Risk Management and Digital Preservation

Sharon McMeekin
Head of Training and Skills, DPC
Getting Started with Digital Preservation
Risk Management and Digital Preservation

• Risk management basics
• Risks to digital media
• Having a go
• Taking it further
What is Digital Preservation?

“the series of managed activities necessary to ensure continued access to digital materials for as long as necessary”

(Beagrie & Jones, Digital Preservation Handbook)
Risk Management Basics

• What is risk?
• ISO:31000 “the effect of uncertainty on objectives”
• So what is risk management?
• Positive or negative
• Why is risk management a good thing [for digital preservation]?
Overview of RM Process

1. Identify internal and external context
2. Identify risks
3. Analyse and assess risks
4. Manage and treat risks
5. Monitor and review
6. Communicate

Sharon McMeekin
sharon@dpconline.org
@SharonMcMeekin

www.dpconline.org
RM Basics

• Identify risk, and the consequence of it happening
• Assign values to likelihood and impact
• Determine mitigation techniques
• (Some models) assign risk areas and define ‘appetite’
• Review periodically
• Also remember ‘opportunity’ as well as ‘risk’
Identifying Risks

Some examples of risks to digital media:

• File format obsolescence
• Media degradation (bit rot)
• Media obsolescence
• Hardware obsolescence
• Viruses
• Dissociation (loss of context)
• Network failures
• ...etc...
## Evaluating Risks

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Major</td>
<td>Moderate</td>
</tr>
<tr>
<td>Likely</td>
<td>Major</td>
</tr>
<tr>
<td>Possible</td>
<td>Major</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Major</td>
</tr>
</tbody>
</table>
## Example Risk

<table>
<thead>
<tr>
<th>RISK</th>
<th>Contents of archive drive deleted by accident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence</td>
<td>Data loss, Disassociation of other data sets</td>
</tr>
<tr>
<td>Likelihood</td>
<td>4</td>
</tr>
<tr>
<td>Impact</td>
<td>5</td>
</tr>
<tr>
<td>Score</td>
<td>20</td>
</tr>
<tr>
<td>Frequency</td>
<td>Weekly, sudden</td>
</tr>
<tr>
<td>Owner</td>
<td>Senior Information Risk Owner</td>
</tr>
<tr>
<td>Response</td>
<td>Regular tiered back-ups, integrity checking, access policy, strict control of permissions, staff training</td>
</tr>
<tr>
<td>New Likelihood</td>
<td>2</td>
</tr>
<tr>
<td>New Impact</td>
<td>2</td>
</tr>
<tr>
<td>New Score</td>
<td>4</td>
</tr>
<tr>
<td>Frequency of Review</td>
<td>Annual</td>
</tr>
</tbody>
</table>
Taking It Further

• Risk appetite
• Explosive risks
• Risk AND opportunity
• PRINCE2 project management
• Intelligent Risk Management
Some Resources

- ISO:31000
  Risk management. Principles and guidance
  www.ico.org/iso/home/standards/iso31000.htm

- DRAMBORA
  www.repositoryaudit.eu/about/

- TIMBUS
  www.timbusproject.net/

- TNA digital continuity service

- SPOT
  www.dlib.org/dlib/september12/vermaaten/09vermaaten.html
Exercise

• In small groups pick select a risk and work through RM steps
  – Be clear on difference between risk and consequence
  – Think of possible mitigation steps
  – Decide scores for before and after mitigation

• 20 mins to discuss and then report back
A Simple Risk Assessment

- Identify Risk
- Consequence
- Likelihood
- Impact
- Score
- Owner
- Responses/Mitigation

- New Likelihood
- New Impact
- New Score
- Proximity
- Trend
- Frequency of Review