

**B/02/033**

## **Annex G**

### **ORGANISATIONAL CAPACITY FAILURE**

1. Among the subsidiary risks here are
  - poor leadership
  - inability to respond quickly
  - lack of creativity, innovation
  - initiative overload

This will all be absorbed by the Change Programme and more detailed analysis will be completed later.

2. The other subsidiary risks were
  - information mismanagement
  - sudden loss of key facilities

An analysis for each is attached

## Information Mismanagement

<b>RISK</b>	PROBABILITY OF RISK	INCREASING or DECREASING?	EFFECT \ CONSEQUENCE OF RISK	WHAT CONTROL MEASURES ARE IN PLACE?
<b>1 Statistics</b>  - absence of key statistics relating to fulfilment of business needs  - ICC  - Insufficient/ inadequate evaluation	M	decreasing	Poor use of resources Loss of reputation	Stats programme Intelligence hub
	M	?	As above	Evaluation Committee
	L	decreasing	As above	
<b>2 Knowledge Management</b>  - inability to retrieve key data  - not making best use of resource that is available  - reach wrong conclusions or inability to reach right ones  - tunnel vision (not using other people's intelligence)	M to L	steady	Slow on our feet Lack of consistency Lost opportunities	EPM
	M to L	decreasing	Waste, duplication	Change Programme
	L to M	steady	Loss of reputation, Waste	Professional Management
	M	steady	All the above	Change Programme Management
<b>3 Information confusion</b>	M	steady	As above	Programme approach REFIT Management

**Risk 10 - Sudden, unexpected loss of key facilities**

<b>A: Failure of key components</b> <b>B: Fire, flood, natural disaster</b> <b>C: Attack</b>	
<b>Probability of Risk</b>	low
<b>Increasing or Decreasing</b>	increasing
<b>Effect/consequence of risk</b>	Fixed line telephones/faxes do not work. IT does not work. Scientific facilities do not work. Building cannot be used or may be destroyed. Key HSE personnel may be dead or injured. Consequence is HSE's ability to perform its urgent functions effectively may be impaired.
<b>What control measures are in place?</b>	Duplication/back-up/loan arrangements. Security, fire and IT security arrangements. Disaster recovery plan for HQ sites.
<b>What mechanisms provide assurance that they are operative effectively?</b>	Planned testing eg of fire alarms and evacuation, demolition of St John's House. Unplanned testing and evaluation of response, eg key component failure, suspect parcel containing anthrax at Bootle central despatch.
<b>Do any new measures need to be added?</b>	Likely. To be specified in light of a review of this risk now starting and "civil contingencies" project.
<b>If new measures are to be added when will they be in place?</b>	To be determined in light of review above.

**Risk 8 (part in record keeping)**

**A: Loss of electronic records**

See risk 10 - IT arrangements cover security and availability. Risk is currently being reviewed as part of project to secure ISO 7799 - Information Security - accreditation.