



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?



to our digital assets



Digital Preservation

Proactive

preservation

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)

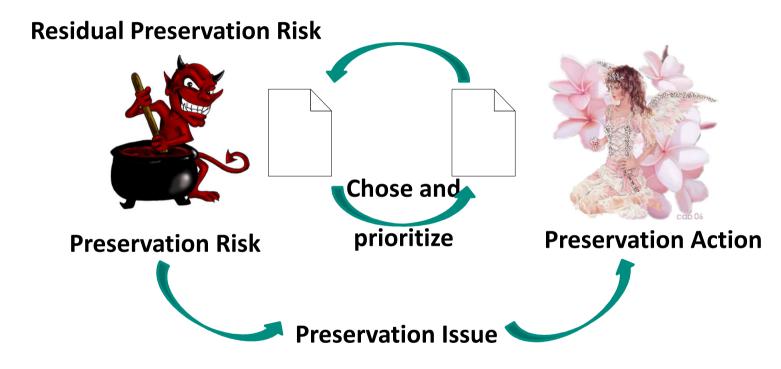
Issue: has happened





Digital Preservation

Central function: Risk Management



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





Risk Management – Familiar Terrain

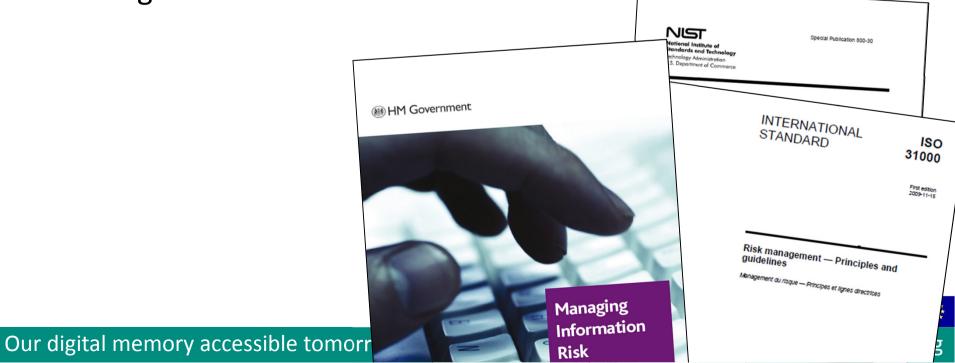
Risk Management – Principles and Guidelines: e.g. ISO 31000

Information Risk Management &

Information Assurance Maturity Model IAMM

Digital Continuity

– e.g. TNA Risk Assessment Handbook







Risk Management

Principles

that need to be satisfied to make risk management effective

Framework

organizational arrangements for

- designing,
- implementing,continually
- monitoring,

- reviewing
- continually improving

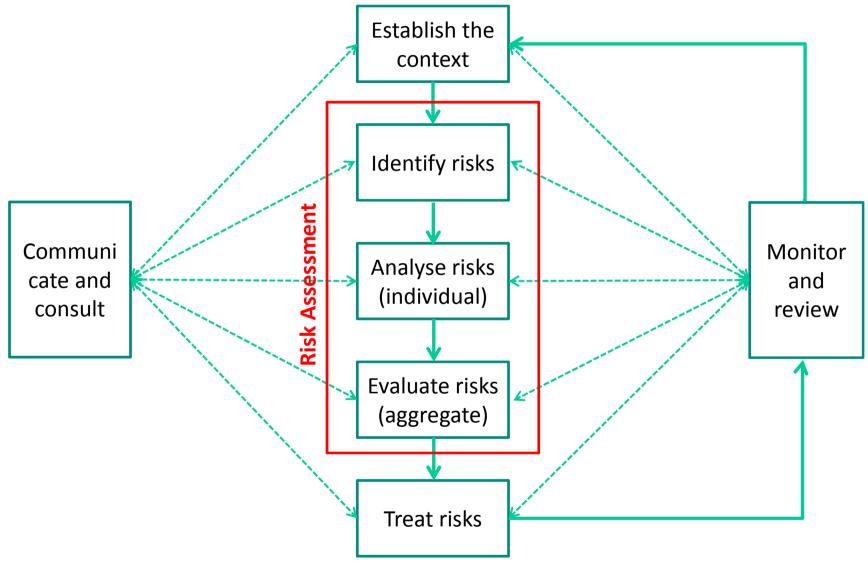
risk management throughout the organization

Process



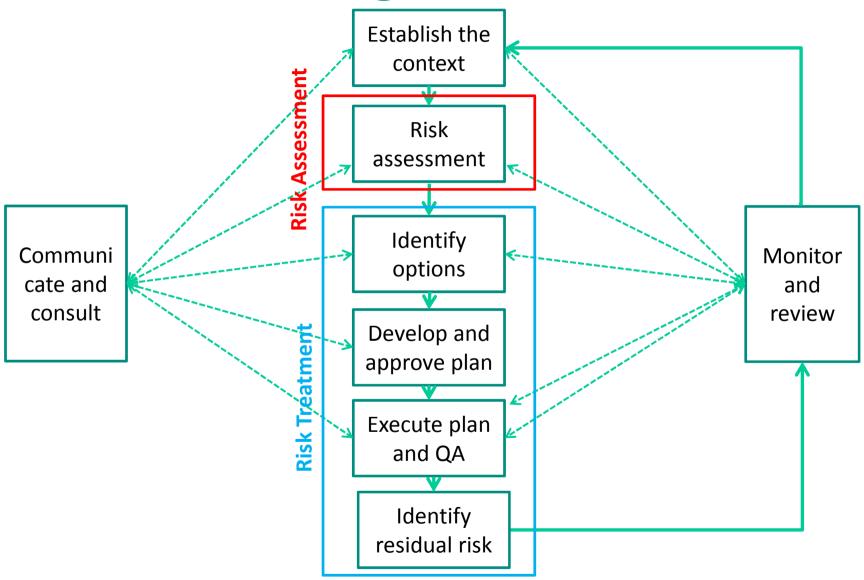






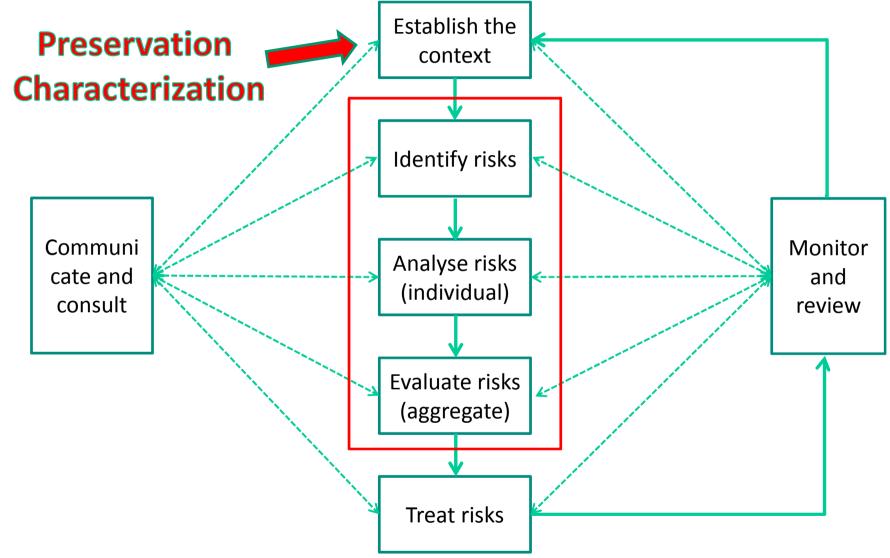






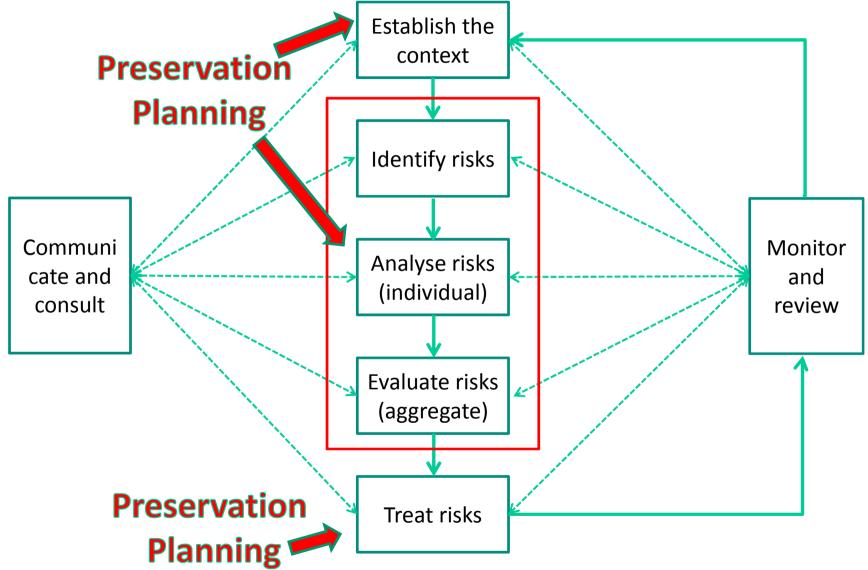






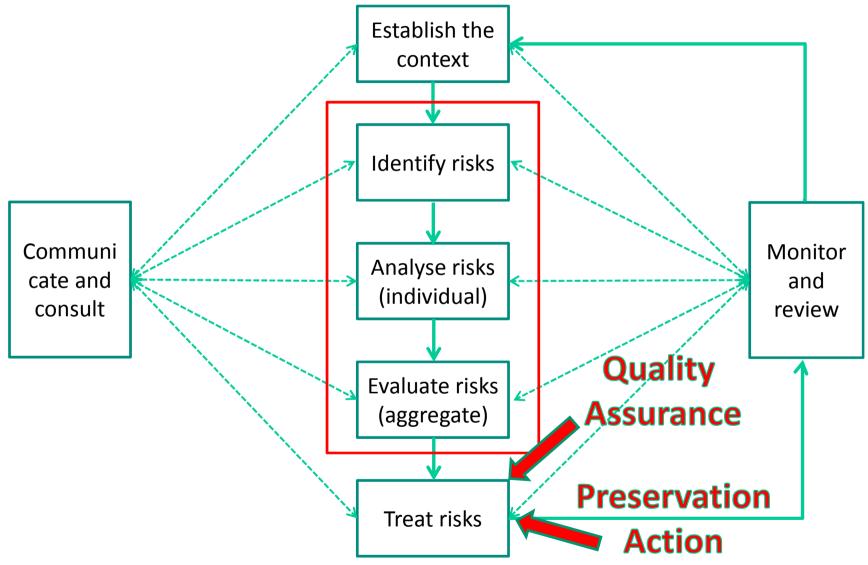






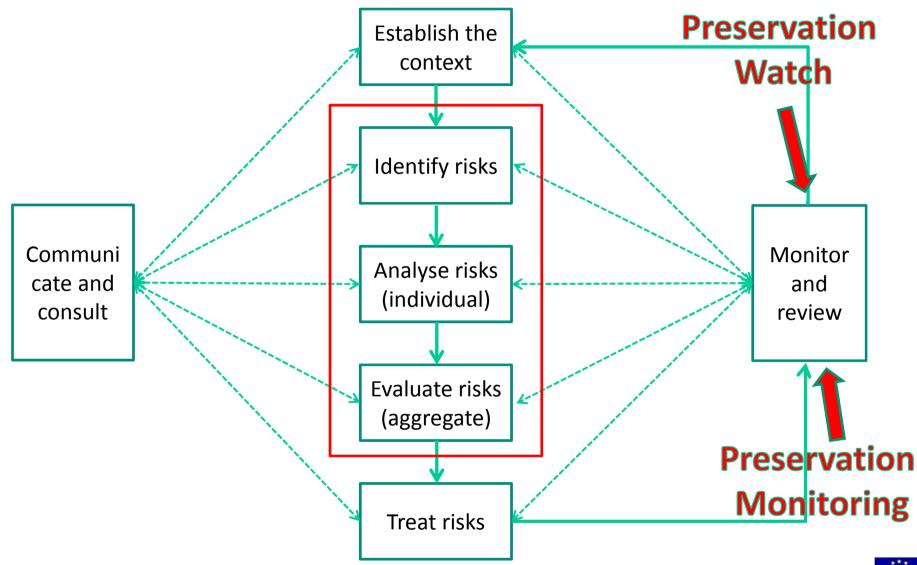
















Risk Context - Dimensions

Scope

Assets

Quality Expectations

Stakeholders

Activities

Objectives

Functions

Assumptions

Mandate

Constraints (PESTLE)



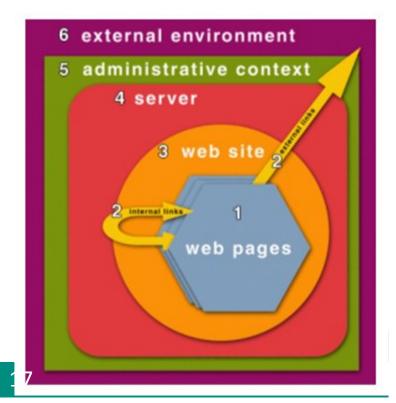




Risk Context: Scope

- 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









Timbus 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	3.3 PROCEDURAL ACCOUNTABILITY & PRESERVATION POLICY			
		FRAMEWORK	3-5		
	3.4	FINANCIAL SUSTAINABILITY	The Consultative Committee		
	3.5	CONTRACTS, LICENSES, & LIABILITIES	The Consultative Committee for Space Data Systems		
4	DIG	SITAL 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	PED -		
	5.1	TECHNICAL INFRASTRUCTURE RISK MANAGEMENT	October-2009¶ Section Break (Continuous)		
	5.1	SECURITY RISK MANAGEMENT	5 12		
	3.4	SECURITINSK MANAGEMENT	3-12 org		



The Context:



Priscilla Caplan

Preservation Goals => Objectives

Authentication

Format strategies

Media management

Secure storage

Documentation

Description

Capture

Selection

Means

Authenticity

Renderability

Viability

Fixity

Understandability

Identity

Availability

Preservation Goals









he 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)





Digital Preservation Coalition

Risk Identification: Breakdown Structures and Prompt Lists

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

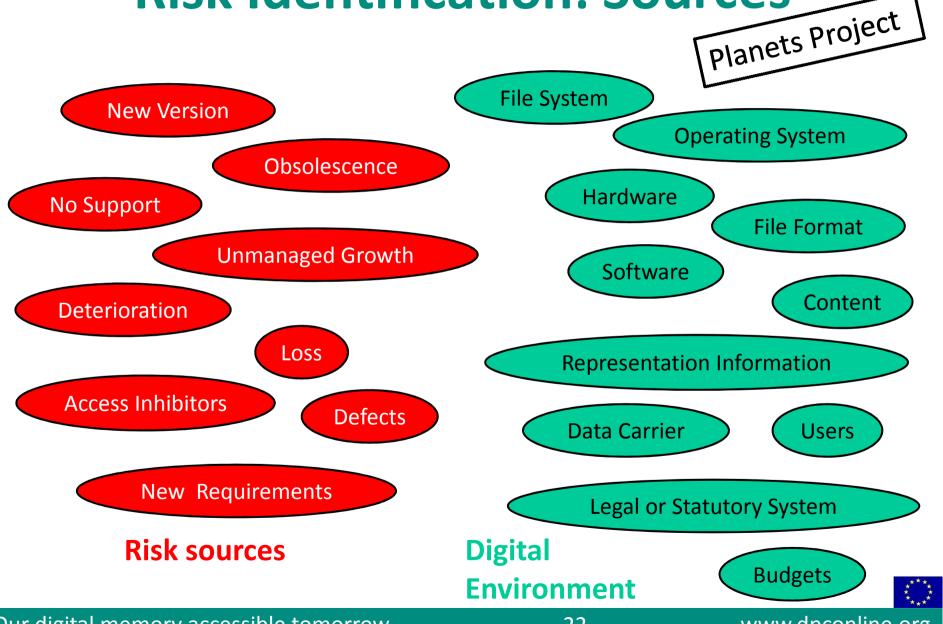
- Economic
- Financial
- Political
- Contractual
- Environmental







Risk Identification: Sources









	+oiro,	Process	Software faults		
Linsé	Barateiro,		Software obsolescence		
	et al.	Data	Media faults		
\			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		
	1	Legislation	Legislative changes		
		_ 3	Legal requirements		
,					

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





Risk identification

Blake, TNA

ORGANISATIONAL RISK

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)

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 i capture

R8. CONTEXT MAINTAINED

Information Context / Metadata is not maintained over time or through

R9. CONTENT SEPARATED

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

R10. CONTEXT

Information Context / Metadata is lost over time or through change

R11. CONTENT

Information ontent (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

TECHNOLOGY The Information Asset format cannot be accessed by available technology infrastructure. platforms. applications

OBSOLESCENT

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

R15. ACCESS R14. TECHNOLOGY RESTRICTIONS

PREVENTING DISCOVERY

The Management Information of encryption Asset is hidden in a passwords for structurally complex Information digital format Asset are not or an maintained inaccessible location

OPERATIONAL RISK

R17. TECHNOLOGY Information Asset format cannot be used with the required functionality by available technology (infrastructure

platforms,

applications)

R19. INSUFFICIENT INSUFFICIENT

PROVENANCE

There is There is insufficient insufficient audit / Information provenance Context / data to trust Metadata to understand authenticity of Information Information Asset 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

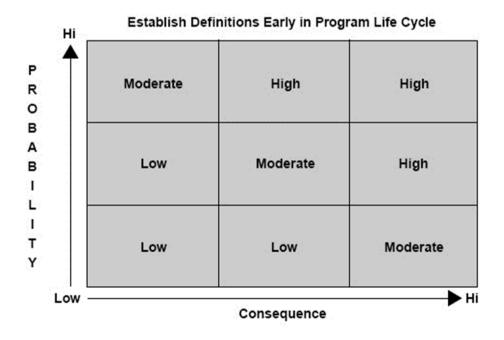
Impact

(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







Control for web

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 Impact



- on repository staff
- on public well-being
- damage to or loss of assets
- statutory or regulatory breach
- damage to reputation
- damage to financial viability
- deterioration of product or service quality
- environmental damage
- loss of authenticity and understandability





Risk Evaluation

Look at all risk as an aggregate

Probability
Impact
(Proximity)

Calculate severity

Cost 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 potential.

This prioritisation will determine the content that will be ingested into The British Library's Digital Object Management system. It is managed and maintained within a framework of continuous improvement and the final prioritisation will reflect this change based upon the most recent information available.







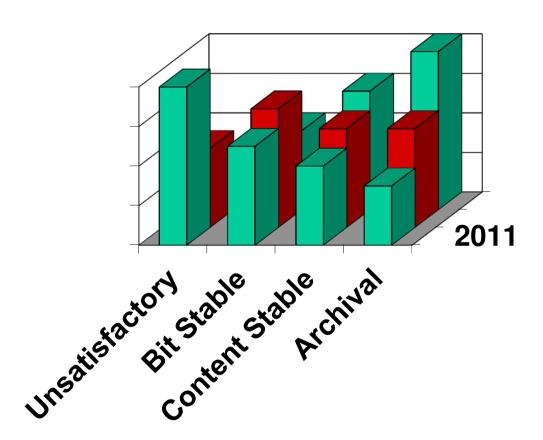
How much information do we need?

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





Performance Goals









Tools to Help

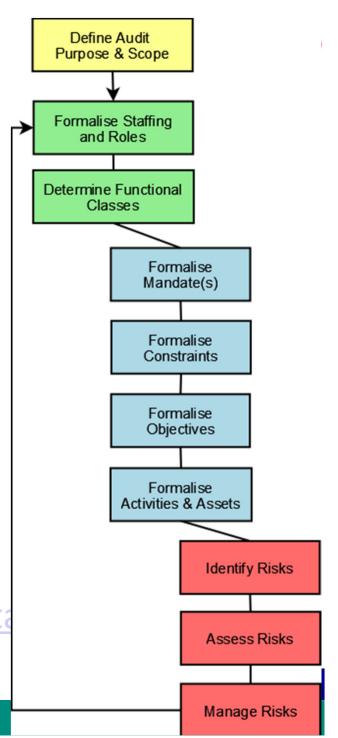
- Risk management:
 - Drambora (The Digital Repository Audit Method Based On Risk Assessment): self-certification



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/ta
g/drambora/





DRAMBORA interactive

Digital Repository Audit Method Based on Risk Assessment







Active Repository: Florida Digital Archive at University of Florida 💠 Update

Register for DRAMBORA

Logged in: Andrew McHugh

- Auditor
- Business Manager
- Data Liaison Officer

at: Florida Digital Archive at University of Florida

Last Login: 28 Nov 2008

Home

Online Help

User Admin

Before the Assessment

Report Results

Latest News

Get Expert Help

Download Offline Version

Submit Feedback

DRAMBORA Training

About

Objectives

Benefits

The DRAMBORA Team

Strategy(ies):

Dissemination

DRAMBORA Users

DRAMBORA C	Online Tool :: Assessment Centre :: View Risk	
	Mandate View Constraints View Objectives View Activities View ssessment and Risk Management View	
	navigate between the various related characteristics of this single risk. You can erisks using the selection panel on the right hand side of the screen.	□ identified risks ■ Budgetary reduction (Repository
Risk Name:	Budgetary reduction	operational budget is reduced)
Identified*:	8th October 2008	 Enforced cessation of repositor operations (Repository is forced to 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	
Risk Relationships:	Budgetary reduction to Enforced cessation of repository operations (Contagious)	⊞assessment progress-
Nature of Risk:	Physical Environment:	⊟saved snapshots
	Operations & Service Delivery:	Quarter 3, 2008 (8th Oct 2008)
	Hardware, Software or Communications Equipt & Facilities:	
Risk Owner(s):	Repository Management	
Functional Class(es):	Supporting Functional Classes	
	Mandate & Commitment to Digital Object Maintenance, Organisational Fitness	
Linked to:		
Management		









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





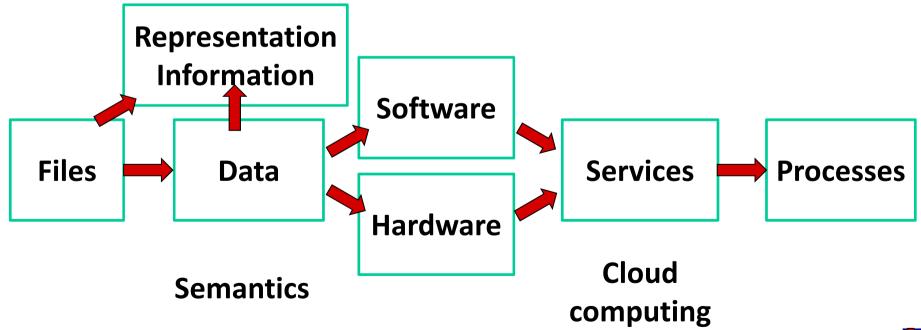


TIMBUS

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. Rather than DP focus alone











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
 - 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 f information would be lost in all the AIPs that relied on that program.

ECSDS The Consultative Committee for Space Data Systems.

Draft-Recommendation-for-Space-Data-System-Practices¶

TRUSTWORTHY -





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
 - 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

