



Risk Assessment of Digital Holdings

Angela Dappert

Digital Preservation Coalition
The TIMBUS Project







Overview

Risk management

In general

In Information Management



In Digital Preservation

Status of RM in Digital Preservation

- Examples
- Guidelines
- Applications
- Tools







Motivation: Risk Impact

- Damage to or loss of our digital assets
- Loss of access, understandability and authenticity
- Statutory or regulatory breach
- Deterioration of product or service quality
- Damage to reputation
- Damage to financial viability
- On public well-being
- On repository staff
- Environmental damage







Risk

is uncertainty of outcome







Digital Preservation

The series of managed activities necessary to ensure continued access to digital materials for as long as necessary.

Beagrie & Jones

How do you determine which action to take?







Digital Preservation

Proactive

preservation

to our digital assets

Keep risks from becoming issues

Risk Management

Deal with issues when they arise

conservation

Reactive

Risk: may happen

- ❖ negative impact threat
- (positive impact an opportunity)

Issue: has happened

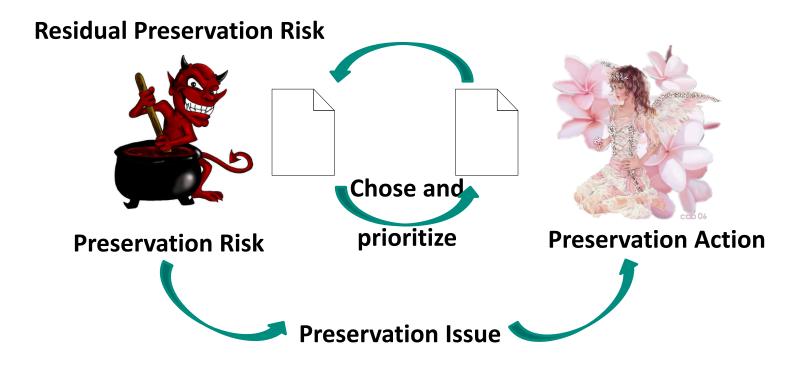






Digital Preservation

Central function: Risk Management



- A support function for the overall organization
- Integrated into the organizational flow







Risk Management – Familiar Terrain

Risk Management – Principles and Guidelines: e.g. ISO 31000

Information Risk Management &

Information Assurance Maturity Model IAMM

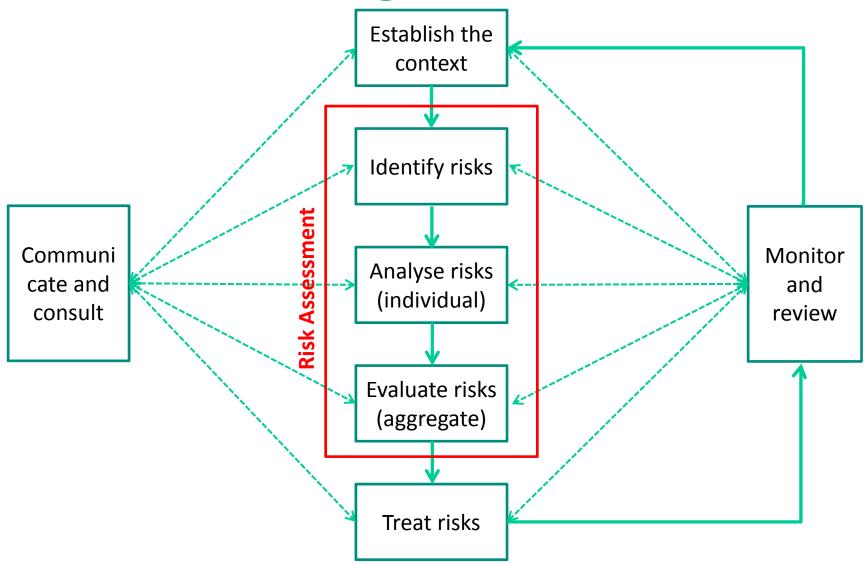
Digital Continuity

e.g. TNA Risk Assessment Handbook



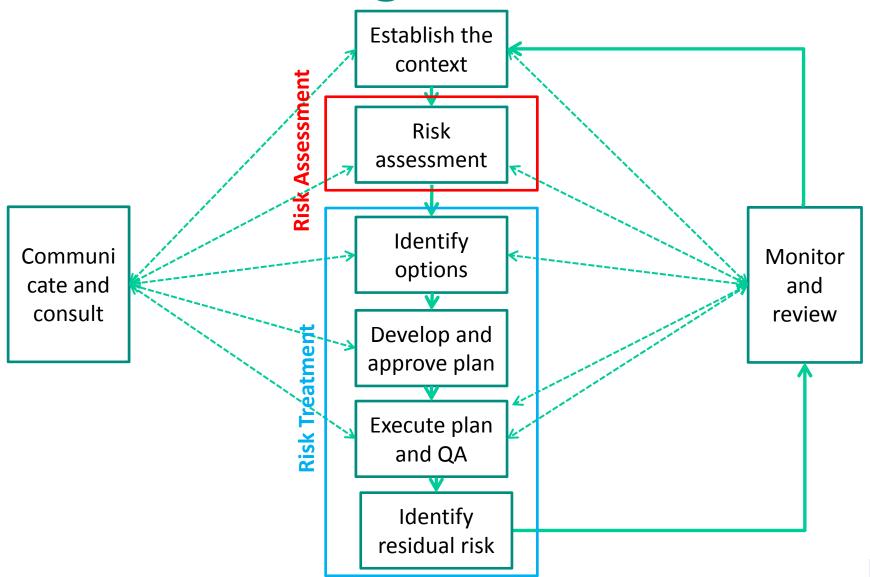






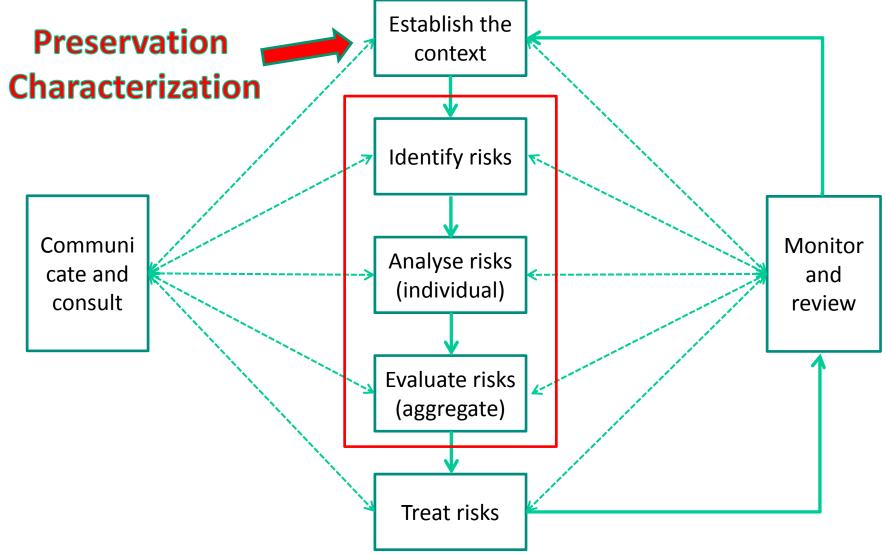






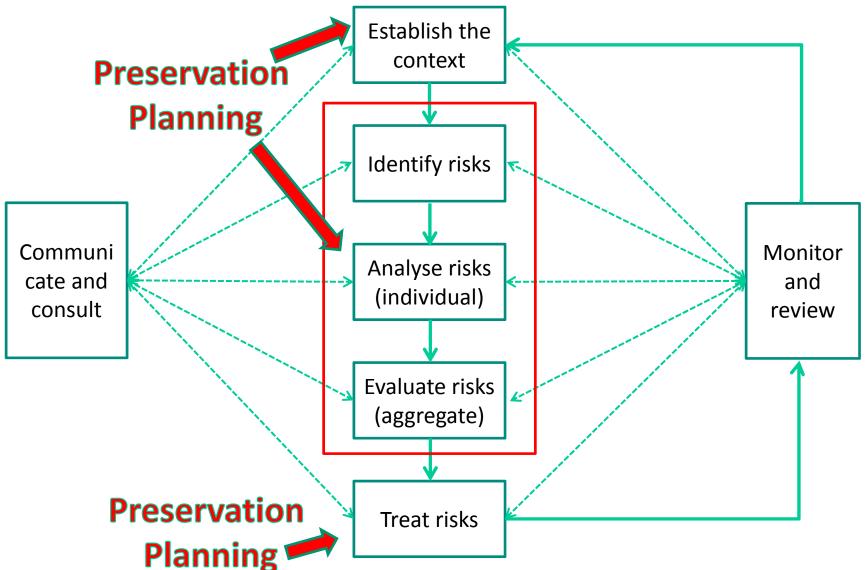






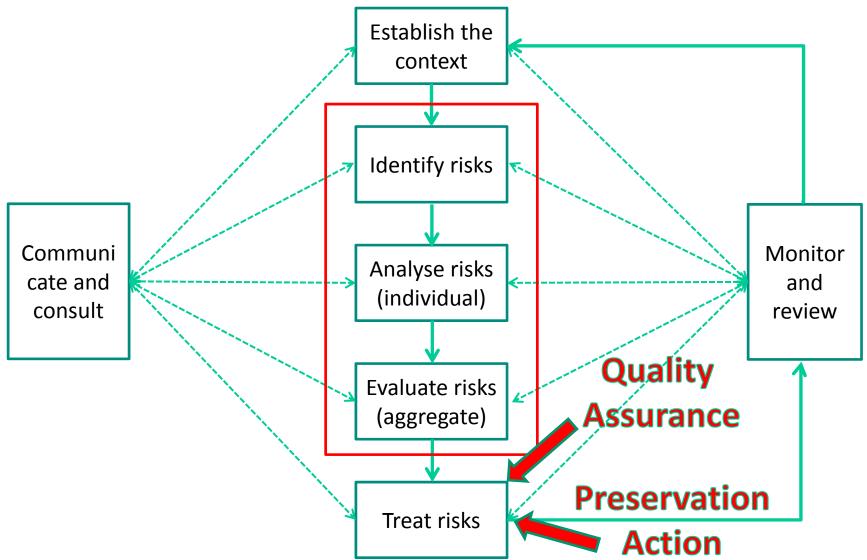






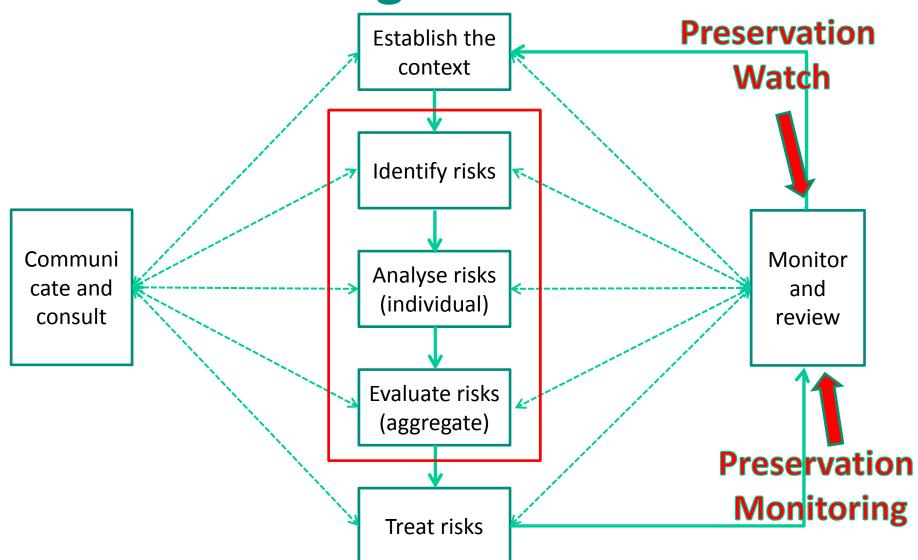
















Risk Context - Dimensions

Scope

Assets

Quality Expectations

Assumptions

Stakeholders

Objectives

Mandate

Constraints (PESTLE)

Activities

Functions





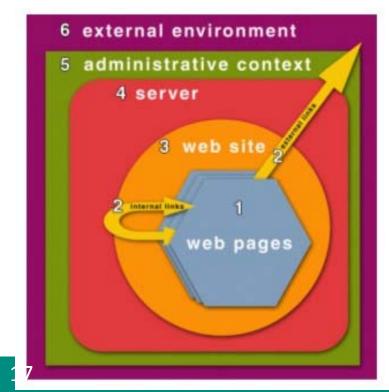




Risk Context: Scope

- A web page as a stand-alone object
- Considering the links into it and out from it
- A semantically coherent set of linked web pages
- A digital entity residing on a server
- A website as an entity within an administrative setting
- A website as part of an external environment







The Context: The Bigger Scope



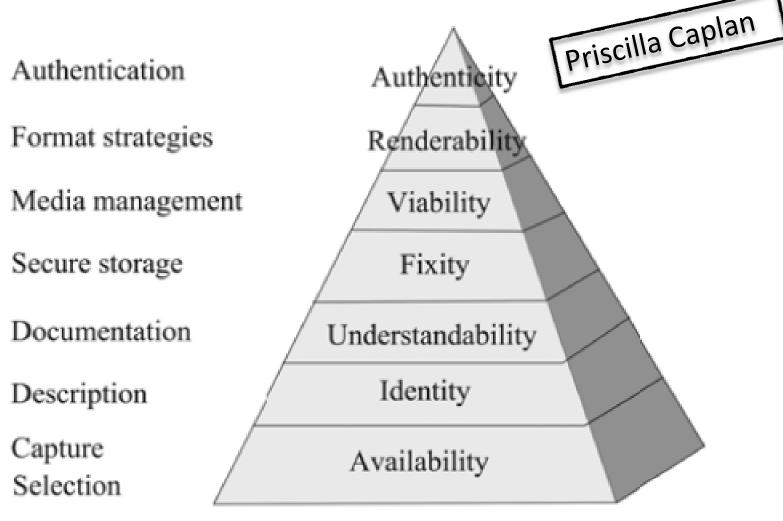
3	OR	GANIZATIONAL INFRASTRUCTURE	3-1
	3.1	GOVERNANCE & ORGANIZATIONAL VIABILITY	3-1
	3.2	ORGANIZATIONAL STRUCTURE & STAFFING	3-3
	3.3	PROCEDURAL ACCOUNTABILITY & PRESERVATION PO	OLICY
		FRAMEWORK	3-5
	3.4	FINANCIAL SUSTAINABILITY	The Consultative Commun.
	3.5	CONTRACTS, LICENSES, & LIABILITIES	The Consultative Committee for Space Data Systems
4	DIG	ITAL OBJECT MANAGEMENT	Draft-Recommendation for Space-Data-System-Practices
	4.1	INGEST: ACQUISITION OF CONTENT	AUDIT-AND.
	4.2	INGEST: CREATION OF THE AIP	CERTIFICATION OF . TRUSTWORTHY DIGITAL . REPOSITORIES
	4.3	PRESERVATION PLANNING	REPOSITORIES#
	4.4	AIP PRESERVATION	
	4.5	INFORMATION MANAGEMENT	DRAFT-RECOMMENDED-PRACTICE¶
	4.6	ACCESS MANAGEMENT	CCSDS-652.0-R-1¶
5	INF	RASTRUCTURE AND SECURITY RISK MANAGEM	RED-BOOK¶ October-2009¶
	5.1	TECHNICAL INFRASTRUCTURE RISK MANAGEMENT	reak (Continuous)
	5.2	SECURITY RISK MANAGEMENT	5-12 or



The Context:



Preservation Goals => Objectives



Preservation Goals



Means





Digital Preservation Coalition The Context: Preservation Functions

An intellectual context for the work:

Commitment to digital object maintenance

Organisational fitness

Legal & regulatory legitimacy

Effective & efficient policies

Acquisition & ingest criteria

Integrity, authenticity & usability

Provenance

Dissemination

Preservation planning & action

Adequate technical infrastructure

DRAMBORA © HATII UofGlasgow, 2007 Digital Object Management Digital Repository Environment Technical Organisational Infrastructure Infrastructure & Security Institutional Context

(CRL/OCLC/NESTOR/DCC/DPE meeting, January 2007)







Risk Identification: Breakdown Structures and Prompt Lists

- Technological
- Physical
- Organisational
- Socio-cultural
- Legal

- Economic
- Financial
- Political
- Contractual
- Environmental

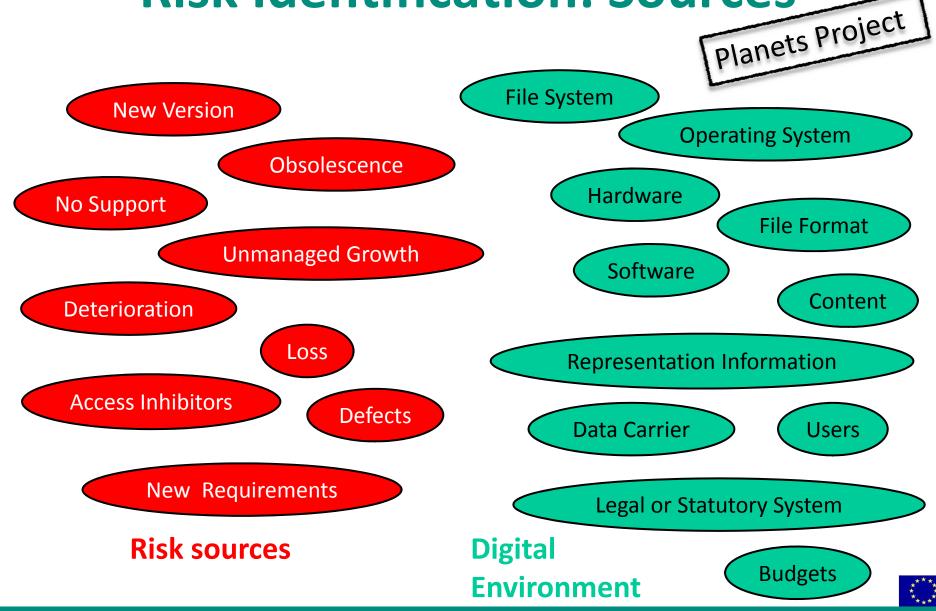








Risk Identification: Sources





Risk Identification:



Vulnerabilities and Sources

,			
	toiro,	Process	Software faults
Linsé	Barateiro,		Software obsolescence
1 300	et al.	Data	Media faults
1			Media obsolescence
Vulnerabilities			Hardware faults
		Infrastructure	Hardware obsolescence
			Communication faults
			Network service failures
		Disasters	Natural disasters
			Human operational errors
		Attacks	Internal attacks
			External attacks
	Threats	Management	Economic failures
			Organizational failures
		Legislation	Legislative changes
			Legal requirements

Table 1. Taxonomy of vulnerabilities and threats to digital preservation.





Risk identification

Blake, TNA

R1. UNDERSTANDING & ACTION

Continuity risk is neither understood nor addressed cohesively at either the right levels or across the organisation (esp. IM, IT and IA responsibilities)

ORGANISATIONAL RISK

R2. RISK GOVERNANCE

Continuity risk is not reflected in the risk management and information governance processes at either the right levels or across the organisation

R3. INFORMATION VALUE

The Organisation does not understand the nature and value of its Information Assets enough to be able to apply Continuity risk management

PROCESS RISK

R4. IM SYSTEMS & PROCESSES

Existing, legacy or future IM systems and processes do not maintain Continuity to Information Assets over time or through change

R5. IT SYSTEMS & PROCESSES

Existing, legacy or future IT systems and processes do not maintain Continuity to Information Assets over time or through technological change

R6. BUSINESS SYSTEMS. STRUCTURES & PROCESSES

Existing, legacy or future organisational business systems. structures and processes do not maintain Continuity to Information Assets over time or through organisational change

OPERATIONAL RISK

R7. CONTEXT ABSENT

Required Information Context / Metadata is absent at creation / capture

R8. CONTEXT

MAINTAINED Information Context / Metadata is not maintained over time or through change

R9. CONTENT & CONTEXT SEPARATED

Information Context / Metadata and Information Content (Data) are separated over time or through change

R10, CONTEXT LOST

Information Context / Metadata is lost over time or through change

R11. CONTENT

Information Content (Data) is lost over time or through change

R12. PROVENANCE MAINTAINED

Provenance / Audit data about the Information Asset is not maintained over time or through change

OPERATIONAL RISK

OBSOLESCENT TECHNOLOGY The Information Asset format cannot be accessed by available technology

infrastructure,

platforms.

applications

R13.

LOCK-IN The Information Asset is locked in to a specific technology /

vendor

R15. ACCESS R14. TECHNOLOGY RESTRICTIONS

Management of encryption and file-level passwords for Information Asset are not maintained

PREVENTING DISCOVERY

The Information Asset is hidden in a structurally complex digital format inaccessible location

OPERATIONAL RISK

TECHNOLOGY CONTEXT Information Asset format There is cannot be insufficient used with the Information Context / functionality Metadata to by available understand technology the (infrastructure, Information platforms, Asset applications)

INCOMPATIBLE

required

R18. INSUFFICIENT INSUFFICIENT PROVENANCE

There is insufficient audit / provenance data to trust the authenticity of Information Asset

CONTINUITY FAILURE

R20. FAILURE IN THE INTEGRITY OF THE INFORMATION ASSET

Information is partial: missing crucial metadata, content or context

CONTINUITY FAILURE

R21. FAILURE IN THE AVAILABILITY OF THE INFORMATION ASSET

Information cannot be located or cannot be opened with available technology

CONTINUITY FAILURE

R22. FAILURE IN THE USABILITY OF THE INFORMATION ASSET

Information cannot be used as needed with the available technology, cannot be understood without its context or cannot be trusted as authentic









Risk Analysis

Determine

Probability

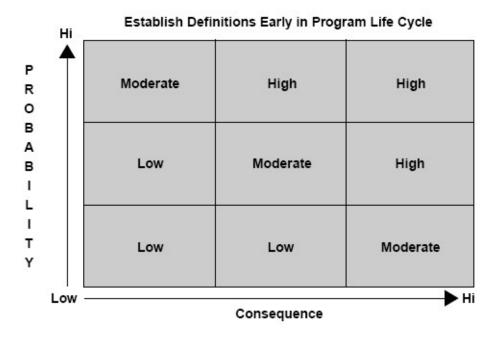
Impact

(Proximity)



Calculate severity

of the identified risks









British Library

Factors Influencing Risk Impact

Risk of loss

Future rarity

Alternative storage provision

Heritage value

Mandatory requirement

Legal deposit obligation

Existing external commitment

Strategic considerations

Opportunity & timing

Size & rate of growth

Opportunities for access

Alternative access provision

Revenue

User need

User demand

Risk to physical collections

Remote access

Doability

Effort

Freely available

Operational improvements







archiving

Risk Impact Influenced by Remote

- relevancy to the organization's collection(s);
- significance (essential, desirable, ephemeral);
- archival role (primary archives for resource, informal agreement for full or partial capture, other);
- maintenance (key indicators of good site management);
- redundancy (captured by more than one archive);
- risk response (time delay and action based on test notifications);
- capture requirements (complexity of site structure, update cycle, MIME types, dynamic content, and behaviour indicators);
- size (number of pages, depth of crawl required, etc.).







Risk Evaluation

Look at all risk as an aggregate

Probability
Impact
(Proximity)

Calculate severity

Objectives

Policy and Strategy

Organisational risk threshold and appetite

Identify need for action







Risk Treatment Options

Accept

accept the potential risk

Reduce

implement controls to lower probability or impact of the risk

Avoid

eliminate the risk cause and/or consequence

Fallback

Put in place alternative action for when the risk materializes

Transfer

compensate for loss, such as purchasing insurance





Example Risk Assessment: The British Library 2007

Available online



Risk Assessment 2007

British Library - Digital Preservation Team

Objective: This document is an internal working document for The British Library. It serves to help prioritise The British Library's digital content based upon This Anioritisation will do analysis of risk.

This prioritisation will determine the content that will be ingested into The British a framework of continuous improvement and the final prioritisation will reflect this change based upon the most recent information available.







How much information do we need?

Unsatisfactory storage	Bit stable storage	Content stable storage	Archival storage
Hand-held carriers	Images have been transferred on managed hard disk storage Storage is backed up	Content has been QA'ed Metadata has been produced and QA'ed File formats have been identified Representation Information has been deposited	Automatic check for corruption via checksums Automatic replication over remote locations Digital signatures Integration with Primo / ILS







Tools to Help

- Risk management:
 - Drambora (The Digital Repository Audit Method Based On Risk Assessment): self-certification

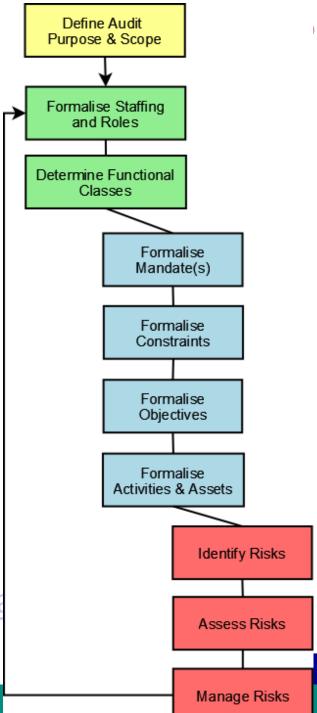




DRAMBORA

- Digital Repository Audit Method Based On Risk Assessment
- Online interactive tool
- Developed by the Digital Curation Centre (DCC) and Digital Preservation Europe (DPE)
- Identify, assess, manage, and mitigate risks
- Risk ontology

http://blogs.ecs.soton.ac.uk/keepit/tag/drambora/





DRAMBORA interactive

Register for DRAMBORA

Logged in: Andrew McHu

Auditor
Business Manager
Data Liaison Office

at: Florida Digital Archive

University of Florida

Last Login: 28 Nov 2008

Home

Online Help User Admin

Report Results

Latest News

Get Expert Help

Download Offline
Version

Submit Feedback

DRAMBORA Training

The DRAMBORA Team
Dissemination
DRAMBORA Users

Management

Strategy(ies):

About Objectives Benefits

Before the Assessment

Digital Repository Audit Method Based on Risk Assessment







DRAMBORA (Online Tool :: Assessment Centre :: View Risk	
	Mandate View Constraints View Objectives View Activities View ssessment and Risk Management View	
select alternativ	navigate between the various related characteristics of this single risk. You can risks using the selection panel on the right hand side of the screen.	Budgetary reduction (Reposito operational budget is reduced)
Risk Name:	Budgetary reduction	Enforced cessation of reposit
Identified*:	8th October 2008	operations (Repository is forced cease its business activities.)
Potential Impact*:	Medium (to Organisational Viability)	_
Probability:	High	defined activities—
Severity:	48%	defined objectives—
Risk Description:	Repository's operational budget is reduced	defined constraints
Risk Vulnerability:	Local recession provokes budgetary reduction of government financed repository	#defined mandate
Risk Relationships:	Budgetary reduction to Enforced cessation of repository operations (Contagious)	· Hassessment progress
Nature of Risk:	Physical Environment:	——————————————————————————————————————
100700	Personnel, Management & Admin Procedures:	
	Operations & Service Delivery:	Quarter 3, 2008 (8th Oct 2008
	Hardware, Software or Communications Equipt & Facilities:	
Risk Owner(s):	Repository Management	
Functional	Supporting Functional Classes	
Class(es):		
Class(es):	Mandate & Commitment to Digital Object Maintenance, Organisational Fitness	









Tools to Help

- Risk Management:
 - Drambora (The Digital Repository Audit Method Based On Risk Assessment): self-certification
 - TIMBUS project: ERM (Enterprise Risk Management) tools extended to digital preservation





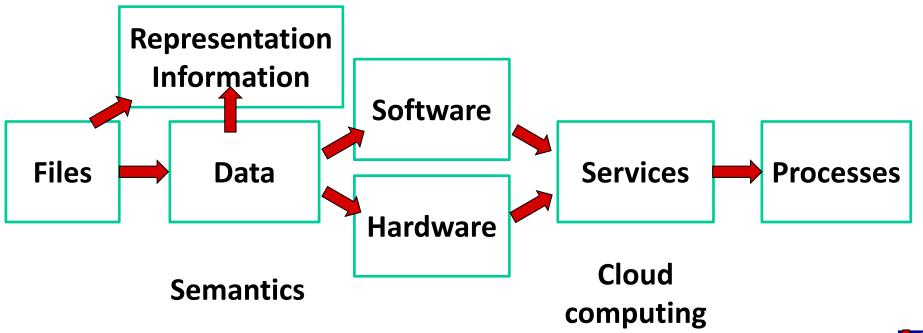


TIMBUS

Digital Preservation

Risk and Business Continuity

Management







TIMBUS Task 4.1 ERM

- Intelligent Risk Management
 - Learning from previous situations



- Reasoning from context
- Automating risk detection and response
- Complete business modelling, including IT systems, legal constraints, etc.











Tools to Help

- Risk management:
 - Drambora (The Digital Repository Audit Method Based On Risk Assessment): self-certification
 - TIMBUS project: ERM (Enterprise Risk Management) tools extended to digital preservation
 - TRAC/TDR: framework for establishing certified trustworthiness







The repository shall have specifications for how the AIPs are stored down to the bit level.

Supporting Text

This is necessary in order to ensure that the information can be extracted from the AIP over the long-term.

Examples of Ways the Repository Can Demonstrate It Is Meeting This Requirement

Documentation of the format of AIPs; EAST and DEDSL descriptions of the data components (see references [B6] and [B7]).

Discussion

The repository should specify the Representation information down to the bit level of each AIP component and must specify how the separate components are packaged together. The Representation Information must be available for each AIP and must to the AIP. Often, repositories are tempted to describe AIP content where a program will then be used to convert the information to a their Designated Communities. However, if those programs ever information would be lost in all the AIPs that relied on that program,

CCSDS The Consultative Committee for Space Data Systems-Draft-Recommendation-for-Space-Data-System-Practices¶

AUDIT-AND. CERTIFICATION OF TRUSTWODTHY,





Tools to Help

- Risk management:
 - Drambora (The Digital Repository Audit Method Based On Risk Assessment): self-certification
 - TIMBUS project: ERM (Enterprise Risk Management) tools extended to digital preservation
 - TRAC/TDR: framework for establishing certified trustworthiness
- Context identification: DROID, JHOVE, FIDO, FITS, file, ...
 - Assess the characteristics of your digital assets
 - Profile your collections
- Risk treatment planning: Plato
- Risk treatment: A variety of preservation and QA tools







Thank you

