<table>
<thead>
<tr>
<th></th>
<th>Level 1 (Protect your data)</th>
<th>Level 2 (Know your data)</th>
<th>Level 3 (Monitor your data)</th>
<th>Level 4 (Repair your data)</th>
</tr>
</thead>
</table>
| Storage and Geographic Location  | - Two complete copies that are not collocated  
- For data on heterogeneous media (optical discs, hard drives, etc.) get the content off the medium and into your storage system | - At least three complete copies  
- At least one copy in a different geographic location  
- Document your storage system(s) and storage media and what you need to use them | - At least one copy in a geographic location with a different disaster threat  
- Obsolescence monitoring process for your storage system(s) and media | - At least three copies in geographic locations with different disaster threats  
- Have a comprehensive plan in place that will keep files and metadata on currently accessible media or systems |
| File Fixity and Data Integrity   | - Check fixity on ingest if it has been provided with the content  
- Create fixity info if it wasn't provided with the content | - Check fixity on all ingests  
- Use write-blockers when working with original media  
- Virus-check high risk content | - Check fixity of content at fixed intervals  
- Maintain logs of fixity info; supply audit on demand  
- Ability to detect corrupt data  
- Virus-check all content | - Check fixity of all content in response to specific events or activities  
- Ability to replace/repair corrupted data  
- Ensure no one person has write access to all copies |
| Information Security             | - Identify who has read, write, move and delete authorization to individual files  
- Restrict who has those authorizations to individual files | - Document access restrictions for content | - Maintain logs of who performed what actions on files, including deletions and preservation actions | - Perform audit of logs |
| Metadata                         | - Inventory of content and its storage location  
- Ensure backup and non-collocation of inventory | - Store administrative metadata  
- Store transformative metadata and log events | - Store standard technical and descriptive metadata | - Store standard preservation metadata |
| File Formats                     | - When you can give input into the creation of digital files encourage use of a limited set of known open formats and codecs | - Inventory of file formats in use | - Monitor file format obsolescence issues | - Perform format migrations, emulation and similar activities as needed |
ACE (Audit Control Environment)


<table>
<thead>
<tr>
<th>Collection Name</th>
<th>Type</th>
<th>Total Files*</th>
<th>Last Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>jdk 1.6.0 installation</td>
<td>local</td>
<td>7083</td>
<td>Mon Jul 21 13:14:06 EDT 2008</td>
</tr>
<tr>
<td>xplot 0.90</td>
<td>local</td>
<td>39</td>
<td>Fri Jul 18 17:05:24 EDT 2008</td>
</tr>
<tr>
<td>important stuff</td>
<td>local</td>
<td>39</td>
<td>Fri Jul 18 16:46:21 EDT 2008</td>
</tr>
<tr>
<td>images</td>
<td>srb</td>
<td>1400</td>
<td>Tue Jul 22 11:44:04 EDT 2008</td>
</tr>
</tbody>
</table>

- Audit in progress     - Audit idle

* - Total files and status not updated until after first sync.
Integrity Management Service (IMS)
Token example

<?xml version="1.0" encoding="utf-8"?>
<token xmlns="http://umiacs.umd.edu/adapt/ace/token/1.0">
  <token-class>SHA-256-0</token-class>
  <digest-service>SHA-256</digest-service>
  <name>/state/myfile.txt</name>
  <round-id>319782</round-id>
  <time-stamp>2008-09-16T14:57:27.936-0400</time-stamp>
  <proof>
    <element index="0">
      <hash>7957e058645f953f8e2d11c919414adffab7df12df3e7902eb446b02a40ac908</hash>
    </element>
    <element index="1">
      <hash>9287c2e19f715a67dcb59da8a724084b448dd9382668f347338f1ce20f435872</hash>
    </element>
    <element index="2">
      <hash>e9cc9417014a43e29870f60504cdebe3c49ba9472b4481bb2ff5f7a68ce147bb</hash>
      <hash>73384002a2fd512874801fb62e1defbb1902668f04d8a96d6cb90b703d16a506</hash>
    </element>
    <element index="1">
      <hash>d312e4551a3d3ee6d695d96b8851f3ad1574096305f18d4f052fe853bfe14482</hash>
    </element>
  </proof>
</token>
An Illustrated Guide to Cryptographic Hashes
Steve Friedl

http://www.unixwiz.net/techtips/iguide-crypto-hashes.html