Best Practice and Minimum Standards in Digital Preservation

Adrian Brown, UK Parliament
Oracle PASIG, London, 5 April 2011
Introduction

- Why do we need best practice?
- Sources for best practice
- Audit and certification standards
- Maturity model for digital preservation
- Developing best practice
Why do we need best practice?

• The right thing to do
• Benchmarking
• Sharing experience
• Defining requirements
• Quantifying benefits
Sources for best practice

- Standards
- Legislation
- Repository audit and certification standards
- Practitioners
Standards

- ISO 14721 – OAIS
- ISO 15489 – Records management
- ISO 9001 – Quality management
- ISO 27001 – Information security
- BS 5454 – Archival storage
- PAS 197 - Code of practice for cultural collections management
Legislation

- General statutes
  - Privacy
  - Freedom of information
- Sector-specific and enabling legislation
  - Public Records
  - Legal Deposit
- Regulation
  - Sarbanes-Oxley
Practitioners
Trustworthy digital repositories

• Provides reliable, long-term access to managed digital resources to its designated community
• Organisation, processes and infrastructure are all fit-for-purpose
• Understands, monitors and mitigates risks
• Periodically and transparently audited
A brief history of certification

- OCLC/RLG Attributes (2002)
- CPA/RLG Task Force (1996)
- TRAC (2007)
- DRAMBORA (2007)
- nestor Criteria (2006)
- CRL 10 Principles (2007)

Dependencies:

Future Standards:
- ISO 16363 (forthcoming)
- ISO 16919 (forthcoming)
- DIN 31644 (forthcoming)
- DSA (2010)
- PLATTER (2008)
Joining them up

- **Basic Certification**: DSA certification

- **Extended Certification**: Basic Certification + externally reviewed and publicly available self-audit based on ISO 16363 or DIN 31644

- **Formal Certification**: Basic Certification + full external audit and certification based on ISO 16363 or DIN 31644
CRL 10 Core Principles

1. Maintenance of digital objects
2. Organisational fitness
3. Contractual and legal rights and responsibilities
4. Policy framework
5. Acquisition and ingest criteria
6. Integrity, authenticity and usability of digital objects
7. Metadata
8. Dissemination requirements
9. Preservation planning
10. Technical infrastructure
A maturity model for digital preservation
Maturity Levels

Awareness

Minimum standards

Good practice

Best practice

Capability
# Maturity Levels

<table>
<thead>
<tr>
<th>Stage</th>
<th>Maturity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness</td>
<td>0 – No awareness</td>
<td>The organisation has no awareness of either the need for the process or the basic principles for applying it.</td>
</tr>
<tr>
<td></td>
<td>1 – Awareness</td>
<td>The organisation is aware of the need to develop the process, and has an understanding of basic principles.</td>
</tr>
<tr>
<td></td>
<td>2 – Roadmap</td>
<td>The organisation has a defined roadmap for developing the process.</td>
</tr>
<tr>
<td>Capability</td>
<td>3 – Basic process</td>
<td>The organisation has implemented a basic process.</td>
</tr>
<tr>
<td></td>
<td>4 – Managed process</td>
<td>The organisation has implemented a comprehensive, managed process, which reacts to changing circumstances.</td>
</tr>
<tr>
<td></td>
<td>5 – Optimised process</td>
<td>The organisation undertakes continuous process improvement, with proactive management.</td>
</tr>
</tbody>
</table>
### Process Perspectives

<table>
<thead>
<tr>
<th>Process Perspective</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A - Organisational viability</td>
<td>Governance, organisational structure and resourcing of the repository, including financial and staff management.</td>
</tr>
<tr>
<td>B - Stakeholder engagement</td>
<td>Processes to engage with stakeholders within and external to the repository, including content depositors and users.</td>
</tr>
<tr>
<td>C - Legal basis</td>
<td>Management of privacy, FOI, contractual, licensing, and other legal rights and responsibilities.</td>
</tr>
<tr>
<td>D - Policy framework</td>
<td>Policies, strategies, and procedures which govern the operation and management of the repository.</td>
</tr>
<tr>
<td>E - Acquisition and ingest</td>
<td>Processes to acquire and ingest content into a repository.</td>
</tr>
<tr>
<td>F - Bitstream preservation</td>
<td>Processes to ensure preservation at the bitstream level of all stored content over time.</td>
</tr>
<tr>
<td>G - Logical preservation</td>
<td>Processes to ensure the continued accessibility of the logical content over time.</td>
</tr>
<tr>
<td>H - Metadata management</td>
<td>Processes to create, manage and update all metadata required to support management and use of the repository.</td>
</tr>
<tr>
<td>I - Dissemination</td>
<td>Processes to enable discovery and dissemination of stored content within the designated user community.</td>
</tr>
<tr>
<td>J - Infrastructure</td>
<td>Physical and technical infrastructure, including security, required to support the repository.</td>
</tr>
</tbody>
</table>
## Assessing maturity

A table with ratings for various aspects of maturity is shown. The table is divided into columns labeled A to J and rows labeled 0 to 5. The ratings range from 0 to 4.

- **An approved digital preservation policy exists**:
  - Row 0: A, B, C, D, E, F, G, H, I, J (all 0)
  - Row 1: A, B, C, D, E, F, G, H, I, J (all 1)
  - Row 2: A, B, C, D, E, F, G, H, I, J (all 2)
  - Row 3: A, B, C, D, E, F, G, H, I, J (all 3)
  - Row 4: A, B, C, D, E, F, G, H, I, J (all 4)

- **Basic characterisation process (format id) and ad hoc preservation planning and action processes exist**:
  - Row 0: A, B, C, D, E, F, G, H, I, J (all 0)
  - Row 1: A, B, C, D, E, F, G, H, I, J (all 1)
  - Row 2: A, B, C, D, E, F, G, H, I, J (all 2)
  - Row 3: A, B, C, D, E, F, G, H, I, J (all 3)
  - Row 4: A, B, C, D, E, F, G, H, I, J (all 4)

- **Acquisition policy exists, ingest standards and processes are updated to reflect new accessions**: Not explicitly shown in the table, but implied by the context of the assessment.
Developing best practice

- Ingest
  - Forensic IT protocols
- Bitstream preservation:
  - Integrity management (e.g. LOCKSS)
- Logical preservation:
  - Preservation strategies
  - Preservation action tools (e.g. PLANETS)
  - Significant properties identification (e.g. JISC studies)
  - Technology risk assessments
Developing best practice

• Stakeholders:
  • Best practice for creators, end users etc.

• Policies:
  • Model Digital Preservation Policies (e.g. JISC DP Policies Study, DCC template, exemplars)

• Organisational:
  • CPD, vocational training (e.g. DPTP, DigCurV)
  • Professional body – Chartered Institute for Digital Preservation?
Thank-you!