Terms and Definitions

Digital Continuity. Digital continuity is the ability to use your information in the way you need, for as long as you need.

Long-Term. A period of time long enough for there to be concern about the impacts of changing technologies, including support for new media and data formats, and of a changing user community. This period extends into the indefinite future.

Internal and External Stakeholders. Plans for different types of records, models for continuity approaches and criteria, and a framework of repository components and services will require tighter cooperation and engagement between long-standing partners such as IT, archives/RM units, software and service providers, and other support functions. Interdependencies between and among the operations of records producing units, legal and statutory requirements, information technology policies and governance, and historical accountability should be systematically addressed.

Legacy Electronic Records. Legacy electronic records are embedded in obsolete software or formats with no backward compatibility or export function to newer software and formats. Legacy electronic records can only be retrieved and rendered by the software application and/or format in which they are embedded or by a viewer. Typically, computer code must be written to transform legacy digital information into newer, technology neutral open file formats.

Open Standard Technology Neutral File Format. A technology neutral file format is one that is designed to run on multiple platforms in a variety of software applications. It is an open file format in that the design of the specification involves collaboration in an open, public environment. Technology neutral open file formats can evolve as technology changes and thereby provide a backward compatibility to older versions. Examples of technology neutral file formats are XML and PDF/A.

Preservation Ready Born Digital Information. Preservation ready born digital information is encoded in a technology neutral open standard format and all necessary metadata has been assembled so that it can be moved (i.e., ingest) into a digital preservation repository with little or no additional processing.

Hash Digest Algorithm (Cryptographic). A cryptographic hash algorithm takes any digital object regardless of size or content type and normalizes it to a fixed length bit stream (e.g., 128 bits). This fixed length bit stream is called a hash digest and it serves as a "digital fingerprint" of a larger digital object. Cryptographic hash algorithms are used to detect accidental or intention corruption in digital objects and to authenticate digital signatures: the change of a single bit in the original digital object will result in a different hash digest. It is computationally infeasible for two different digital objects to have the same hash digest or to reconstruct a data object from this hash digest.

Standard Hash Algorithm 1 (SHA-1). A cryptographic hash digest developed by the U.S. National Security Agency A 160-bit hash function to be part of the Digital Signature Algorithm. The hash digest contains 160 bits, which increases the computational infeasibility of two different digital objects having the same hash value. However, researchers have demonstrated that it in rare circumstances it is computationally feasible for two different digital objects to have the same SHA-1 hash digest.

Standard Hash Algorithm 2 (SHA-2). Designed by the National Security Agency, SHA-2 has a 256 bit hash value, which makes it the most powerful hash digest algorithm currently available.

Digital Continuity Resources

UNITED KINGDOM

- Digital Continuity Project - The National Archives of the UK can be found at www.nationalarchives.gov.uk/dc-guidance.
- Government Procurement Service, Digital continuity framework agreement can be found at http://www.archives.qld.gov.au/Recordkeeping/DigitalContinuity/Pages/Publications.aspx

NEW ZEALAND

- Digital Continuity Action Plan Managing Information for Public Sector Efficiency, Archives New Zealand (2009), can be found at http://www.archives.govt.nz/.

AUSTRALIA

- National Archives of Australia Digital Continuity Plan can be found at http://www.naa.gov.au/records-management/agency/digital/digital-continuity/plan/index.aspx.
- Queensland State Archives digital continuity publications page can be found at http://www.archives.qld.gov.au/Recordkeeping/DigitalContinuity/Pages/Publications.aspx.

CENTER FOR RESEARCH LIBRARIES

- The Center for Research Library list of reports on digital archives and repositories is available at http://www.crl.edu/archiving-preservation/digital-archives/digital-archive-reports.

ARMA INTERNATIONAL

- Gordon E.J. Hoke, CRM, "Future Watch: Strategies for Long-Term Preservation of Electronic Records," Information Management, May/June 2012.
- "How the Information Management Governance Reference Model (IGRM) Complements ARMA International's Generally Accepted Principles of Records Management (GARP) - White Paper," ARMA International (2011). http://www.edrm.net/resources/edrm-white-paper-series/igrm-garp

Usable Information is Available and Complete

Usable *= Information meets your requirements for how you want to use it.*

Available *= You can find the information you need and have the technology to open it and work with it in the way you need.*

Complete *= Everything you need to use, understand and trust the information is present, including the content, context and all the necessary metadata.*