Guidance Note 3 - Pre-Incident Planning

Introduction

Pre-incident planning follows the phases of an incident, as illustrated below:

- **Prevention Planning**: those arrangements needed to limit the possibility of untoward events happening.
- **Pre-incident planning**: preparations for mitigating likelihood and severity of an incident.
- **Emergency response**: the measures needed to ensure a rapid and appropriate response to an emergency.
- **The preparation of a post incident recovery plan**, to return to “research-as-usual”.

The diagram above illustrates the concept on which plans may be formulated:

- The planning activity takes place before an incident. This is the preparation of a Research Continuity Plan, and includes both planning and testing.
- As soon as an incident occurs then an emergency response is made.
- Concurrent with this is a crisis management response by the organisation locally and with head office support, for example the issuing of press statements in conjunction with the site affected.
- Also initiated concurrently is the recovery of the building, people and processes necessary to regain Research as Usual (RAU).
- The time scale is arbitrary and the time taken to regain normal working will vary from days to months.
Prevention Planning

Time spent in preparing emergency and recovery plans will be well rewarded should your establishment face a potentially harmful unexpected event. However, prevention is better than a cure, and resource invested in preventing disruption can help maximise productivity.

Prevention Planning could include:
♦ Suitable Health and Safety, Security and Fire measures that prevent incidents. Such measures should include assessment and control of risk; reporting, investigation and correction of non-conformances
♦ Suitable IT security to prevent malicious outages; suitable redundancy to prevent routine outages
♦ Suitable security measures for staff, visitors and contractors, as well as for incoming packages and mail
♦ Establishing "housekeeping" rules that will minimise operational risk, e.g. clear corridors, safe storage of hazardous materials including waste
♦ Supplier selection during the procurement process to minimise supply chain risk
♦ Planned preventative maintenance to ensure vital equipment and facilities are in good order and serviced/maintained according to manufacturer's instructions or to accepted best practice
♦ Awareness training ensuring that all staff are proactive in highlighting areas of improvement in management systems

There will also be a need to ensure that regular checks are made of systems to ensure that up to date information is held. A template is shown below of examples of such checks that may be made on a rolling programme to help with pre-incident planning.

Pre-incident planning

In the pre-incident planning stage, those facilities and procedures that will reduce the risk (likelihood and severity) of a failure or emergency are identified and put into place. This allows the organisation to maintain a state of “readiness” to respond to disruptions.

♦ Ensuring all emergency equipment is suitable and in good working order
♦ Ensuring staff understand potential risks and know how to deal with them through suitable training programmes, exercises and rehearsals, e.g. fire safety training and dealing with telephone, bomb and similar threats, evacuations and drills
♦ Ensure staff contact lists are up-to-date, and communication systems are in working order
♦ Third parties (e.g. neighbours, local planning offices, emergency services and response contractors) should be regularly contacted to ensure continuity of relationship, and their potential response known and accounted for
♦ Ensure suitable insurance is in place, and in lieu of insurance, potential liabilities should be known, and appointed loss adjusters should be known
Press statements and media training can be prepared in advance

Post-incident counselling and staff welfare facilities should be in place

**Emergency Response Planning**

Foreseeable events such as fire, bomb or other security threats should be included in these plans. Detailed guidance for fire safety management is dealt with in the MRC "Fire Safety" Policy and Guidance. Detailed guidance for security management is dealt with in the MRC "Security" Policy and Guidance.

Establishments should have plans for reacting to an emergency, for example:

- An incident or threat occurring during normal hours.
- An incident or threat occurring out of normal hours.
- Evacuating the building (to primary and secondary assembly/muster points) and ensuring the safety of personnel
- The first steps to take such as contacting host institute, regional MRC administration and head office
- Foreseeable disruption scenarios, such as loss of staff (e.g. pandemic, inclement weather), denial of access (e.g. protest/roadworks), loss of utility (e.g. power, water), fire/flood, Malicious event (e.g. bomb/white powder incident), loss of key supply (e.g. diet/bedding, cryogen)

For further information on emergency planning, please see Guidance Note 6 of the MRC Security Policy and Guidance.

**Recovery Planning**

Recovery planning should assist with returning to business as usual after an incident. Typical considerations for recovery planning should include:

- Third-party assistance for salvage, clean-up and document recovery
- Third party assistance for completing work back-logs
- Overtime arrangements for completing work back-logs
- Procedures for mobilising additional resources and funds to return to normal operation
## Appendix 1 – Pre-incident Planning template

<table>
<thead>
<tr>
<th>TASK</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monthly</strong></td>
<td></td>
</tr>
</tbody>
</table>
| At normal monthly meetings make ‘Consequence Management’ an agenda point and debate one of the suggested 12 issues each month. In this way no issue is more than 11 months away from having been reviewed. Ensure that issues raised that might have a strategic ramification are passed to Head Office for consideration. | 1. Care for staff post incident, counselling etc  
2. Alternate facilities and equipment  
3. Third parties involved in the plan  
   - Contractors  
   - Suppliers  
   - Landlords  
   - Neighbouring facilities  
4. Financial ramifications of an incident, cost codes, hardship payments, lines of credit etc.  
5. Liaison with host’s insurers and loss adjusters  
6. Recovery services for documents and IT hardware  
7. IT backups and recovery times  
8. Critical systems recovery including telephony  
9. Pre prepared Press statements and media hosting plans  
10. HR issues internal and procedural e.g. next of kin contact addresses, telephone help lines etc  
11. Local authority and emergency services relationships  
12. Any other issues not covered above |
| **Quarterly** | |
| Review detailed training needs analysis of existing and any new staff who hold roles in the response system | In conjunction with HR and training managers Ensure that where appropriate the crisis management role is placed on personnel records and put into the job specification of the post holder |
| Conduct a scenario based exercise increase awareness and learn of potential gaps in planning | To construct the desktop scenario refer to risk and hazard analysis and BIA materials. Report remedial actions to the BC manager of the unit(s) |
| Ensure improvement plans are progressed and cascaded to Corporate Resilience | Update progress plans for health & safety, research continuity |
| Ensure information systems are up-to-date | Update telephone cascades |
| Conduct localised inspections | Ensure operational risk (e.g. fire) is minimised |

MRC Research Continuity Standard of Practice  
Corporate Safety, Security and Resilience  
Version 2, October 2013