. The risks should be described using the Impact, Causal Factor & Context (ICC) approach. (See Appendix 2 for further details). The risks described will be used for the next break out session where attendees will work in groups.
- After the attendees have described a number of risks (at least one per group), the Risk Management support person should use one of these to demonstrate how to assess a risk using the HSE Risk Assessment Tool (see Appendix 3). As part of this demonstration the Risk Management support person should use the risk assessment exercise sheet (see Appendix 4) to step through the process.
- Conduct the second break out session, during this attendees work in groups to take a number of the risks identified and risk assess each of the risks. The risk assessment exercise sheet (see appendix 4) and the HSE Risk Assessment tool should be used by the groups in this exercise (see appendix 3).
- After the second breakout session the Risk Management support person outlines the next stages in the risk register development process and thanks the attendees for their valuable input and contribution to the workshop. All employees present at the workshop should fill out an evaluation form so as to evaluate the degree to which the objectives of the workshop were achieved.

Step 4. Development of Risk Registers with Service Management Teams

Initial post workshop meeting

This is ideally held directly following the workshop. The service lead should then convene the services management team or a smaller group of senior employees if a formal management team is not in place. This group will consider the issues identified from the workshop and consider any other sources of risk information with a view to identifying the risks to the service. The local Risk Management support person should provide support and advice to this group. The outcome of this meeting will be a draft risk list (using the ICC approach to risk description – see Appendix 2) which should then be circulated to the members of the group for final consideration. It may also be decided to circulate it to other persons who the group may wish to consult.

Subsequent meetings to complete the Risk Register

The purpose of subsequent meetings is to agree the risk list and to complete the risk assessment for each risk identified. Each risk identified should be documented on a Risk Assessment Form (see Appendix 5).

(**Hint:** It is recommended that prior to the first of these meetings that the risks on the draft risk list are copied and pasted (one per form) onto blank HSE Risk Assessment Forms. At the meeting a soft copy of these can be projected on a screen and any amendments/additional information inputted directly onto them at the meeting).

- Consider each of the risks separately, describe and document on the risk assessment form the impacts/vulnerabilities of the risk. (Note: these are the impacts and vulnerabilities that attach to the risk in general and are not an indication of impacts/vulnerabilities existing within the service). The documenting of these here will assist with both the impact assessment process and with identifying the types of impacts/vulnerabilities which need to be controlled i.e. assist in identifying additional controls required.
- For each risk agree what controls are required in order to manage the risk effectively. A combination of different types of control may be required. See Appendix 6 for detailed information regarding control measures. When trying to think of what controls should be in place it is often useful to consider these in a logical manner e.g. starting with policy and procedures, (clinical and non-clinical), the actions undertaken to implement these (training, education, resources, use of physical environment etc), through to monitoring and evaluation to ensure compliance.
- Identify and document which of the required controls are currently in place i.e. existing controls.
- Consider the adequacy of the existing control measures and their effectiveness in minimising risk to the lowest reasonable practicable level. (see Appendix 6)
- Rate the risk by assessing the likelihood and impact of the risk and plotting these scores on the HSE Risk Matrix. In rating the risk, account must be taken of the adequacy the existing controls that are in place. The HSE's Risk Assessment Tool must be used for the process of rating the risk. A copy of this tool may be accessed through the following link. OQR012 Risk Assessment Tool and Guidance (Including guidance on application)
- Depending on the initial risk rating and the adequacy of the existing controls in place an evaluation must be made on whether to accept the risk or that additional controls or other actions are required to mitigate the risk i.e. risk treatment
- For those risks deemed acceptable a process needs to be put in place to monitor and review the risk. The review date and the risk status of 'monitoring' need to be documented on the risk assessment form.
- For those risks that are not deemed acceptable, the team need to consider the options available to them to treat the risk e.g. those controls that were identified at the outset as necessary to manage the risk and that do not currently exist. It is important when documenting the actions required to ensure that they are explicit to others when read as some actions may need to be escalated to a manager outside the service where there may not be the same level of implicit understanding.
- To ensure that the additional controls identified in this step of the process will adequately mitigate the risk, the group should re-rate the risk taking account of a situation where the additional controls would be in place. This should be done using the HSE Risk Assessment tool (see appendix 3) and documented on the risk assessment form.
- After the additional controls required have been agreed the team should identify and assign a person who has responsibility for ensuring that these additional controls are

implemented. For those additional controls that can be managed within the service the name of the person within the service who has been assigned responsibility to action the additional control should be captured on the risk assessment form. The Service Lead(s) need to arrange a meeting with the person's assigned responsibility to manage the additional control(s). The purpose of this meeting is to agree the action plan(s) required and to agree the due date for implementation. The agreed due date will have to be documented on the relevant risk assessment form. **Note:** For this meeting it is important to have an up to date soft copy of the relevant service risk assessment forms so that any changes made at the meeting can be done on the day. It is important that one person is assigned responsibility to co-ordinate the management of the additional control (action). (See Risk Management Escalation Pathway, Appendix 7). In the absence of an ICT system it is important that those persons who have been assigned responsibility for the additional controls are given a copy of the completed risk assessment form. This is important as the responsible persons will have to provide an update on the status of these additional controls on a 3 monthly basis.

- For those additional controls that are identified as not within the span of control of the service to implement the action should be escalated to the person responsible at the next level of management e.g. a speciality directorate to the general manager/CEO of a hospital (see Step 5 for a description of the escalation process). The name of the relevant senior manager to whom the action is being assigned should be captured on the risk assessment form. In the absence of an ICT system it is important that those persons who have been assigned responsibility for the additional controls are given a copy of the completed risk assessment form. This is important as the responsible persons will have to provide an update on the status of these additional controls on a 3 monthly basis.
- Each of the risks should be assigned a risk status. With regard to the risk status the options available are:
    - Open, i.e. additional controls have been identified as necessary
    - Monitor, i.e. existing controls are deemed adequate to manage the risk but these need to be periodically reviewed.
    - Closed, i.e. that the risk no longer exists e.g. where an unsuitable premises is replaced by a suitable one.
- Categorise the type of risk by assigning a primary, secondary and tertiary risk category from the Risk Categorisation (see Appendix 8). In categorising risk the primary category should link to the primary area of impact. The secondary and tertiary categorisation will flow naturally from this choice and taking account of the overall risk description. This categorisation should be documented on the risk assessment form.
- At this point ensure that all remaining information required on the form has been filled in (see appendix 5 for a description of the information required for each field)

Hint: The time taken to complete the assessment of the first risk with the team will be considerable. As the group gets more familiar with the process the time taken will shorten. This can be accelerated further when members of the group are confident with the process by agreeing to divide the remaining risks to be assessed between the members of the group (email the forms to members) and for each of the members to work between meetings to complete a draft assessment of the risks emailed to them. The drafted risk assessments should be emailed back to one nominated person before the next meeting. The nominated person saves all draft risk assessments and brings these on a laptop for discussion and agreement with the group. The focus of the next meeting is therefore around reaching consensus on each drafted risk assessment form rather than working from scratch with each risk.

- At the end of this step in the process the service will have a complete risk assessment form for each risk identified for their service. These forms collectively represent the services risk register and are in a format which can be inputted directly onto the HSE ICT Risk Register when available. In the absence of the HSE ICT Risk Register the persons responsible for the additional controls will also have received a copy of the completed risk assessment forms to enable them to provide a 3 monthly update to the Service Manager.
- If an improvement plan is not required the agreed timeframe for action should be documented and attached to the risk assessment form. If an improvement plan is required this should be developed in accordance with the FOCUS – PDCA improvement model. An outline of the FOCUS - PDSA cycle can be obtained in Appendix 9.

At this stage in the process each of the services within the Service Area will have a completed risk assessment form for each risk identified in their services.

The assessed risks can be categorised as follows:

1. Those risks that require monitoring and review within the service they were identified i.e. risks where no further additional control(s) have been identified as necessary.
2. Those risks where the additional controls(s) can be managed at local level and the responsibility for managing those additional control(s) has been assigned to person(s) within the service.
3. Those risks where there is a combination of escalated and locally managed additional control(s). **Note:** It is important for those risks that have a combination of local and escalated additional controls that any changes to the risk assessment form need to be notified to the co-ordinator of this step in the process so as to ensure that the Service Area Manager has the most up-to-date risk assessment form on their risk register
4. Those risks where the additional control(s) cannot be managed at local level and these have been identified as requiring escalation up to the Service Area Manager.

It is those risks that fall into categories 3 & 4 above that form the basis of the development of the Risk Register for the Service Area Manager.

Step 5. Development of the Service Area Manager's Risk Register

The Service Area Manager convenes a separate meeting with each of the service leads and the person assigned responsibility to co-ordinate this step of the process.

The purpose of this meeting is to evaluate and agree with the service lead the additional controls identified as being the responsibility of the Service Area Manager.

At this meeting the Service Area Manager can:

- Agree to accept responsibility for the additional control(s) or consider assigning the additional control(s) required to a relevant senior manager on their management team or;
- Where the additional control(s) required is outside of the control of the Service Area Manager, they can escalate the additional control(s) up to the Regional Operations Manager or;
- Modify or add additional control(s) and accept responsibility for this, assign it to a relevant manager on their management team or escalate to the Regional Operations Manager or;
- Where the Service Area Manager is notified of a risk from one service that they feel has an impact on all services or where the Service Area Manager has been notified of the same/similar risk from all or a number of services or where a risk identified in one or more services impacts on other groupings the following applies:

Aggregation of same/similar Risks

The Service Area Manager creates a new risk onto the Service Area risk register and then identifies the additional control(s) and person(s) responsible required to manage the risk. The Service Area Manager may decide to assign responsibility of the additional control to a member of his/her management team or they may decide to escalate relevant additional control(s) up to the Regional Operations Manager for action.

Following this the Service Area Manager needs to notify the service manager(s) where the original risk was identified and advise them that he/she has created a new risk on his/her risk register and that there is still a need for the service manager(s) to manage and monitor the original risk at a service level and to inform the Service Area Manager of any change in circumstances.

Finally the Service Area Manager needs to notify the Service Leads (who have **not** identified this as a risk in their service) that he/she has created a new risk on their risk register and that there is a need for the service lead(s) to create a risk on their risk register and to manage and monitor this risk at a service level and to inform the Service Area Manager of any change in circumstances.

NOTE: For this meeting it is important to have an up to date soft copy of the relevant service Risk assessment forms so that any changes made at the meeting can be done on the day.

Following on from this meeting the Service Area Manager should meet with his/her management team members who have been assigned responsibility to manage the actioning of the additional control(s) to discuss and agree the risk treatment plans. Risk Treatment plans should include:

- Risk reduction/additional controls required
- Resource requirements
- Timescale for implementation, review date, completion date.
- Performance measures
- Reporting and monitoring requirements.

The risk treatment plan should be documented and attached to the risk assessment form. It might be useful to consider the Plan, Do, Check, Act (PDCA) Cycle for this purpose. An outline of this process can be obtained in Appendix 9

The escalation of additional controls to the Regional Operations Managers Risk Register.

The process as identified above needs to be repeated with the Regional Operations Manager and the Service Areas Manager's in his/her area of responsibility.

The escalations of additional controls to the relevant National Director's risk register

The process as identified above needs to be repeated with the relevant National Director and the Regional Operations Managers in his/her area of responsibility.

Step 6. Sign off and Handover

The purpose of this stage is to conduct a final meeting with the Heads of Service/Departments of those areas in which the workshops took place and the Service Area Manager in order to

- To sign off the registers
- To present feedback from the evaluations carried out to date
- To advice on the business process for using the registers as a dynamic management tool to manage risk
- To receive any other feedback that will inform future processes in other areas.

Updating Risk Registers

Until the HSE's ICT Risk Register System is implemented in your area it is vital to have an agreed manual process in place for updating the registers at all levels in the Service Area.

In the absence of an ICT risk register system a possible interim process for updating risk registers is as follows:

- At stage 4 in the process the Grouping/Directorate/Service Lead will have already given a copy of the completed risk assessment forms to those persons assigned responsibility for the additional controls. On a regular basis e.g. 3 monthly, the relevant Grouping/Speciality/Service Lead will send an email together with a blank update form to those responsible persons and request an update by an agreed date. (See **Appendix 5a** for a copy of a blank update form)

- The relevant responsible person(s) will complete the update form(s) and email back to the Grouping/Speciality/Service Lead.

- The Grouping/Speciality/Service Lead will gather all the update forms, check for completeness and attach the relevant update forms to the appropriate risk assessment form(s).

- The above process should be repeated regularly e.g. every 3 months until the ICT risk register is in place.

Monitor and Review

The risk assessment process should be seen as a dynamic process with the adequacy of the control measures subject to continual review and monitoring and revised where necessary. In general terms, monitoring will be one of three types:

1. **At service level**
    a. Monitoring of risks
        i. Identification of new risks

Within any service new risks are likely to emerge from time to time, these are likely whilst operating in an environment of limited resources, changing work environment e.g. regulatory, management, technological etc. The service must be aware of such issues which may impact on it and on a continuous basis be reflecting on sources of risk information (See Section 2.2. Phase 1)

Any new risk identified should be included on the risk register following assessment and the identification of actions required in the same way as those that were identified through the initial risk register development process.

ii. Re-assessment of existing risks

It is good practice to review the risk assessment annually taking account of any new controls that have been put in place since the original assessment. This will allow for a re-prioritisation of the risk list thereby focusing the efforts of the service to address those risks that are most pertinent to the service.

When re-assessing existing risks, services should compare the risk rating from the re-assessment with the risk rating of the original assessment. If the reduction (or maintenance in certain circumstances) of risk levels is not as anticipated in the original assessment, then they need to check why i.e. have the additional controls been effectively implemented? If they have why are they not reducing the rating? Are they the right controls and if not is there a need to revisit and enhance the control measures?

2. At Service Area Level

In the same way as risks are monitored within services, risks should be monitored at a Service Area Level as outlined above:

a. Monitoring of actions arsing from risks identified at Service Area Level

b. Monitoring risks

i. Identification of new risks

ii. Re-assessment of existing risks

3. Monitoring for independent assurance

From a governance perspective it is essential that not only to demonstrate that services have conducted a proactive risk identification process but also to be able to demonstrate that the process was robust and that it has resulted in a positive effort to reduce risk.

a. Integrity and effectiveness of the process

The integrity of the process is governed by the use systematic application of this guidance and the associated tools (including involvement of relevant stakeholders). The ongoing management of the risks identified by this process can be audited using the audit facility inherent in the ICT Risk Register thereby making it a key tool for the monitoring of improvement actions identified as required for a service.

Independent assurance in relation to this should be sought external to the service e.g. internal/healthcare audit. The National Office of Quality and Risk is one source of independent assurance.

b. Linkages with other sources of risk information

As the risk register is a repository for risk identified from a wide variety of sources (see Section 2.2. Phase 1) it is essential that evidence is available that the services efforts to identify risk go beyond the workshop. This will ensure that risks not identified at the workshop can be included in the risk register or that risks identified at the workshop can be validated further.

4. Monitoring performance against Criterion 9 of the HSE Quality and Risk Management Standard

Criterion 9 of the HSE's Quality and Risk Management Standard states:

"Risks of all kinds are systematically identified, assessed and managed in order of priority in accordance with Australian/New Zealand Standard AS/NZS 4360:2004 'Risk management.' "

The degree to which conformance with all aspects of this guidance can be demonstrated will be key in the provision of evidence for performance.

4.0 Bibliography:

Publications consulted in the compilation of the Developing and Populating a Risk Register Best Practice Guidance

1. CASU and Risk Register Working Group *Making it Happen – A Guide for Risk Managers on How to Populate a Risk Register* Controls Assurance Support Unit (CASU) Keele University October 2002
2. CSA (1997) Risk Management: Guideline for Decision Makers –A Standard of Canada. Canadian Standards Association (1997 reaffirmed 2002) CAN/CSA-Q850-97
3. Deming, W.E. *Out of the Crisis.* Cambridge, Mass: Massachusetts Institute of Technology Centre for Advanced Engineering Study, 1992.
4. Deming WE. *The New Economics for Industry, Government, Education.* Cambridge, Massachusetts, USA: The MIT Press; 2000
5. Department of Health (UK) *Risk Management Standard* Controls Assurance Support Unit 2001
6. Dineen M, Six Steps to Root Cause Analysis 18 September Consequence (Oxford, 2002) ISBN 0-9544328-0-0
7. Health and Safety Authority Guidelines on Risk Assessment and Safety Statements, January, 2006.
8. Health and Safety Authority Auditing a Safety and Health Management System - A Safety and Health Audit Tool for the Healthcare Sector HSA 0138:2006
9. Healthcare Risk Department *Guideline for Undertaking a Risk Assessment* HSE West (Mid West) 2006
10. Healthcare Risk Management Department Guideline 001-Hazard identification, Guideline 002-Risk Assessment, Guideline 003 - Risk Control Development and Implementation HSE Dublin Mid Leinster (Midlands)
11. HealthCare Standards Unit and The Risk Management Working Group *Making it Work – Guidance for Risk Managers on Designing and Using a Risk Matrix* HealthCare Standards Unit, Keele University 2004
12. Hong Kong Hospitals Authority Risk Register Guidelines – Managing risk using the specimen Hospital Authority risk register Version 1.1 2004
13. Hong Kong Hospitals Authority Risk Register Tool (to accompany Risk Register Guidelines – Managing risk using the specimen Hospital Authority risk register Version 1.1 2004)
14. HSE Risk Management in the HSE an Information Handbook http://hsenet.hse.ie/HSE_Central/Office_of_the_CEO/Quality_and_Risk/Documents/OQR011_Risk_Management_in_the_HSE,_An_Information_Handbook.pdf
15. HSE Incident Management Policy and Procedure http://hsenet.hse.ie/HSE_Central/Office_of_the_CEO/Quality_and_Risk/Documents/OQR006_Incident_Management_Policy_Procedure.pdf
16. HSE Serious Incident Management Policy and Procedure http://hsenet.hse.ie/HSE_Central/Office_of_the_CEO/Quality_and_Risk/Documents/SIMT_01_Part_2_Serious_Incident_Management_Policy_and_Procedure.pdf
17. HSE Toolkit of documentation to support incident management

    http://hsenet.hse.ie/HSE_Central/Office_of_the_CEO/Quality_and_Risk/Documents/OQR008_HSE_Toolkit_of_documentation_to_support_incident_management1.pdf

18. HSE Risk Assessment Tool and Guidance
http://hsenet.hse.ie/HSE_Central/Office_of_the_CEO/Quality_and_Risk/Documents/OQR012_Risk_Assessment_Tool_and_Guidance_including_guidance_on_application_.pdf

19. HSE Quality and Risk Management Standard
http://hsenet.hse.ie/HSE_Central/Office_of_the_CEO/Quality_and_Risk/Documents/OQR009_Quality_Risk_Management_Standard.pdf

20. HSE Quality and Risk Taxonomy Governance Group Report
http://hsenet.hse.ie/HSE_Central/Office_of_the_CEO/Quality_and_Risk/Documents/OQR026_Quality_and_Risk_Taxonomy_Governance_Group_Report.pdf

21. Institute for Healthcare Improvement Methods – How to Improve
http://www.ihi.org/IHI/Topics/Improvement/ImprovementMethods/HowToImprove/

22. Langley GL, Nolan KM, Nolan TW, Norman CL, Provost LP. *The Improvement Guide: A Practical Approach to Enhancing Organisational Performance.* San Francisco, California, USA: Jossey-Bass Publishers; 1996

23. Leveson, N. 1995. Safeware; System Safety and Computers. Addison-Wesley, Massachusetts

24. NHS Quality Improvement Scotland *Core Risk Assessment Matrices* October 2005

25. National Patient Safety Agency *Guidance Contributory Factors Classification System* Version 1.0
www.msnpsa.nhs.uk/rcatoolkit/resources/word_docs/Guidance/Guidance_Contributory_Factors_Classification_System.doc

26. North Eastern Health Board, Guidance on Occupational Health & Safety Risk Assessment, March, 2005.

27. Risk Management Department *Seven Steps to Risk Assessment* HSE Dublin North East (North East) 2005

28. Standards Australia/Standards New Zealand, Australian/New Zealand Standard: Risk Management (AU/NZS 4360) 2004

29. Standards Australia/Standards New Zealand, Australian/New Zealand Standard: Risk Management Guidelines Companion to AU/NZS 4360:2004

30. Standards Australia/Standards New Zealand, *Australian/New Zealand Standard:* Guidelines for Managing Risk in the Healthcare Sector HB 228:2001

31. Treasury Board of Canada Secretariat Integrated Risk Management – Implementation Guide 2004

32. Vincent C.A, Taylor-Adams S.E, Hewett D, Chapman J et al, *A Protocol for the Investigation and Analysis of Clinical Incidents* (London: Royal Society of Medicine Press Ltd, 1999)

LIST OF APPENDICIES

Appendix 1: List of relevant HSE Support Staff

When enlisting the support of relevant staff in your area consider the following:

- Risk Management Personnel
- Occupational Health Personnel
- Fire Prevention and Safety Personnel
- Safe Moving and handling Personnel
- Pharmacy / Medications Safety Personnel
- Laboratory Safety Personnel
- Complaints Management & Consumer Affairs Personnel
- Clinical Engineers (Medical Equipment Safety)
- Technical Services Personnel (Construction Safety)
- Health & Safety Personnel
- Waste Management Personnel
- Infection Control Personnel
- Transfusion Safety Personnel
- Dangerous goods Safety Advisory Personnel
- Security Personnel
- Fleet Management Personnel
- Clinical and Non Clinical Audit Personnel
- Internal Audit and Finance Personnel
- Emergency Planning Personnel
- Accreditation Personnel
- Hygiene / Cleaning Services Personnel
- Radiation Protection Personnel
- Records Management Personnel
- Decontamination Personnel
- Continuous Quality Improvement Management Personnel
- Change Management and Organisational Development Personnel
- Corporate Learning and Development Personnel
- Communications Personnel
- Ergonomics and Human Factors Personnel
- Environmental Safety Personnel
- Maintenance and housekeeping Personnel
- Frontline employees

Appendix 2: Describing the Risks Identified using the Impact, Causal Factors and Context (ICC) approach

It is important that a brief description of each risk is provided that accurately and comprehensively ensures that the exact nature and magnitude of the risk is captured. This applies whether the risks have been identified from a relevant information source or from a grouping/hospital directorate risk assessment workshop.

The 'ICC approach' to risk description

- Risk is inherently negative, implying the possibility of adverse impacts. Describe the potential primary area of **Impact** if the risk were to materialise.
- Describe the **Causal Factors** that could result in the risk materialising.
- Ensure that the **Context** of the risk is clear, e.g. is the risk 'target' well defined (e.g. employees, patient, department, hospital, etc.) and is the 'nature' of the risk clear (e.g. financial, safety, physical loss, perception, etc.)

Example: Premature discharge of patients from the hospital *(context)* leading to death or poor outcome *(primary are of impact)* due to bed shortage *(causal factor).*

Other examples of Risk descriptions include:

1) Direct service user-related risk descriptions

- Delay or missed diagnosis/treatment resulting in increased mortality and morbidity within the Emergency Department
- Long waiting lists within Orthodontics resulting in increased morbidity and complaints
- Failure to adequately protect children identified as 'at risk' from harm due to long waiting lists for assessment.
- Medication error resulting in death or serious harm to patient within the ICU
- Risk of NCHD's making unsound clinical judgement after long hours of duty
- Malfunctioning of resuscitation equipment in the hospital due to lack of maintenance
- Risk of injury to patients arsing from falls off trolley in the recovery room
- Wrong patient label on ECG leading to wrong treatment within the Medical OPD
- Administration of incompatible blood to patients due to unlabeled or incorrectly labelled blood samples or wrong blood unit issued by blood bank

2) Other risk descriptions may include.

- Risk of occupational blood exposure to staff due to needle stick injuries within the Emergency Department
- Financial loss due to payments to fictitious vendors
- Harm to employees due to violent patients/clients within mental health services
- Computer virus on service/area/department network causing lengthy system shutdown

Appendix 3: Risk Assessment Tool HSE RISK ASSESSMENT TOOL

2. IMPACT TABLE

	Negligible	Minor	Moderate	Major	Extreme
Injury	Adverse event leading to minor injury not requiring first aid. No impaired Psychosocial functioning	Minor injury or illness, first aid treatment required <3 days absence < 3 days extended hospital stay Impaired psychosocial functioning greater than 3 days less than one month	Significant injury requiring medical treatment e.g. Fracture and/or counselling. Agency reportable, e.g. HSA, Gardaí (violent and aggressive acts). >3 Days absence 3-8 Days extended hospital Stay Impaired psychosocial functioning greater than one month less than six months	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling Impaired psychosocial functioning greater than six months	Incident leading to death or major permanent incapacity. Event which impacts on large number of patients or member of the public Permanent psychosocial functioning incapacity.
Service User Experience	Reduced quality of service user experience related to inadequate provision of information	Unsatisfactory service user experience related to less than optimal treatment and/or inadequate information, not being to talked to & treated as an equal; or not being treated with honesty, dignity & respect - readily resolvable	Unsatisfactory service user experience related to less than optimal treatment resulting in short term effects (less than 1 week)	Unsatisfactory service user experience related to poor treatment resulting in long term effects	Totally unsatisfactory service user outcome resulting in long term effects, or extremely poor experience of care provision
Compliance with Standards (Statutory, Clinical, Professional & Management)	Minor non compliance with internal standards. Small number of minor issues requiring improvement	Single failure to meet internal standards or follow protocol. Minor recommendations which can be easily addressed by local management	Repeated failure to meet internal standards or follow protocols. Important recommendations that can be addressed with an appropriate management action plan.	Repeated failure to meet external standards. Failure to meet national norms and standards / Regulations (e.g. Mental Health, Child Care Act etc). Critical report or substantial number of significant findings and/or lack of adherence to regulations.	Gross failure to meet external standards Repeated failure to meet national norms and standards / regulations. Severely critical report with possible major reputational or financial implications.
Objectives/Projects	Barely noticeable reduction in scope, quality or schedule.	Minor reduction in scope, quality or schedule.	Reduction in scope or quality of project; project objectives or schedule.	Significant project over – run.	Inability to meet project objectives. Reputation of the organisation seriously damaged.
Business Continuity	Interruption in a service which does not impact on the delivery of service user care or the ability to continue to provide service.	Short term disruption to service with minor impact on service user care.	Some disruption in service with unacceptable impact on service user care. Temporary loss of ability to provide service	Sustained loss of service which has serious impact on delivery of service user care or service resulting in major contingency plans being involved	Permanent loss of core service or facility. Disruption to facility leading to significant 'knock on' effect
Adverse publicity/ Reputation	Rumours, no media coverage. No public concerns voiced. Little effect on employees morale. No review/investigation necessary.	Local media coverage – short term. Some public concern. Minor effect on employees morale / public attitudes. Internal review necessary.	Local media – adverse publicity. Significant effect on employees morale & public perception of the organisation. Public calls (at local level) for specific remedial actions. Comprehensive review/investigation necessary.	National media/ adverse publicity, less than 3 days. News stories & features in national papers. Local media – long term adverse publicity. Public confidence in the organisation undermined. HSE use of resources questioned. Minister may make comment. Possible questions in the Dáil. Public calls (at national level) for specific remedial actions to be taken possible HSE review/investigation	National/International media/ adverse publicity, > than 3 days. Editorial follows days of news stories & features in National papers. Public confidence in the organisation undermined. HSE use of resources questioned. CEO's performance questioned. Calls for individual HSE officials to be sanctioned. Taoiseach/Minister forced to comment or intervene. Questions in the Dail. Public calls (at national level) for specific remedial actions to be taken. Court action. Public (independent) Inquiry.
Financial Loss (per local Contact)	<€1k	€1k – €10k	€10k – €100k	€100k – €1m	>€1m
Environment	Nuisance Release.	On site release contained by organisation.	On site release contained by organisation.	Release affecting minimal off-site area requiring external assistance (fire brigade, radiation, protection service etc.)	Toxic release affecting off-site with detrimental effect requiring outside assistance.

1. LIKELIHOOD SCORING

Rare/Remote (1)		Unlikely (2)		Possible (3)		Likely (4)		Almost Certain (5)	
Actual Frequency	Probability	Actual Frequency	Probability	Actual Frequency	Probability	Actual Frequency	Probability	Actual Frequency	Probability
Occurs every 5 years or more	1%	Occurs every 2-5 years	10%	Occurs every 1-2 years	50%	Bimonthly	75%	At least monthly	99%

3. RISK MATRIX

	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
Almost Certain (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Rare/Remote (1)	1	2	3	4	5

Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Appendix 4:

Risk Assessment Exercise

1. Risk Issue

2. Risk Description (using ICC approach)

3. Risk Analysis & Evaluation

a. Impacts/Vulnerabilities (list here)

b. What Controls need to be in place to manage this risk?

c. Existing Controls (list here)

d. Initial Likelihood Score (tick appropriate box)

Rare/Remote (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain(5)

e. Initial Impact Score (tick appropriate box)

Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme(5)

f. Initial Risk Rating (Insert Number in Box below colour)

GREEN	AMBER	RED

g. Does the risk need further actions to control it? Y ☐ N ☐

h. Additional Controls Required (Action Plan)

i. Residual Likelihood Score (tick appropriate box)

Rare/Remote (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain(5)

j. Residual Impact Score (tick appropriate box)

Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme(5)

k. Residual Risk Rating (Insert Number in Box below colour)

GREEN	AMBER	RED

Appendix 5,
(fig a.)

Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Risk Assessment Form

* One Risk only per form

Administrative Area: _____
Location: _____
Section/Ward/Dept: _____
Date of Assessment: _____
Source of Risk: _____
Unique ID No: _____

Primary Risk Category: _____
Secondary Risk Category: _____
Tertiary Risk Category: _____
Name Risk Owner: (BLOCKS) _____
Signature of Risk Owner: _____

RISK DESCRIPTION	IMPACTS/VUNERABILITIES	EXISTING CONTROL MEASURES	ADDITIONAL CONTROLS REQUIRED	PERSON RESPONSIBLE FOR ACTION	DUE DATE

RISK ANALYSIS

INITIAL RISK			RESIDUAL RISK			STATUS
Likelihood	Impact	Initial Risk Rating	Likelihood	Impact	Residual Risk Rating	

Appendix 5 Continued: - Completing the Assessment Form and populating the electronic risk register.

The information required to populate the risk assessment form is detailed below. The risk assessment form will be used to populate the electronic risk register.

Administrative Area	Enter Administrative Area e.g. HSE Dublin North East, Hospital Network 3
Location	Enter Location name e.g. Hospital Name
Section/Ward/Dept	Enter the section/ward/department e.g. Surgery
Date of Assessment	Enter the date the assessment was made e.g. date of the workshop.
Risk Source	Identify from the drop down list how the identified risk was sourced i.e. did it come from a facilitated workshop, or from a risk suggestion scheme.
Unique ID	This is required for the purpose of transferring risks elsewhere and also for the purpose of aggregation; every risk on the risk register should have a unique ID reference.
Risk Category (Primary)	Select the Primary Risk Category from the HSE Risk Categorisation List (see Appendix 8)
Risk Category (Secondary)	Select the Secondary Risk Category from the HSE Risk Categorisation List (see Appendix 8)
Risk Category (Tertiary)	Select the Tertiary Risk Category from the HSE Risk Categorisation List (see Appendix 8)
Risk Owner	This is the individual who will be held accountable for the risk and its effective control. The maxim of the 'risk take is the risk owner' should be taken.
Signature of Risk Owner	The signature of the Risk Owner.
Risk Description	When describing risk it is important to describe the risk using the 'ICC' approach. Describe the potential **'IMPACT'** if the risk were materialised. Describe the **'CAUSAL FACTORS'** that could result in the risk materialising. Ensure that the **'CONTEXT'** of the risk is clear, e.g. is the risk 'target' well defined (e.g. employees, patient, department, hospital etc.) and the 'nature' of the risk clear (e.g. financial, safety, physical loss, perception, etc.)
Impacts/Vulnerabilities	Enter the impacts and vulnerabilities that the risk has on the service user, employees and organisation.
Existing Control Measures	Enter a description of what administrative/procedural/existing controls measures are currently in place to mitigate the risk
Likelihood	Based on the HSE Risk Matrix – what likelihood score would you give the risk (1-5)? The Likelihood is the rating

	based on the risk with its current controls in place and NOT the risk as it would be with no controls in place.
Impact	Based on the HSE Risk Matrix – what Impact score would you give the risk (1-5)? The Impact is the rating based on the risk with its current controls in place NOT the risk as it would be with no controls in place.
Initial Risk Rating	Based on the HSE Risk Matrix – multiplying the inherent Impact by the likelihood will give the risk rating (1-25)
Additional Controls Required	What measures are needed to eliminate or further reduce the level of risk that the risk presents? Consider the hierarchy of controls: elimination / substitution / engineering / administrative / PPE. Try to consider both long and short-term measures.
Likelihood	Based on the HSE Risk Matrix – what likelihood score would you give the risk (1-5)? The Likelihood is the rating based on the risk with additional controls required in place and NOT the risk as it would be with no additional controls required in place.
Impact	Based on the HSE Risk Matrix – what Impact score would you give the risk (1-5)? The Impact is the rating based on the risk with the additional control required in place NOT the risk as it would be with no additional controls required in place.
Residual Risk Rating	Based on the HSE Risk Matrix – multiplying the Impact by the likelihood will give the risk rating (1-25)
Person Responsible	Enter the name of the person responsible for the additional control necessary to mitigate the risk. The person responsible could be the risk owner but could also be someone else.
Due Date	Enter the date by which implementation of the additional controls to mitigate the risk are due.
Risk Status	The three options available for risk status are: Open, i.e. additional controls have been identified as necessary Monitor, i.e. existing controls are deemed adequate to manage the risk but these need to be periodically reviewed. Closed, i.e. that the risk no longer exists e.g. where an unsuitable premises is replaced by a suitable one.

Appendix 5,
(fig. b)

Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Additional Controls (Actions) Update Form

*** Attach this form to original Risk Assessment Form**

Action Owner: _____

Unique Risk ID No: _____

Date of Update: _____

ACTION NUMBER	ADDITIONAL CONTROL (ACTION) SUMMARY UPDATE	PERSON RESPONSIBLE FOR ACTION (if changed)	Action STATUS { Behind Schedule / On Schedule / Complete }	NEW REVIEW DATE

Appendix 6: – Control Measures

What is a Control Measure?

A control measure is any process, policy, device, practice or other action that acts to minimise negative risk or enhance positive opportunities. It is essential consequently, when seeking to minimise the risk posed by any hazard to have in place sufficient controls.

Classification of Internal Controls

There are two main ways of classifying the nature of internal controls available.

1. By function i.e. what are they attempting to do
2. By robustness i.e. their level of effectiveness in preventing risks occurring

Classification by Function

- **Preventative:** These focus on preventing errors or exceptions, examples include:
    - Standards, policies and procedures are the most basic type of preventive control.
    - Segregation of duties also acts as a preventive control against fraud.
    - Authorization / Approval levels also prevent the risk of an illegal act and are thus preventive in nature.

- **Detective:** These are designed to detect errors or irregularities that may have occurred, examples include:
    - Reviews
    - Reconciliation
    - Variance Analysis
    - Audit

- **Directive:** These are designed to tell employees what to do, examples include:
    - Written Policies
    - Reporting lines
    - Supervision
    - Training

- **Corrective:** These are designed to correct errors or irregularities that have been detected, examples include:
    - Continuity Plans e.g. major incident plans, business continuity plans
    - Insurance
    - Contract terms

Classification by Robustness

Some controls are better at minimising risk than others and to assist managers in identifying the most robust controls reference should be made to the hierarchy of control measures. The higher on the hierarchy the control is, the greater the potential is that it will minimise the risk. Consideration should be given as to what level on the hierarchy of control the controls are selected from.

The hierarchy of control measures are as follows:

A. Elimination the job is redesigned so as to remove the hazard (risk factor). However, the alternative method should not lead to a less acceptable product or less effective process. If hazard elimination is not successful or practical, the next control measure is:

B. Substitution replacing the material or process with a less hazardous one. If no suitable practical replacement is available, the next control measure is:

C. Engineering controls installing or using additional equipment. If this method is not effective, the next control measure is:

D. Administrative procedures or safe work practices e.g. policies, procedures, guidelines.

Only after all the previous measures have been tried and found to be ineffective in controlling the risks should Personal Protective Equipment be considered.

E. Personal Protective Equipment (PPE)

This is the last control measure to be considered. If chosen, PPE should be selected and fitted to the person who uses it. Employees must be trained in the function and limitation of each item of PPE. PPE may be used as a temporary control measure until other alternatives are installed. In most cases a combination of engineering controls, administrative procedures and PPE are chosen to effectively control the risks. Where PPE is the main control method it should be (where practical) used in conjunction with another method of PPE and safe work practices.

It is important to realise that the higher up the control hierarchy the controls are, the more reliable they tend to be and should be considered as a first option. Controls which rely on people following correct procedures i.e. administrative or PPE controls are not as reliable and if the control of a risk is reliant on these then it is necessary to actively consider weakness in existing procedures and opportunities for error. This enables treatment of risks to be improved by reducing the likelihood of error or introducing focused monitoring procedures.

Existing Controls

All controls to minimise the risk that currently in place should be listed on the risk assessment form. When listed, time should be taken to consider their adequacy, method of implementation and level of effectiveness in minimising the identified risk to the lowest reasonably practicable level.

Evaluating the adequacy of Existing Controls

It is accepted that risk will never be eradicated from services, however it is important that managers seek to minimize the risk to the lowest reasonably practicable level.

To this end the ALARP principle can be used to assist managers in making this judgement (see figure 2 below).

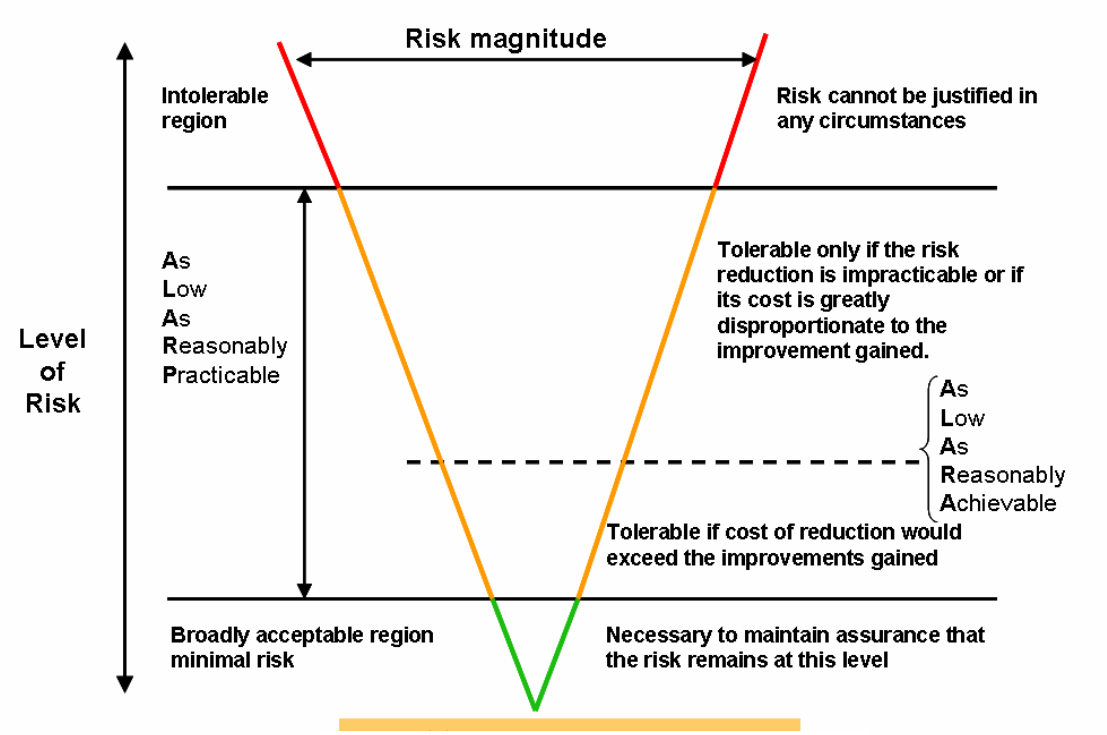


Fig 2 The ALARP Principle

The width of the cone indicates the size of the risk. In general, two criteria can be defined. A level where risk is negligible and can be accepted without specific treatment other than monitoring (these risks are often rated as green); and a level which is intolerable and the activity must cease unless the risk can be reduced (these risks are often rated as red). Between these levels is the region where costs and benefits are taken into account. When risk is close to the intolerable level the expectation is that risk will be reduced unless the cost of reducing the risk is grossly disproportionate to the benefits gained. Where risks are close to the negligible level then action may only be taken to reduce risk where benefits exceed the costs of reduction.

Accept the Risk

A risk is called acceptable if it is not going to be treated, accepting a risk does not imply that the risk is insignificant. Risks in a service may be accepted for a number of reasons,

- The level of the risk is so low that specific treatment is not appropriate within available resources (* as low as is reasonably practicable – ALARP see above)
- The risk is such that no treatment option is available within the control of the HSE. For example, the risk that a project might be terminated following a change of government is not within the control of the HSE.
- The opportunities presented outweigh the threats to such a degree that the risk is justified.

Once a decision has been made to accept the risk a process needs to be put in place to monitor and review the risk. The review date and the risk status of ‘monitoring’ needs to be documented on the risk assessment form.

Additional Controls

For those risks that are not deemed accepted, the team need to consider the options available to them to treat the risks. A combination of options may be appropriate in treating risks. The options may be avoidance, transference, & internal controls.

2.1 Avoidance

This is achieved by either deciding that the additional control required is not to proceed with the activity that contains an unacceptable risk, choosing an alternate more acceptable activity, which meets the objectives and goals of the organisation, or choosing an alternative and less risky methodology or process within the activity.

2.2 Transference

Risk transference is achieved by deciding that the additional control required is to transmit the organisation's risk to an outside party. The most common method of risk transfer is the purchase of insurance or indemnity. The cost and conditions of such a transfer will be dependant on the level of assurance the organisation can provide to the insurer in terms of the likelihood of a claim occurring. The insurer would require information on type of risk, the robustness of the systems that the organisation has in place and the claims history to date. An example of this is clinical, public and employee liability coverage.

2.3 Internal Controls

This is the most commonly used treatment option as it is focused on reducing the likelihood of the risk occurring or the impact of the risk if it occurs, or both. Note that there is a trade off between the level of risk and the cost of reducing those risks to an acceptable level. The most effective methods of risk control are those which redesign the systems and processes so that the potential for an adverse outcome is reduced. In choosing additional internal controls the hierarchy of controls should be considered. It is important to remember to ensure that the controls chosen should target the vulnerabilities/impacts identified and that they can only been considered as controls when they are effectively implemented.

Appendix 7 - Risk Management Escalation Pathway

Appendix 8 – Risk Categorisation

Primary Risk Category	Secondary Risk Category	Tertiary Risk Category
Patient Care & Safety (Provision of Care)	**Communication**	Verbal Communication
		Written Communication
		Non Verbal Communication
	Task Factor	Guidelines Procedures &policies
		Decision making aids
		Procedural or task design
	Team and Social Factors	Role Congruence
		Leadership
		Support and Cultural Factors
	Access and Continuity	Availability/Access
		Appropriateness
		Timelines/delays
		Continuity
		Over/under Utilisation
		Volume/capacity
		Interfaces
	Patient & Family & Advocate Rights	Information & Consent
		Confidentiality
		Security
		Satisfaction/Complaints
		Privacy
		Participation
		Comfort/Convenience
	Assessment of Patient	Adequacy of assessment
		Error (laboratory/reporting/interpretation)
		Appropriateness
	Delivery of Care	Standards of care
		Competence
		Safety
		Care/treatment accidents/prescribing accidents
		Drug admin accidents
		Efficacy
		Clinical trial/new treatment
		Care planning
		Availability & adequacy of protocols
		Nosocomical Infection
		Immunisation
		Product/Service failure

		Availability of appropriate clinical expertise
	Patient & Family Education	Clear Communication
		Clear Language
		Patient Compliance
		Medicine Management
		Tissue Viability
	Information Management	Documentation/Recording
		Management of Healthcare Records
	Planning of Services	Standards of Care
		Resource Availability
		Information for Decision making
		Management planning & service development
	Other	Other
Human Resources	**Employee Safety Health & Welfare**	Safe Systems of work
		Instruction/Training/Supervision
		Security (inc Violence & Aggression)
		Psychosocial Hazard
		Moving & Handling
		Slips/Trips/Falls
		Hazardous Exposure
		Administrative factors
		Design of physical environment
		Environment
		Staffing
		Workload
	Recruitment	Verification of Qualifications/ Registration
		Recruitment
		Selection
		Retention
		Competence Assurance
		Garda Vetting
		Occupational Health Screening
	Learning & Development	Induction
		Employee Performance
		Team Performance
		Employee Development
		Education Training & Development
		Training Records & Qualifications maintenance

		Personal & Professional Development Process
		Employment Law (Managers)
		Teamwork
	Maintaining a Quality Workforce	Succession planning
		Turnover
		Performance/Appraisal
		Workforce planning
		Culture
		Productivity
		Efficiency
		Coverage/skill mix
		Employees morale
	Employee Relations	Absence Management
		Dignity in the Workplace
		Trust in Care
		Employee and Industrial Relations
		Employment Contract Management
		Terms and Conditions of Employment
Governance	**Goals/Objectives**	Structure
		Leadership
		Accountability
		Authority
		Capability
		Outcomes
		Consultation
		Change Management
		Information for decision making
	Integrity	Confidentiality
		Fraud
		Corruption Unauthorised use
		Unethical practice
		Illegal Acts
		Reputation
		Conflict of Interest
		Compliance
		Accountability
	Assurance	Internal Controls
		External Controls
Legal & National Standards/Policy	**Regulatory**	Compliance
		Organisational Liability

		Individual Liability
	Contractual	Compliance
		Organisational Liability
		Individual Liability
	National Standards/Policy	Compliance
Financial	**Procurement**	Product/service failure
		Service delivery Internally/Externally
		Vendor / Suppliers Management Contract
		Vendor / Suppliers Management Non-Contract
		Quality Control
		Procurement policies and protocols.
		Inventory Management (Stock Control)
	Management Accounting	Budget Control/Vote
		VFM
	Financial Accounting	Cash Flow
		Revenue (Tax, PRSI, VAT)
		Cash Collection/Accounts Receivable
		Bad Debts
		Investments
		Foreign Exchange
		Accounts Payable
		Insurance
		Misappropriation/Fraud
		Payroll
		Asset Management
		Patients Private Property (PPP)
ICT Information Communication Technology	**Systems failure/availability**	
	Information Security	
	Hardware	
	In-house Software	
	Software Other	
	Networks	
	Operating Systems	
	ICT Training	
Equipment (Non ICT)	**Clinical Equipment**	Availability
		Reliability
		Efficiency/Economy
		Compatibility

		Operator competence
		Unauthorised interference
		Tracking/Security
		Maintenance
		Cleaning/Decontamination
	Non Clinical Equipment	Availability
		Reliability
		Efficiency/economy
		Compatibility
		Operator competence
		Unauthorised interference
		Tracking/Security
		Maintenance
		Cleaning/Decontamination
Estates Management	**Existing Facilities**	Preventative Maintenance
		Fit for purpose
	Capital Developments	Project Planning
		Resource availability
	Environmental	Environmental Impact
		Conservation
		Waste
		Fire/Explosion/Flooding
		Radiation Hazard
		Chemical Hazard
		Biological Hazard
		Electricity Hazard
		Food Hygiene
		Security
		Physical Hazard
		Insects Rodents
		Contractors
External Influences	**Government/Political**	Policy
		Funding
	Demographics	
	Technological advances	
	Other Health providers	
	Customer needs and expectations	
	Public awareness	
	External Disasters	
	External Relations	
	Labour Market/Suppliers Market	
	Industrial Relations	

	Environmental	
	Pandemic Disease	

Appendix 9: FOCUS - PDCA Model

To improve the safety and quality of services it is vital that risks identified are addressed. One mechanism for doing this is to use them as a basis for developing quality improvement strategies. There are many tools that can be used to improve quality. A simple yet powerful tool for accelerating improvement is the FOCUS - PDCA Model. The model is not meant to replace change models that services may already be using, but is proven in relation to accelerating improvement. This model has been used very successfully by hundreds of health care organisations in many countries to improve many different health care processes and outcomes.

The model has two parts:

1. The FOCUS Phase (this helps to narrow the team's attention to a discrete opportunity for improvement)
   - F- Find a process to improve (e.g. an *action on the register)*
   - O- Organise to improve the process
   - C – Clarify current knowledge of the process
   - U – Understand sources of process variation
   - S – Select the process improvement

2. The PDCA Phase (this allows the team to peruse that opportunity and to review its outcome i.e. to test and implement changes in real work settings)
   - P – Plan the improvement data collection
   - D – Do the improvement/data collection/data analysis
   - C – Check the data for process improvement
   - A – Act to hold the gain/continue the improvement

See Table below for a more detailed description of this model.

FOCUS P-D-C-A Performance Improvement Model to Identify and Solve Problems and Processes		
The FOCUS phase helps to narrow the team's attention to a discrete opportunity for improvement.		
F	**FIND**	*Find a process that needs improvement.* Define the process and its customers. Decide who will benefit from the improvement. Understanding how the process fits within the hospital's system and priorities.
O	**ORGANIZE**	*Select a team who is knowledgeable in the process.* Determine team size, members who represent various levels in the organization, select members, and prepare to document their progress.
C	**CLARIFY**	*Clarify the current knowledge of the process.* Define the process as it is and as it should be. Team reviews current knowledge and then must understand the process to be able to analyze it and differentiate the way it actually works and they way it is meant to work.
U	**UNDERSTAND**	*Understand the causes of variation.* Team will measure the process and learn the causes of variation. They will then formulate a plan to data collection, collecting the data, using the information to establish specific, measurable, and controllable variations.
S	**SELECT**	*Select the potential process improvement.* Determine the action that needs to be taken to improve the process (must be supported by documented evidence.)
The P-D-C-A phase allows the team to pursue that opportunity and review its outcome.		
P	**PLAN**	*Plan the improvement/data collection.* Plan the change by studying the process, deciding what could improve it, and identifying data to help.
D	**DO**	*Do the improvement/data collection/data analysis.* Execute the plan on a small scale or by simulation.
C	**CHECK**	*Check the data for process improvement.* Observe the results of the change. Document the results of the change. Modify the change, if necessary and possible.
A	**ACT**	*Act to hold the gain/continue improvement.* Implement the change if it is working. If it fails, abandon the plan and repeat the cycle.