

### COMPLETING A RISK ASSESSMENT

#### Introduction

Risk assessment is not complicated. This guidance should help you complete a risk assessment using the Trust proforma found in Appendix 2.

There are 5 steps to carrying out a risk assessment

- i. Risk Identification
- ii. Risk Analysis
- iii. Risk Evaluation
- iv. Risk Treatment – (Action Planning)
- v. Review

Risk assessment establishes **actual** levels of risk and most importantly, should lead to action to prevent or control the risk.

#### **1. Where to Start – Risk Identification**

In order to produce a baseline risk profile for the speciality/department/Directorate, the following steps might be useful:

- i. Review all risk assessments held on the existing Risk Register. For any risks that no longer exist - update the old risk assessment form accordingly, remove from risk register and file in an **archive** risk register file for resolved risks. Note any risks that **still** remain a risk.
- ii. Review the department's incident reports, complaints and claims over the past 12 months (reports from the DATIX system will help with this) to see whether any risks become apparent.
- iii. Review departmental service delivery objectives, any project objectives and risk assess.
- iv. Brainstorm (involving as many team members as possible) what the key areas of work are (in and out of hours) and what clinical and non-clinical risks are associated with them. Example checklists for considering Health & Safety Risks and clinical risks are available under Risk Management on ICID.
- v. Articles in professional or other journals or summaries of complaints, claims, or reviews from other organisations may flag up potential risk areas for your area/service.
- vi. You may come across some risks which can be dealt with quickly and without needing approval from anyone else e.g. re-route a trailing wire, remove boxes in danger of falling on someone. If so - take the action immediately and do not analyse further or record.
- vii. Some risks may be identified that are never going to happen and even if they did they would cause very little harm - take no further action with them unless the level of risk increases later.

- viii. For risks that might occur and if they did might cause some injury, damage, organisational or financial loss you will want to carry out some further ANALYSIS and EVALUATION.

## **2. Risk Analysis**

Each risk identified should be analysed.

The following should be considered:

- i. What the risk is e.g. what hazard is present (object, substance, activity with the potential to cause harm), what harm might potentially be caused e.g. injury/damage/financial loss, and who might be at risk of being harmed e.g. patients, staff, visitors, or the organisation. This information should be inserted into the box on page 1 of the risk assessment document entitled 'Description of Risk.'
- ii. What are the current controls in place for this risk? Identify existing management, technical systems and procedures, which are in place to control the risk e.g. policies, guidelines, physical barriers, checking systems and audit procedures. Bullet point these in the box titled 'existing controls'.
- iii. Next identify whether the controls are adequate/inadequate/uncertain and note for yourself what their weaknesses are (as this will form part of the action plan).

## **3. Risk Evaluation**

Risks are evaluated to give a risk rating by multiplying the consequence with the likelihood of the risk materialising. This process, if applied as accurately as possible, allows the prioritisation of risks i.e. separating the high from the low and so prioritising where resources and actions should be focused.

To evaluate the level of risk refer to the Risk Matrix (Assessing the Level of Risk - Appendix 3). The risk must be evaluated in the context of existing controls, be objective, realistic and evidence based where possible – this allows for a more robust system which can be held up to scrutiny.

For the identified risk consider:

What would the **consequences** be if the risk did occur (taking into account the current levels of control)? This assessment should be realistic and based on knowledge of actual events, experience or reported events wherever possible. Potential sources of information may include past records, incident data, published data, audit data, expert opinion.

What would the **likelihood** be of this risk occurring at the level of consequence identified (taking into account the current level of controls)? This assessment should also be based on knowledge or experience whenever possible, for example taking into account the number of similar incidents that have been reported already. Potential sources of data are described above.

A **risk rating score** is then produced by multiplying the consequence rating by the likelihood rating.

This **risk rating score** can then be looked up on the level of risk matrix and a **level of risk** determined (low, moderate, high, extreme). Appendix 3, section 4 then indicates what level of action and should be taken with level of responsibility within the organisation.

## **4. Risk Treatment and Action Planning**

### **Risk Treatment Plan**

In the Risk Treatment Plan area of page 1 of the risk assessment form the risk can be accepted with a future date for monitoring and review (this should only be the treatment of choice if the risk is deemed to be low). Otherwise the risk assessor should indicate that the risk is not accepted and continue to complete the action planning area of the form.

### **Action Planning**

A Risk Action Plan should be developed for any risks requiring action to reduce or avoid.

In some cases a combination of treatment options may be necessary e.g. actions to reduce the likelihood of the risk and/or actions to reduce the potential consequences if the risk does occur.

**Treatment** options include:

- **Avoid** the risk  
e.g. by ceasing the risk activity, withdrawing the equipment from use etc.
- **Reduce** the **likelihood** of the risk materialising  
e.g. through contract conditions, audit and compliance programmes, preventative maintenance, supervision, training etc.
- **Reduce** the potential **consequences** if the risk does occur  
e.g. through contingency planning, minimising exposure to the risk, public relations, relocation of activity
- **Transfer** all or part of the risk to another party  
e.g. through contractual arrangements or 'insurance'.

Selecting the most appropriate treatment option involves balancing the cost of implementing each treatment option against the benefits to be derived from it. In general the cost of managing risks needs to be commensurate with the benefits obtained.

The action plan should be documented on page 2 and 3 of the risk assessment paperwork.

The treatment options and Risk Action Plans should be discussed and agreed at departmental/Directorate meetings, cascading the matter up the organisation as appropriate to the level of risk, and as set out in this policy.

Page 3 of the Risk Assessment form should be used to document the risk treatment options being pursued, the target risk rating or residual risk i.e. the estimated level of risk remaining once the actions have been completed, the resource implications, and monitoring arrangements. The target risk rating (often referred to as residual risk) is an important measure as it gives an indication as to how well the risk can be managed with current measures.

## **5. Monitoring and Review**

Risk assessments should have realistic review dates.

All risks should be reviewed at time intervals appropriate to the level of risk using page 4 of the risk assessment paperwork. The higher the risk the more frequently it should be reviewed to capture progress with the risk reduction measures.

Any risk should be reviewed at least annually.

Any new high level (8 or above) risks or changes to risks/action plan updates must be communicated through the relevant Directorate office so that Datix can be updated as appropriate.