# Protecting Official Records as Evidence in the Cloud Environment

Anne Thurston

International Records Management Trust

# Introduction

In a cloud computing environment, government records are held in virtual storage. A service provider looks after much of the maintenance, but the government still owns the records, and government agencies still must comply with legal requirements. The records still are essential for protecting citizens' rights and entitlements, demonstrating accountability, and providing the basis for data credibility.

# Record Keeping Requirements

Cloud computing has obvious benefits and less obvious risks. The risks are mainly in relation to how records and data, particularly in terms of their security and integrity, are managed in the cloud. Records management requirements for official records must be defined in relation to legal requirements, for instance for personal and financial information, access to information, privacy, data protection, and disaster recovery.

# Requirements

Metadata (data describing the context, content and structure of records) is essential to demonstrate that the records are authentic and to make it possible to access and interpret them over time. Metadata must be captured when the records are created and then, through system logs and audit trails, to document how the records are used and any changes to their structure.

# Risks

1. Records and data can be lost or corrupted unintentionally or as the result of unauthorised action by a malicious insider, a hacker or a shared server user.
2. The service provider may not be able to preserve records with very long retention periods, such as property or pension records.
3. The records may not be returned at the end of contract or they may be returned in a format that the agency finds difficult to access or use.

# Risks

4 A lack of standardised interfaces can make it difficult or expensive to transfer services or information from one cloud provider to another.

5 Service providers may not share audit logs documenting access to applications and services and how they are used. In this case, it is not possible to demonstrate authenticity, integrity and legal compliance.

# Risk Assessment

Some records management applications can be integrated with cloud computing services, but many cloud computing services lack records functionality, and cloud architectures often lack technical standards for records storage and use. A risk assessment should be carried out when a contract is negotiated to insure that information integrity and security can be protected.

# Questions for a Risk Assessment

1. Does the service provider have experience of implementing records management solutions in the cloud? Have the records requirements been defined; can the service provider demonstrate the ability to meet the requirements?
2. What are the provisions for preventing hackers and security threats? Is there information, for instance personnel records, that is too sensitive or important to be held in the cloud computing environment?

# Risk Assessment

3 What back-up arrangements are in place to ensure that records and the associated structure and metadata can be restored if anything happens to them?

4 Will the records will be available when 24/7 access is required?

5 Can the service provider demonstrate that the information will be stored in acceptable jurisdictions?

# Risk Assessment

6 When the contract ends, will all records be returned to the agency within an agreed timeframe and in an acceptable format?

7 What are the provisions for external risk auditing, certification and monitoring, and how are they enforced? How often is the provider audited by external bodies, and when did the last audit take place? How are incidents reported and addressed?

8 Who will have access to the records and what controls will govern third party access?

# Risk Assessment

9 Is the provider's system functionality capable of accommodating the required metadata fields? Can additional metadata fields be added as needed?

10 Does the vendor provide certificates of destruction?

9 Are there provisions for transferring records with permanent value to secure long-term storage (Trusted Digital Repositories)?

# Risk Assessment

If you are planning for cloud computing in your country, it is important to assess the risks for official records.