



Business Continuity Planning for Sponsored Bodies - the Step by Step Approach

***First Stage Part 2 Workshop –
Business Recovery Requirements &
Risk Reduction***

**20th January 2006
Amanda Millhouse
Gerry Boulton
Robin Moses**



Agenda

- Introduction
- The overall approach
- The first stage – part 2
 - obtain the business recovery requirements information
 - resolve queries, agree and document results
 - Stage 1 report
 - exercise 1
 - start to consider required risk reduction controls
 - exercise 2
- Open forum discussion
- Summary and next steps
- “Surgeries”

The overall approach to business continuity planning





First stage – part 2: obtain the business recovery requirements information (1)

- interviews with/forms completion by senior managers - for each business function per location
 - based agreed potential adverse impacts on business operations - five differing unavailability time periods
 - criticality priorities and related resources, etc.
 - timescales for recovery related to criticality priorities
 - minimum business recovery requirements per business function per location by time period



First stage – part 2: obtain the business recovery requirements information (2)

- Each form completed with (a):
 - ‘identification information’ (at top of form)
 - for each row against five time periods in column
 - personnel roles in business function (only if useful)
 - minimum resources required: personnel
 - minimum resources required: IT & data communications equipment, services and facilities
 - minimum resources required: voice (if relevant including mobile, fax and pager) communications



First stage – part 2: obtain the business recovery requirements information (3)

- Each form completed with (b):
 - for each row against five time periods in column
 - minimum resources required: other non-IT equipment, facilities, services, collections, etc. – as relevant
- Then - based on minimum requirements for personnel, IT & data comms, voice comms and other non-IT facilities, etc.
 - record for each of the five time periods
 - minimum resources required: accommodation



First stage – part 2: the business recovery requirements - resolve queries, agree and document results (1)

Things to watch out for (a)

- Business impact ratings as informal indicator of proportion of:
 - people to be at work immediately following a disaster/failure
 - those who don't need to come in to work
 - etc.
- Potential inconsistencies - minimum requirements must be justified by the potential adverse business impacts



First stage – part 2: the business recovery requirements - resolve queries, agree and document results (2)

Things to watch out for (b)

- Requirements are realistic
- Requirements account for critical points in year
- Minimum requirements are identified, rather than 'would like to have' requirements
- Care taken in identifying and handling issues associated with 'collections'



First stage – part 2: resolve queries, agree and document results (3)

- Resolve queries and agree results
- Document results:
 - Form for consolidating requirements by business area and by location
 - Produce first stage report

(see template on www.agora.culture.gov.uk)



First stage – part 2: business recovery requirements – Boulton Museum Case Study

- Exercise 1 – be the senior manager and
.....



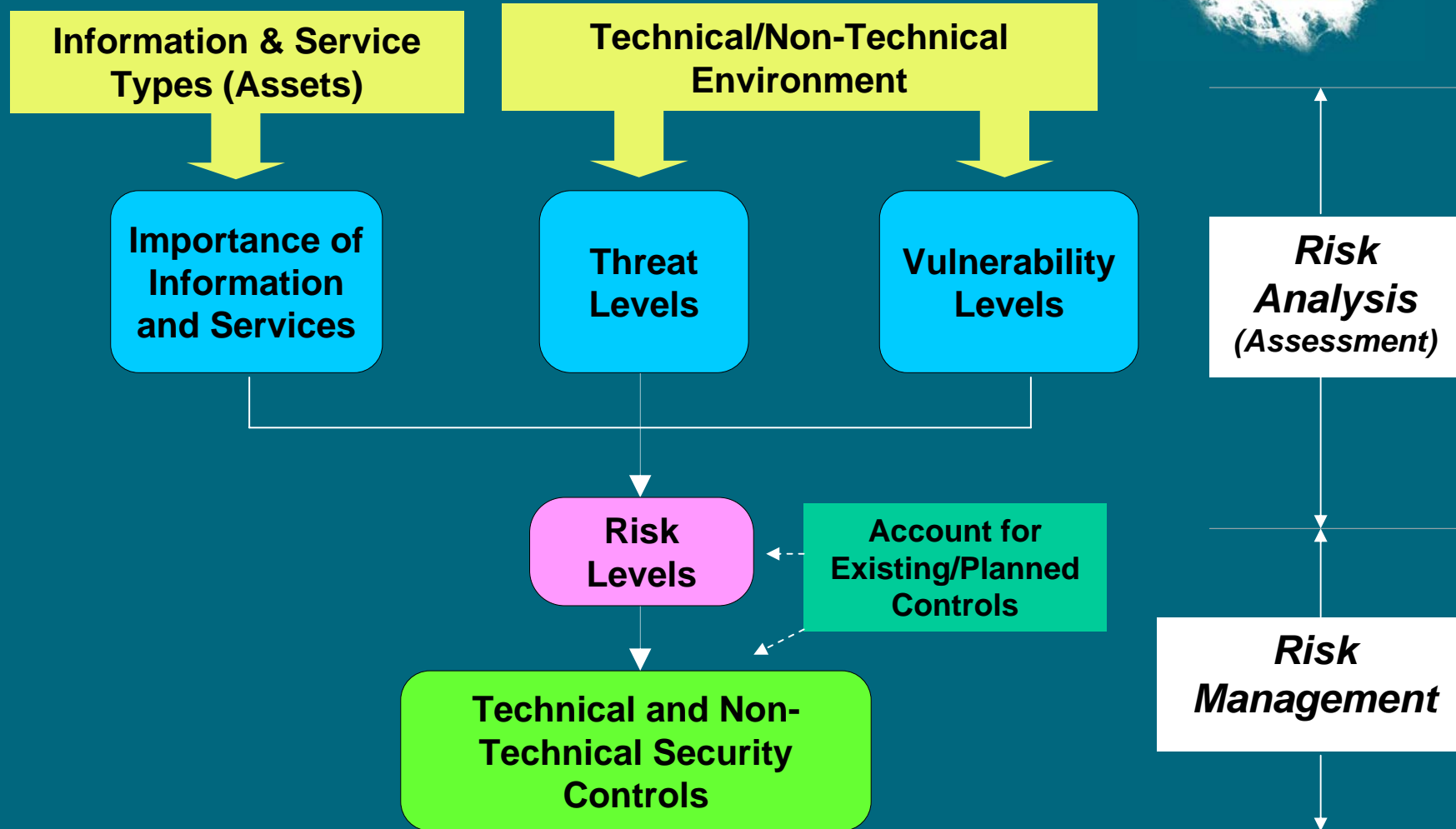
First stage – part 2: business recovery requirements

Boulton Museum Case study

- Exercise 1 – specimen completed forms
(copy later)



First stage: risk reduction – assessing the risks





First stage: risk reduction – types of control

- Risk avoidance
- Risk transfer
- Reduction of threat
- Reduction of vulnerability
- Reduction of impact
- Detection
- Recovery



First stage: risk reduction – control examples (1)

To mitigate the risks to IT, including communications, systems:

- identification and authentication (I&A) controls
- logical access control mechanisms
- ongoing use of audit logs (trails)
- facilities and procedures to ensure malicious software is prevented, or detected and removed
- content scanning facilities
- routing tables protected and subject to good change control facilities and procedures
- network protected against denial of service attacks
- effective back-up procedures and related facilities in place



First stage: risk reduction – control examples (2)

To mitigate the risks not just to IT etc., but also other facilities, services, collections, etc.:

- control of physical access to sites and buildings
- control of physical access to rooms and areas within buildings
- fire protection
- water/liquid/flood protection
- environmental protection
- power protection
- personnel procedures
- Incident reporting and handling scheme



First stage: risk reduction – document results

- Initial draft list of risk reduction controls
- Review with appropriate management
- Confirm in stage 2

(see guidance & template -
www.agora.culture.gov.uk)

- Part wider security risk analysis & management review??



First stage – risk reduction controls – Boulton Museum Case Study

- Exercise 2



First stage: risk reduction controls

Boulton Museum Case study

- Exercise 2 – example answers
(copy later)



First stage: part 2

- Open forum discussion:
 - horizon scanning
 - working together
 - any other topic



First stage: part 2 - summary

- Visible senior ('Board level') management backing at outset for business continuity programme & then key documents from the various stages
- Senior management aware & reminded of importance of an effective business continuity programme & consequences if not in place ... & indeed that effective business continuity management a strategic issue
- All business areas & related senior personnel involved, particularly to ensure all key areas covered
- Senior business managers have sufficient understanding of business impact results – otherwise recovery requirements will be inaccurate, & either excessive or inadequate
- Results from first stage signed off by senior ('Board' level) management
- ***Above all that it is kept simple!***



First stage: part 2 - next steps

- Business recovery requirements forms to senior managers for completion
- Time for completion & resolving queries
- Document business recovery requirements
- Produce Stage 1 report and obtain 'Board' level sign-off
- Document initial view on risk reduction controls and obtain agreement
- Next workshop – business continuity strategy - 7th March 2006



First stage: business recovery requirements

- “Surgeries”