




Trust, Audit and Certification


FACULTY OF INFORMATICS



Compliance

- Trustworthy repositories
- Compliance to best practices, standards
- 3 core initiatives, of which 2 prescriptive
 - RLG- National Archives and Records Administration Digital Repository Certification Task Force: Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC)
 - NESTOR: Catalogue of Criteria of Trusted Digital Repositories
 - DCC/DPE: DRAMBORA: Digital Repository Audit Method Based on Risk Assessment
- Embedding into OAIS model

FACULTY OF INFORMATICS




Compliance

TRAC:

- Three sections
 - A. Organisational Infrastructure
 - B. Digital Object Management
 - C. Technologies, Technical Infrastructure & Security

FACULTY OF INFORMATICS




Compliance

TRAC and Preservation Planning 1:

- **A3.2** Repository has procedures and policies in place, and mechanisms for their review, update, and development as the repository grows and as technology and community practice evolve
 - Watch Services, triggers
 - Verification against changes in the environment
 - Update of preservation plans
- **A3.6** Repository has a documented history of the changes to its operations, procedures, software, and hardware that, where appropriate, is linked to relevant preservation strategies and describes potential effects on preserving digital content
 - History of preservation plans (created, reviewed and updated)
 - Plato: Automated documentation of planning activities

FACULTY OF INFORMATICS




Compliance

TRAC and Preservation Planning 2:

- **A3.7** Repository commits to transparency and accountability in all actions supporting the operation and management of the repository, especially those that affect the preservation of digital content over time
 - Solid workflow in consist manner enables informed and well-documented decisions
 - Explicit definition of objectives and measurement units
- **B1.1** Repository identifies properties it will preserve for digital objects
 - Objective Tree

FACULTY OF INFORMATICS



Compliance

TRAC and Preservation Planning 3:

- **B3.1** Repository has documented preservation strategies
 - Preservation Plan
- **B3.3** Repository has mechanisms to change its preservation plans as a result of its monitoring activities.
 - Watch Services, triggers
 - Verification against changes in the environment
 - Update of preservation plans

FACULTY OF INFORMATICS

TU VIENNA Trust in a Repository

- How is trust established, maintained, and secured?
- How to verify trust?
- Audit and Certification
- Digital Repository Audit and Certification Wiki
 - <http://wiki.digitalrepositoryauditandcertification.org/bin/view>
 - ISO/DIS 16363 - Audit and certification of trustworthy digital repositories
 - ISO/DIS 16919 - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories

FACULTY OF INFORMATICS

TU VIENNA Nestor

- Kompetenznetzwerk Langzeitarchivierung
- Kriterienkatalog vertrauenswürdige digitale Langzeitarchive, 2006
- Kriterien für die Bereiche
 - Organisatorischer Rahmen
 - Umgang mit Objekten
 - Infrastruktur und Sicherheit

FACULTY OF INFORMATICS

TU VIENNA Nestor Kriterien

- Organisatorischer Rahmen
 - A2.2 Das digitale Langzeitarchiv stellt die Interpretierbarkeit der digitalen Objekte durch seine Zielgruppe sicher.
 - A4.5 Die Fortführung der festgelegten Aufgaben ist auch über das Bestehen des Archivs hinaus sichergestellt.
- Umgang mit Objekten
 - B9.2 Das Archiv definiert, welche Eigenschaften der digitalen Objekte für den Erhalt von Information signifikant sind.
 - B12.1 Das Archiv identifiziert seine Objekte und deren Beziehungen eindeutig und dauerhaft.

FACULTY OF INFORMATICS

TU VIENNA ...and in practice?

- Criteria catalogues not always helpful
 - How to measure fulfilment
 - How to prove trust
 - How to improve
- Audit and Certification as ultimate goal
- Self-audit as important step
- Risk assessment

FACULTY OF INFORMATICS

TU VIENNA Risk and Digital Preservation

- Digital Preservation *is* Risk Management
- Transform uncertainties into manageable risks
- Standard risk management models in many disciplines

FACULTY OF INFORMATICS

TU VIENNA DRAMBORA

- Digital Repository Audit Method Based on Risk Assessment
 - Risk assessment workflow
 - Risk catalogue
- Facilitate internal self-assessment & reporting
- Validate appropriateness of repository's efforts
- Generate appropriate documentation

FACULTY OF INFORMATICS


TU VIENNA **Goals and Outcomes**

- Documented organisational self-awareness
- Catalogued risks
 - Composite risk score for each of eight functional classes
 - Comparison of risk scores
 - Identification of most vulnerable areas of repository
- Understanding of infrastructural successes and shortcomings
- Preparation for a full scale external audit

FACULTY OF **INFORMATICS**

TU VIENNA **Process overview**

- Establish organisational profile
- Develop contextual understanding
- Identify and classify repository activities and assets
- Derive risk register
- Assess risks
- Commit to management strategies
- Guided process with tool support



FACULTY OF **INFORMATICS**


TU VIENNA **Evidence**

- Documentary
 - Mission statement
 - Business plan, financial reports
 - Job descriptions
 - Technical documents,...
- Testimonial evidence
 - Find omissions in documentation
 - Validate documentation vs. Reality
- Observation of practice
 - Less objective, but important

FACULTY OF **INFORMATICS**

TU VIENNA **Stage 1+2: Defining the Context**

- Mandate of the repository
- Goals and objectives
- Policies the repository has in place
- Legal and contractual requirements
- Standards
- any other influences
- Basis for risk definition and assessment



FACULTY OF **INFORMATICS**

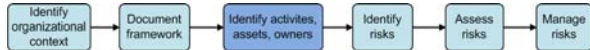
TU VIENNA **Organisational Goals**

- Associated with one of 8 functional classes
 - Acquisition & Ingest
 - Preservation & Storage
 - Metadata Management
 - Access & Dissemination
 } operational classes
- Organisation & Management
 - Staffing
 - Financial Management
 - Technical Infrastructure & Security
 } supporting classes

FACULTY OF **INFORMATICS**

TU VIENNA **3: Identify Activities, Assets and Owners**

- Conceptual model of what the repository does
- Split mission and goals into specific activities
- Assign to responsible actors
- Link to key assets
 - information
 - Software and physical assets
 - services and utilities
 - Processes and people
 - Intangibles



FACULTY OF **INFORMATICS**

TU VIENNA **Stage 4: Identify Risks**

- Assets & Activities associated with vulnerabilities
- List of risks for associated activities and assets
- Iterative brainstorming process
- Kinds of risks
 - Activities or assets fail to achieve goals
 - Internal threats
 - External threats
 - Threats to assets

FACULTY OF INFORMATICS

TU VIENNA **Examples**

- R32: Hardware or software incapable of supporting emerging repository aims
 - Insufficiently scalable
 - Incompatible with emerging systems
- R66: Preservation strategies result in information loss
 - Migration might lose 'look and feel' of documents
 - Acceptable loss?
- R30: Hardware failure
- R21: Loss of key member of staff

FACULTY OF INFORMATICS

TU VIENNA **Stage 5: Assess Risks**

- Probability
- Impact
- Relationships
- Plus
 - Manifestations
 - Risk escalation owner

FACULTY OF INFORMATICS

TU VIENNA **Risk Impact**

- In terms of:
 - impact on repository staff or public well-being
 - impact of damage to or loss of assets
 - damage to reputation
 - damage to financial viability
 - deterioration of product or service quality
 - loss of digital object authenticity and understandability
- Scale 0-6
 - Recoverable, 0-3: Zero, negligible, superficial, medium
 - Unrecoverable, 4-6: High, considerable, cataclysmic

FACULTY OF INFORMATICS

TU VIENNA **Risk Likelihood and relationships**


- Likelihood: Scale 1-6
 - 1: minimal probability, every 100 years
 - 6: very high probability, more than once a month
- Relationships
 - Atomic
 - Domino
 - Complementary
 - Contagious
 - Explosive

FACULTY OF INFORMATICS

TU VIENNA **Stage 6: Manage Risks**


- Combination of avoidance, tolerance and transfer
 - avoid circumstances in which risk arises
 - limit likelihood of risk
 - reduce potential impact of risk
 - share the risk
 - Transfer to others

FACULTY OF INFORMATICS

 **Examples**


- R32: Hardware or software incapable of supporting emerging repository aims
 - Allocate time to monitor scalability and compatibility of technologies
- R66: Preservation strategies result in information loss
 - Evaluate strategies in controlled environment before execution
 - Ensure procedures are reversible

.....
FACULTY OF **INFORMATICS**

 **Example risk**


- R31: Software failure or incompatibility
- System software is rendered incapable of facilitating current business objectives
- Example: Software update breaks dependencies of other core software services
- Avoidance:
 - Monitor ongoing suitability of software and assess value of emerging technologies
 - Evaluate effects of system changes prior to implementation
 - Anticipatory investment in software
- Transfer:
 - Seek formal assurance or SLAs from software suppliers

.....
FACULTY OF **INFORMATICS**

 **The Audit Result**


- Risk score for each risk quantifies risks' severity
- Composite risk score for each category
- Illustrates vulnerabilities
- Facilitates resource investment

.....
FACULTY OF **INFORMATICS**

 **DRAMBORA: A Summary**

- Risk-based self assessment
- Evidence is essential
- Documented self-awareness
- Risk register as basis for ongoing management
- Preparation for external audit
- Building of Trust

.....
FACULTY OF **INFORMATICS**

 **Summary**

- Trust in Digital Repositories
- Criteria catalogues
 - Trustworthy Repositories Audit and Certification (TRAC)
 - Nestor: Kriterien für digitale Archive
- Risk and Digital Preservation
- Principles of DRAMBORA
 - Overview
 - Workflow
 - Results
 - Benefits

.....
FACULTY OF **INFORMATICS**